Unitary designs in nearly optimal depth

Laura Cui,[1,*] Thomas Schuster,[2,1,3,*] Fernando Brandão,[4,1] and Hsin-Yuan Huang[1,3]

[1] *Institute for Quantum Information and Matter and Department of Physics, California Institute of Technology, Pasadena, California 91125, USA*
[2] *Walter Burke Institute for Theoretical Physics, California Institute of Technology, Pasadena, California 91125, USA*
[3] *Google Quantum AI, Venice, California 90291, USA*
[4] *AWS Center for Quantum Computing, Pasadena, California 91125, USA*

We construct ε-approximate unitary k-designs on n qubits in circuit depth $\mathcal{O}(\log k \log\log nk/\varepsilon)$. The depth is exponentially improved over all known results in all three parameters n, k, ε. We further show that each dependence is optimal up to exponentially smaller factors. Our construction uses $\tilde{O}(nk)$ ancilla qubits and $\mathcal{O}(nk)$ bits of randomness, which are also optimal up to $\log(nk)$ factors. An alternative construction achieves a smaller ancilla count $\tilde{\mathcal{O}}(n)$ with circuit depth $\mathcal{O}(k \log\log nk/\varepsilon)$. To achieve these efficient unitary designs, we introduce a highly-structured random unitary ensemble that leverages long-range two-qubit gates and low-depth implementations of random classical hash functions. We also develop a new analytical framework for bounding errors in quantum experiments involving many queries to random unitaries. As an illustration of this framework's versatility, we provide a succinct alternative proof of the existence of pseudorandom unitaries.

Random unitaries are ubiquitous across quantum science, serving both as fundamental theoretical tools and practical building blocks for quantum technologies. They provide useful models for understanding chaotic many-body dynamics [1–3], quantum gravity phenomena [4–6], and thermalization in isolated quantum systems [7–9]. Beyond their theoretical significance, random unitaries have been essential for device benchmarking [10–12], state tomography [13–15], quantum advantage demonstrations [16–18], and quantum cryptography [19–21]. From an analytical perspective, the uniform Haar measure over unitaries enables tractable mathematical investigations through its elegant structure and a wealth of established results in random matrix theory [22–27].

These fundamental roles have sparked an immense effort to understand in what situations and time-scales quantum systems can realize random unitaries. This effort is spearheaded by two notions of approximate random unitaries: *unitary k-designs* [28–34] and *pseudorandom unitaries* (PRUs) [35–37]. Intriguingly, recent work has revealed that both objects can form in drastically lower times, or *circuit depths*, than previously thought. In particular, unitary designs on n qubits can form in depth $\tilde{\mathcal{O}}(k) \cdot \log(n/\varepsilon)$ on any circuit geometry, where ε quantifies the approximation error [38, 39]. Meanwhile, PRUs can form in depth $\mathrm{poly}(\log n)$ in one-dimensional systems, and depth $\mathrm{poly}(\log\log n)$ in systems with long-range two-qubit gates [39]. At the heart of these findings is a surprising realization: that quantum systems can appear Haar-random even when their light-cones are only a small fraction of the total system size.

Despite this progress, key open questions remain, especially regarding unitary designs. While existing circuit depths for designs are optimal for *one-dimensional* systems, lower bounds suggest they may be *exponentially worse* than optimal for more general circuit architectures [39]. Resolving this question could have substantial practical importance, as many leading quantum computing platforms feature long-range circuit geometries [40–42].

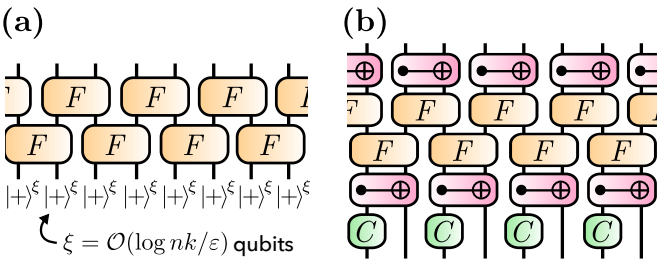

FIG. 1. Schematic of our low-depth constructions of state and unitary designs. Black vertical lines denote local patches of $\xi = \mathcal{O}(\log nk/\varepsilon)$ qubits. **(a)** Our random state designs apply a two-layer circuit of random phase gates F to the plus state. The random phases are drawn from k-wise independent hash functions on 2ξ bits. **(b)** Our random unitary designs sandwich the two-layer phase circuit between local 2-designs C and right-shuffle gates. The latter gates shuffle bitstrings on even patches conditional on odd patches (and vice versa), and are also instantiated using k-wise independent functions.

In this work, we show that, with long-range two-qubit gates, ε-approximate unitary k-designs over n qubits can be realized in a remarkably low circuit depth of $\mathcal{O}(\log k \cdot \log\log nk/\varepsilon)$. This represents an exponential improvement in the dependence on all three parameters n, k, and ε compared to all known results; the exponentially reduced dependence on k is particularly striking. Our construction uses $\tilde{\mathcal{O}}(nk)$ ancilla qubits (which begin and end in the zero state), $\mathcal{O}(nk)$ bits of randomness, and two-qubit gates of range $\mathcal{O}(\log nk/\varepsilon)$. We achieve these designs by introducing a novel random unitary ensemble (Fig. 1) that combines existing classical hash function constructions with inherently quantum ingredients to enable ultra-low circuit depths for random unitary designs.

Our main contributions are detailed as follows. First,

Unitary k-designs	Circuit depth	Ancilla count	Error
Random 1D circuit [32, 34]	$\mathcal{O}((nk + \log 1/\varepsilon) \cdot \text{poly} \log k)$	None	Relative
Blocked random 1D circuit [39]	$\mathcal{O}(k \cdot \text{poly} \log k \cdot \log n/\varepsilon)$	None	Relative
PFC circuit [35, 37]	$\mathcal{O}(nk \cdot \text{poly} \log(n))$	None	Measurable
Blocked LRFC circuit *(this work)*	$\mathcal{O}(\log k \cdot \log\log nk/\varepsilon)$	$kn \cdot \tilde{\mathcal{O}}(\log\log n/\varepsilon)$	Measurable
	$\mathcal{O}(k \cdot \log\log nk/\varepsilon)$	$n \cdot \tilde{\mathcal{O}}(\log\log nk/\varepsilon)$	Measurable
State k-designs	Circuit depth	Ancilla count	Error
Random phase state [19, 43]	$\mathcal{O}(\log k \cdot \log n)$	$kn \cdot \tilde{\mathcal{O}}(\log n)$	Additive
Blocked random phase state *(this work)*	$\mathcal{O}(\log k \cdot \log\log nk/\varepsilon)$	$kn \cdot \tilde{\mathcal{O}}(\log\log n/\varepsilon)$	Additive
	$\mathcal{O}(k \cdot \log\log nk/\varepsilon)$	$n \cdot \tilde{\mathcal{O}}(\log\log nk/\varepsilon)$	Additive
Lower bound *(this work)*	$\Omega(\log k + \log\log n/\varepsilon)$	Any	Additive
	$\Omega(k + \log\log n/\varepsilon)$	$\mathcal{O}(n)$	Additive

TABLE I. Comparison of the circuit depth and ancilla count of several known constructions of designs. The Permutation-Function-Clifford (PFC) ensemble and random phase state have fixed approximation error $\varepsilon = \mathcal{O}(k^2/2^n)$. The PFC and blocked LRFC circuits can be improved to relative error at the cost of an additional factor of k in the circuit depth [35, 44].

we introduce our new random unitary ensemble and prove that it forms a design in the ultra-low circuit depths described above. We also provide a streamlined construction of low-depth state designs. Second, we introduce a new notion of approximation error for unitary k-designs that captures the strongest experimentally-achievable distinguishability. This *measurable error* quantifies how well a unitary ensemble can be distinguished from Haar-random by any quantum experiment that makes k queries to the unitary. Our results hold under this strong form of approximation error [45]. Third, we prove a complementary lower bound, showing that unitary designs, with any reasonable notion of error, require circuit depth at least $\Omega(\log k + \log\log n/\varepsilon)$. To establish this bound, we provide a simple and efficient test that can distinguish any lower-depth quantum state or unitary from Haar-random. Fourth, a core technical contribution of our work is the development of a new analytic approach for proving that random unitary ensembles are indistinguishable from Haar-random. To demonstrate the versatility of our approach, we apply it to give a succinct alternative proof of the existence of pseudorandom unitaries (following recent work by Ma and Huang [37]). We anticipate that this analytical framework will facilitate continued developments in the field.

Background.—We begin with a short review of state and unitary designs. A random state ensemble $\mathcal{S}$ is a state k-design with additive error ε if its k-th moment,

$$\chi_{\mathcal{S}} \equiv \mathop{\mathbb{E}}_{\psi\in\mathcal{S}} \left[|\psi\rangle\langle\psi|^{\otimes k} \right], \tag{1}$$

is equal to the k-th moment χ_H of the Haar ensemble on the unit sphere of $\mathbb{C}^{2^n}$ up to small trace-norm error, $\|\chi_{\mathcal{S}} - \chi_H\|_1 \leq \varepsilon$. This trace norm condition ensures that $\mathcal{S}$ is indistinguishable from Haar-random in any experiment that queries a random state k times.

A random unitary ensemble $\mathcal{E}$ is a unitary k-design with additive error ε if its k-th moment, i.e. the channel

$$\Phi_{\mathcal{E}}(\cdot) \equiv \mathop{\mathbb{E}}_{U\in\mathcal{E}} \left[U^{\otimes k}(\cdot)U^{\dagger,\otimes k} \right], \tag{2}$$

is equal to the k-th moment Φ_H of the Haar ensemble on $U(2^n)$ up to small diamond-norm error, $\|\Phi_{\mathcal{E}} - \Phi_H\|_\diamond \equiv \max_\rho \|\Phi_{\mathcal{E}}(\rho) - \Phi_H(\rho)\|_1 \leq \varepsilon$. Here, ρ could be supported on a larger system containing both the n qubits and an arbitrary number of ancilla qubits. As mentioned earlier, our unitary design results in fact hold under a much stronger notion of approximation error, the measurable error, which captures the maximum distinguishability achievable by any experiment making k queries to U. We defer a formal definition to the technical sections below.

At present, the best-scaling constructions of state and unitary k-designs are one-dimensional random circuits. Recent works have established that such circuits, in which each gate is drawn independently and randomly from the two-qubit unitary group, create designs in depth $\mathcal{O}(k \cdot \text{poly} \log k \cdot \log(n/\varepsilon))$ [32, 34, 39]. Two key challenges have prevented improvements over this scaling, even when allowing long-range two-qubit gates. First, standard methods to amplify designs [32] decrease the design error exponentially in the circuit depth; achieving a sub-logarithmic depth scaling is thus difficult. Second, the dependencies $\Omega(k)$ and $\Omega(\log n/\varepsilon)$ *are* in fact optimal for random circuits [32, 46, 47], whose lack of structure prevents faster design formation. Hence, any further improvements in design depths must involve highly-structured ensembles.

Nearly optimal state designs.—We now introduce our construction of state designs. Our construction utilizes a binary phase state, $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle$. When $f : \{0,1\}^n \to \{0,1\}$ is a random function, the

phase state forms a k-design with exponentially small additive error, $k^2/2^n$ [43]. However, this state has very high circuit depth, since a random function on n qubits requires exponentially many gates to compute.

To design a more resource-efficient state ensemble, we make two modifications. First, and most crucially, we introduce a blocked variant of the random phase state [Fig. 1(a)]. Blocks of random phase gates are applied to an initial product state using a two-layer brickwork structure. Each block acts on a local patch of 2ξ qubits as $F_i = \sum_{x_i \in \{0,1\}^{2\xi}} (-1)^{f_i(x_i)} |x_i\rangle\langle x_i|$. Blocks in the first and second layer overlap on ξ qubits each. We prove that this blocked random phase state forms a state k-design with additive error $\varepsilon = nk^2/2^\xi$. Hence, the size of each local patch scales only logarithmically in all three parameters, $\xi = \log_2(nk^2/\varepsilon)$.

Second, following earlier works [35, 43], we replace each random function $f_i(x_i)$ with a *$2k$-wise independent random hash function* [48] on 2ξ bits. By definition, a $2k$-wise independent hash function reproduces the $2k$-th moment of a random function. Hence, the resulting $2k$-wise blocked random phase state achieves a state k-design with the same error as before. The factor of two accounts for each function appearing in both the bra and the ket [49].

To implement each $2k$-wise random function, we borrow a standard construction from the classical literature [43, 48]. Namely, we define $f_i(x_i) = \sum_{j=0}^{k-1} \alpha_j (x_i)^j$ where $\alpha_j \in \mathrm{GF}(2^{2\xi})$ are randomly drawn from the Galois field of dimension $2^{2\xi}$. Each bitstring x_i is uniquely associated with an element of the Galois field $\mathrm{GF}(2^{2\xi})$. All arithmetic operations occur within the field $\mathrm{GF}(2^{2\xi})$. In the supplemental material [44], we provide a detailed accounting showing that such functions can be computed in quantum circuit depth $\mathcal{O}(\log k \cdot \log \xi)$ using $\mathcal{O}(\xi k \log \xi \log\log \xi)$ ancilla qubits, and depth $\mathcal{O}(k \cdot \log \xi)$ using $\mathcal{O}(\xi \log \xi \log\log \xi)$ ancilla qubits. From this construction, we immediately achieve state k-designs in quantum circuit depth $\mathcal{O}(\log k \cdot \log\log nk/\varepsilon)$ with $nk \cdot \tilde{\mathcal{O}}(\log\log nk/\varepsilon)$ ancilla qubits, and depth $\mathcal{O}(k \cdot \log\log nk/\varepsilon)$ using $n \cdot \tilde{\mathcal{O}}(\log\log nk/\varepsilon)$ ancilla qubits.

Our proof that the blocked random phase state forms a state k-design proceeds via a surprisingly simple argument [Fig. 2(a-b)]. We consider k copies of the state, decomposed in the computational basis $x^{(1)}, x^{(2)}, \ldots, x^{(k)}$ on each copy. We then project onto a subspace where the local bitstrings x_i at each patch are distinct across the k copies, i.e. $x_i^{(j)} \neq x_i^{(j')}$ for all patches i and copies $j \neq j'$. This projection incurs only a small trace-norm error, since the original state is a superposition over all bitstrings, and most bitstrings are locally distinct. Finally, we show that *on* the local distinct subspace, the two-layer blocked structure $\prod_i F_i$ acts identically to a global random phase operator F, which in turn acts identically to the Haar twirl. These equivalences follow from straightforward computations.

Nearly optimal unitary designs.—To construct low-depth random unitary designs, we combine the two-layer brickwork structure consisting of blocks of random phase gates with several new ingredients. These new ingredients are necessary because a quantum experiment can apply a unitary to any initial state, including those outside the local distinct subspace.

Our unitary ensemble is inspired by the Luby-Rackoff-Function-Clifford (LRFC) ensemble, $U = S_L S_R F C$, introduced in [50]. Here, S_L randomly shuffles the left $n/2$ qubits based on the right $n/2$ qubits, $S_L |x_L, x_R\rangle = |x_L + h_L(x_R), x_R\rangle$, where $h_L : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ is a random function. S_R is the analogous operation for shuffling the right $n/2$ qubits, F is a random phase unitary on all n qubits, and C is a random Clifford unitary. The LRFC ensemble forms a unitary design with an exponentially small additive error, $6k^2/2^{n/2}$ [50].

Before presenting our simplest and most resource-efficient unitary ensemble, let us first describe an alternative approach. Consider a two-layer blocked circuit similar to Fig. 1, but where each block of gates is a random LRFC circuit on 2ξ qubits. We know that the LRFC ensemble forms a design with additive error $6k^2/2^\xi$ [50]. Hence, the two-layer blocked circuit consisting of small LRFC circuits is indistinguishable from a two-layer blocked circuit consisting of small Haar-random unitaries. From the gluing lemma of [39], the two-layer Haar-random blocked circuit forms a unitary design with error $nk^2/2^\xi$. The shuffle operations S_L, S_R and phase unitary F can be implemented in short depth using $2k$-wise independent functions [44, 48]. The random Clifford C can be replaced with an exact unitary 2-design, with circuit depth $\mathcal{O}(\log \xi)$ and ancilla count $\tilde{\mathcal{O}}(\xi)$ [51]. Together, this yields a unitary design with circuit depth $\mathcal{O}(\log k \log\log nk/\varepsilon)$ and ancilla count $nk \cdot \tilde{\mathcal{O}}(\log\log nk/\varepsilon)$.

We can further simplify this unitary ensemble via the construction in Fig. 1(b). We consider the circuit, $U = S_o(\prod_i F_i) S_e C_o$, where S_o is a tensor product of random shuffles of odd patches conditional on even patches, $\prod_i F_i$ is our two-layer blocked random phase circuit, S_e shuffles even patches conditional on odd patches, and C_o is a tensor product of random Clifford unitaries on each odd patch. This *blocked LRFC ensemble* requires fewer shuffle operations, and both fewer and smaller Clifford unitaries, compared to the two-layer blocked LRFC circuit. Its simplicity will also enable a stand-alone design proof, independent of previous results. As before, the ensemble has circuit depth $\mathcal{O}(\log k \log\log nk/\varepsilon)$ and ancilla count $\tilde{\mathcal{O}}(nk)$, or depth $\mathcal{O}(k \log\log nk/\varepsilon)$ and ancilla count $\tilde{\mathcal{O}}(n)$. It uses $3nk + 5n/2$ bits of randomness [44], which is near the optimal value of $2nk$ [29, 52].

Measurable error of unitary designs.—Before describing our proof of unitary designs, let us briefly digress to discuss notions of approximation error in the design lit-

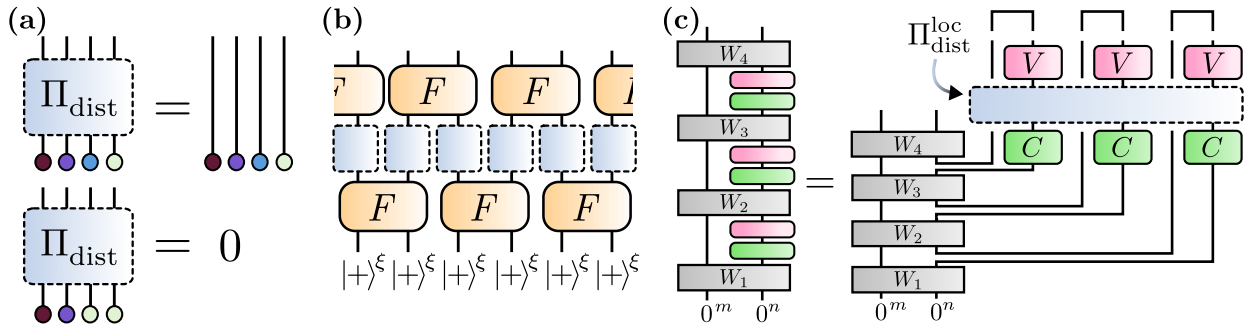

FIG. 2. Illustration of key ideas from our design proofs. **(a)** The distinct subspace projector [35] Π_{dist} eliminates bitstrings that are equal on different copies of the state or unitary (bottom), while leaving "distinct" sets of bitstrings invariant (top). Here, each leg represents one of k copies, and the colored circles indicate the n-bit string $x^{(j)}$ of a computational basis state on each copy ($j = 1, \ldots, k$). **(b)** To prove that the blocked random phase state is a state k-design, we insert projectors onto the local distinct subspace between each random phase gate. On the local distinct subspace, the blocked random phase circuit acts identically to a Haar-random unitary, which completes the proof. **(c)** To prove that the blocked LRFC circuit forms a unitary k-design with small measurable error, we reformulate any quantum experiment involving sequential applications of a unitary $U = VC$ (with $V \equiv S_o \prod_i F_i$ and $C \equiv S_e C_o$ for the blocked LRFC circuit) into an equivalent experiment involving parallel applications and post-selection on EPR states (top bars). We then insert projectors onto the local distinct subspace, $\Pi^{\text{loc}}_{\text{dist}}$, between V and C in the parallel applications. On the local distinct subspace, the blocked LRFC circuit acts identically to a Haar-random unitary, which completes the proof.

erature. Unfortunately, the additive error for unitary designs provides only a weak guarantee, that a unitary appears Haar-random in experiments that query it k times in *parallel* [39]. To address this, one common approach uses the so-called *relative error*, $(1-\varepsilon)\Phi_H \preceq \Phi_{\mathcal{E}} \preceq (1+\varepsilon)\Phi_H$, where $\preceq$ denotes the channel inequality [53]. The relative error is remarkably strong: it can bound any property that can be efficiently measured in any experiment, as well as many exponentially small quantities that can never be measured. While this strength can be convenient, it often represents an overly stringent and un-physical requirement. Indeed, recent works have established unitary ensembles that have large relative error, yet cannot be distinguished from Haar-random unitaries by any efficient experiment [37, 50].

To address this, we define a new, natural notion of error for unitary designs: the *measurable error*. A unitary ensemble has small measurable error if it cannot be distinguished from Haar-random by any experiment that queries it k times. To be precise, if we denote the output of a general quantum experiment as $|*\rangle \psi^U_W = W_{k+1} U W_k U \cdots U W_1 |0\rangle$ where W_j are arbitrary quantum operations (involving arbitrary ancilla qubits) applied between successive queries to U [44], then the measurable error demands

$$\left\| \mathop{\mathbb{E}}_{U\sim\mathcal{E}} \left[|\psi^U_W\rangle\langle\psi^U_W| \right] - \mathop{\mathbb{E}}_{U\sim H} \left[|\psi^U_W\rangle\langle\psi^U_W| \right] \right\|_1 \leq \varepsilon \qquad (3)$$

for all W_j. This resembles the notion of adaptive security in the context of PRUs [54]. The measurable error is substantially stronger than the additive error, which only concerns experiments in which $U^{\otimes k}$ is applied once in parallel. Moreover, if a unitary ensemble fails to have small measurable error, there always exists an experiment that can measure that the ensemble is not Haar-random [44].

To prove that the blocked LRFC ensemble forms a unitary design with small measurable error, we develop a new general approach for bounding the measurable error of random unitary ensembles. Our approach combines and refines recent ideas from the study of PRUs. At a high-level, it proceeds in three steps. First, we reformulate any experiment involving sequential applications of a random unitary as an equivalent experiment involving parallel applications and post-selection [see Fig. 2(c)]. Then, we prove that one can insert a projector onto the local distinct subspace between key components of the parallel random unitaries in the post-selected experiment. Finally, we show that the ensemble of interest, i.e. the blocked LRFC ensemble, acts identically to a Haar-random unitary on the local distinct subspace, thereby completing the proof. Following these steps, we prove that the blocked LRFC ensemble has measurable error $\varepsilon = 3(n/\xi)k^2/2^{\xi}$, which leads to the stated depths of our unitary designs.

Minimum depth of designs.—Given rapid recent improvements in design circuit depth, a natural question to ask is: Can one do any better? Unfortunately, while a simple counting argument shows that a circuit depth $\Omega(\log k)$ is indeed optimal [32, 44] (and thus our k-dependence is optimal up to an exponentially smaller $\log\log k$ factor), existing lower bounds leave gaps in the dependence on n and ε. Specifically, lower bounds for n apply only to the relative error, while bounds for ε apply only to unitaries and not states [39].

Here, we resolve this by introducing a simple and efficient test to distinguish any sufficiently low-depth quan-

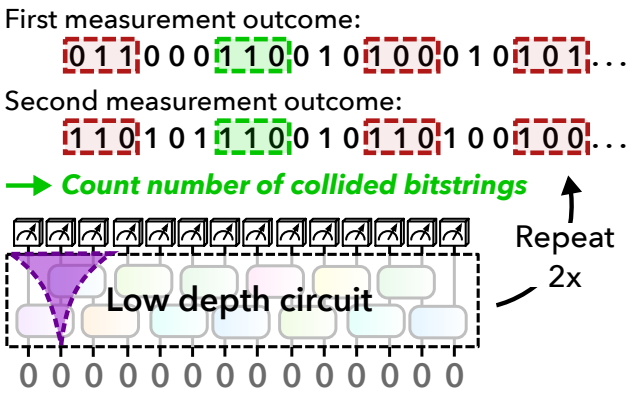

FIG. 3. Illustration of our lower bound on state and unitary designs. We consider the output distribution when the state of interest is measured in a random product basis. We show that with two measurements, one can efficiently distinguish any state with circuit depth less than $\log\log n/\varepsilon$ from Haar-random, by counting local collisions (green) in the measurement outcomes. The collisions are considered on regions (red/green) of the same size as the circuit light-cone (purple).

tum state from Haar-random. Our test implies that n-qubit state and unitary designs with additive error ε require circuit depth $\Omega(\log\log n/\varepsilon)$, as we achieve. Our test proceeds as follows: We choose a random product basis, and measure two identical copies of the state of interest in the chosen basis. We then divide the measurement outcomes, represented as n-bit strings, into local patches of $\sim L$ bits each, where L is the size of the light-cone of the state preparation circuit. Then, we count the number of patches where the two measurement outcomes are equal (i.e. collide). We prove that for any low-depth state, the number of collisions is high, whereas in a Haar-random state it is very low. A detailed analysis yields the precise scaling with n and ε [44].

Physically, our test builds upon the intuition from [39] that large numbers of non-commuting observables are essential for quantum circuits to appear random. We show that for circuits of insufficient depth, an extensive number of observables both have high expectation value in the state, and commute with the random product measurement. This causes the measurement distribution to retain large amounts of information about the state. This manifests in some local bitstrings appearing (and hence, colliding) more often than others.

Application to pseudorandom unitaries.—Finally, although our work focuses primarily on unitary designs, the techniques we develop also have immediate applications to the study of PRUs. A PRU is any efficient unitary ensemble indistinguishable from Haar-random unitaries in all computationally-bounded quantum experiments [19]. The standard approach to proving the security of PRUs involves, as an intermediary step, proving that a more-random version of the ensemble is a design with small measurable error [35, 37, 43, 50].

Thus far, the only existing method for proving the security of PRUs is the path-recording framework proposed in [37], which relies on analyzing sums of computational paths through computational basis states. Our proof that our unitary ensemble [Fig. 1(b)] has small measurable error introduces a new methodology that complements existing techniques. To illustrate the versatility of our approach, we apply it in the supplemental material [44] to give two short and self-contained proofs that the PFC [35, 37] and LRFC [50] ensembles form PRUs.

Outlook.—Our work comes near to closing a long line of research on the circuit depths of random unitary designs. Nonetheless, several questions remain open. First, constructing truly optimal designs, which requires decoupling the $\log(k)$ and $\log\log(n/\varepsilon)$ dependences, remains open. Second, applications of k-designs with $k > 3$ remain comparatively sparse. One theoretical application concerns the growth of quantum circuit complexity [32, 34]; here, our results prove that the complexity of unitaries without ancilla qubits can grow exponentially in the depth of the unitary with ancilla qubits [55]. A second application involves using higher-order designs to lower bound the probability that individual random unitaries will mimic lower-order average behavior [39, 56]. Finally, while our construction of unitary k-designs is nearly optimal in terms of scaling, it is not readily implementable on near-term quantum computing architectures. The development of practical implementations of unitary and state designs remains an important open direction.

Acknowledgements—We are tremendously grateful to Gregory D. Kahanamoku-Meyer for several discussions on the resource requirements for quantum arithmetic. T.S. acknowledges support from the Walter Burke Institute for Theoretical Physics at Caltech. T.S. and H.H. acknowledge support from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator. The Institute for Quantum Information and Matter is an NSF Physics Frontiers Center.

---

* These authors contributed equally to this work.

[1] M. P. Fisher, V. Khemani, A. Nahum, and S. Vijay, Random quantum circuits, Annual Review of Condensed Matter Physics **14**, 335 (2023).
[2] A. Nahum, J. Ruhman, S. Vijay, and J. Haah, Quantum Entanglement Growth Under Random Unitary Dynamics, Phys. Rev. X **7**, 031016 (2017), arXiv:1608.06950 [cond-mat.stat-mech].
[3] J. Cotler, N. Hunter-Jones, and D. Ranard, Fluctuations of subsystem entropies at late times, Physical Review A **105**, 022416 (2022).
[4] Y. Sekino and L. Susskind, Fast scramblers, Journal of High Energy Physics **2008**, 065 (2008).
[5] P. Hayden and J. Preskill, Black holes as mirrors: quan-

tum information in random subsystems, JHEP **2007** (09), 120.
[6] A. R. Brown, H. Gharibyan, S. Leichenauer, H. W. Lin, S. Nezami, G. Salton, L. Susskind, B. Swingle, and M. Walter, Quantum gravity in the lab. i. teleportation by size and traversable wormholes, PRX quantum **4**, 010320 (2023).
[7] J. M. Deutsch, Quantum statistical mechanics in a closed system, Phys. Rev. A **43**, 2046 (1991).
[8] M. Srednicki, Chaos and quantum thermalization, Phys. Rev. E **50**, 888 (1994), arXiv:cond-mat/9403051.
[9] M. Rigol, V. Dunjko, and M. Olshanii, Thermalization and its mechanism for generic isolated quantum systems, Nature **452**, 854 (2008).
[10] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, Journal of Optics B: Quantum and Semiclassical Optics **7**, S347 (2005).
[11] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Randomized benchmarking of quantum gates, Physical Review A **77**, 012307 (2008).
[12] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, The randomized measurement toolbox, Nature Reviews Physics **5**, 9 (2023).
[13] M. Guţă, J. Kahn, R. Kueng, and J. A. Tropp, Fast state tomography with optimal error bounds, Journal of Physics A: Mathematical and Theoretical **53**, 204001 (2020).
[14] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, Nature Physics **16**, 1050 (2020).
[15] A. Zhao, N. C. Rubin, and A. Miyake, Fermionic partial tomography via classical shadows, Physical Review Letters **127**, 110504 (2021).
[16] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, Quantum supremacy using a programmable superconducting processor, Nature **574**, 505 (2019).
[17] A. Morvan, B. Villalonga, X. Mi, S. Mandra, A. Bengtsson, P. Klimov, Z. Chen, S. Hong, C. Erickson, I. Drozdov, *et al.*, Phase transition in random circuit sampling, arXiv preprint arXiv:2304.11119 (2023).
[18] D. A. Abanin, R. Acharya, L. Aghababaie-Beni, G. Aigeldinger, A. Ajoy, R. Alcaraz, I. Aleiner, T. I. Andersen, M. Ansmann, F. Arute, *et al.*, Constructive interference at the edge of quantum ergodic dynamics, arXiv preprint arXiv:2506.10191 (2025).
[19] Z. Ji, Y.-K. Liu, and F. Song, Pseudorandom quantum states, in *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38* (Springer, 2018) pp. 126–152.
[20] P. Ananth, L. Qian, and H. Yuen, Cryptography from pseudorandom quantum states, in *Annual International Cryptology Conference* (Springer, 2022) pp. 208–236.
[21] W. Kretschmer, L. Qian, M. Sinha, and A. Tal, Quantum cryptography in algorithmica, in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing* (2023) pp. 1589–1602.
[22] D. Weingarten, Asymptotic behavior of group integrals in the limit of infinite rank, Journal of Mathematical Physics **19**, 999 (1978).
[23] B. Collins, Moments and cumulants of polynomial random variables on unitarygroups, the itzykson-zuber integral, and free probability, International Mathematics Research Notices **2003**, 953 (2003).
[24] B. Collins and P. Śniady, Integration with respect to the haar measure on unitary, orthogonal and symplectic group, Communications in Mathematical Physics **264**, 773 (2006).
[25] M. L. Mehta, *Random Matrices*, 3rd ed., Pure and Applied Mathematics, Vol. 142 (Academic Press, San Diego, 2004).
[26] T. Tao, *Topics in Random Matrix Theory*, Graduate Studies in Mathematics, Vol. 132 (American Mathematical Society, 2012).
[27] G. W. Anderson, A. Guionnet, and O. Zeitouni, *An Introduction to Random Matrices*, Cambridge Studies in Advanced Mathematics (Cambridge University Press, 2009).
[28] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, Pseudo-random unitary operators for quantum information processing, science **302**, 2098 (2003).
[29] D. Gross, K. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, Journal of mathematical physics **48** (2007).
[30] C. Dankert, Efficient simulation of random quantum states and operators, arXiv preprint quant-ph/0512217 (2005).
[31] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Exact and approximate unitary 2-designs and their application to fidelity estimation, Physical Review A **80**, 012304 (2009).
[32] F. G. Brandao, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, Communications in Mathematical Physics **346**, 397 (2016).
[33] J. Haah, Y. Liu, and X. Tan, Efficient approximate unitary designs from random pauli rotations, arXiv preprint arXiv:2402.05239 (2024).
[34] C.-F. Chen, J. Haah, J. Haferkamp, Y. Liu, T. Metger, and X. Tan, Incompressibility and spectral gaps of random circuits, arXiv preprint arXiv:2406.07478 (2024).
[35] T. Metger, A. Poremba, M. Sinha, and H. Yuen, Simple constructions of linear-depth t-designs and pseudorandom unitaries, arXiv preprint arXiv:2404.12647 (2024).
[36] C.-F. Chen, A. Bouland, F. G. Brandão, J. Docter, P. Hayden, and M. Xu, Efficient unitary designs and pseudorandom unitaries from permutations, arXiv preprint arXiv:2404.16751 (2024).
[37] F. Ma and H.-Y. Huang, How to construct random unitaries, arXiv preprint arXiv:2410.10116 (2024).
[38] N. LaRacuente and F. Leditzky, Approximate unitary k-designs from shallow, low-communication circuits, arXiv preprint arXiv:2407.07876 (2024).
[39] T. Schuster, J. Haferkamp, and H.-Y. Huang, Random unitaries in extremely low depth, Science **389**, 92 (2025).
[40] D. Bluvstein, S. J. Evered, A. A. Geim, S. H. Li, H. Zhou, T. Manovitz, S. Ebadi, M. Cain, M. Kalinowski, D. Hangleiter, *et al.*, Logical quantum processor based on reconfigurable atom arrays, Nature **626**, 58 (2024).
[41] M. Iqbal, N. Tantivasadakarn, R. Verresen, S. L. Campbell, J. M. Dreiling, C. Figgatt, J. P. Gaebler, J. Johansen, M. Mills, S. A. Moses, *et al.*, Non-abelian topological order and anyons on a trapped-ion processor, Nature **626**, 505 (2024).

[42] S. Slussarenko and G. J. Pryde, Photonic quantum information processing: A concise review, Applied physics reviews **6** (2019).

[43] Z. Brakerski and O. Shmueli, (pseudo) random quantum states with binary phase, in *Theory of Cryptography Conference* (Springer, 2019) pp. 229–250.

[44] See Supplemental Material for additional details.

[45] The expert reader may recall an even stronger notion of approximation error in the design literature, the *relative error*. Our designs achieve relative error at the cost of an additional factor of k in the circuit depth (Table I). As discussed later in the main text, the relative error cannot be measured in any (sub-exponential-time) quantum experiment [44].

[46] D. Aharonov, X. Gao, Z. Landau, Y. Liu, and U. Vazirani, A polynomial-time classical algorithm for noisy random circuit sampling, in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing* (2023) pp. 945–957.

[47] B. Fefferman, S. Ghosh, and W. Zhan, Anti-concentration for the unitary haar measure and applications to random quantum circuits, arXiv preprint arXiv:2407.19561 (2024).

[48] M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set equality, Journal of computer and system sciences **22**, 265 (1981).

[49] M. Zhandry, How to construct quantum random functions, J. ACM **68**, 10.1145/3450745 (2021).

[50] T. Schuster, F. Ma, F. Brandão, and H.-Y. Huang, Strong random unitaries and fast scrambling, Forthcoming (2025).

[51] R. Cleve, D. Leung, L. Liu, and C. Wang, Near-linear constructions of exact unitary 2-designs, arXiv preprint arXiv:1501.04592 (2015).

[52] A. Roy and A. J. Scott, Unitary designs and codes, Designs, codes and cryptography **53**, 13 (2009).

[53] Here, $\Phi \preceq \Phi'$ indicates that $\mathrm{tr}(M\Phi(\rho)) \leq \mathrm{tr}(M\Phi'(\rho))$ for all positive operators ρ and M.

[54] We remark that the adjectives "adaptive" and "non-adaptive" do not perfectly capture the distinction between experiments that query a unitary in parallel versus general experiments. For example, an experiment could query a unitary on many copies in parallel and then perform adaptive measurements on the many copies.

[55] X. Sun, G. Tian, S. Yang, P. Yuan, and S. Zhang, Asymptotically optimal circuit depth for quantum state preparation and general unitary synthesis, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **42**, 3301 (2023).

[56] A. Nietner, M. Ioannou, R. Sweke, R. Kueng, J. Eisert, M. Hinsche, and J. Haferkamp, On the average-case complexity of learning output distributions of quantum circuits, arXiv preprint arXiv:2305.05765 (2023).

[57] A. W. Harrow, The church of the symmetric subspace, arXiv:1308.6595 (2013).

[58] W. Fulton and J. Harris, *Representation theory: a first course*, Vol. 129 (Springer Science & Business Media, 2013).

[59] R. Goodman, N. R. Wallach, *et al.*, *Symmetry, representations, and invariants*, Vol. 255 (Springer, 2009).

[60] S. Aaronson, BQP and the polynomial hierarchy, in *Proceedings of the forty-second ACM symposium on Theory of computing* (2010) pp. 141–150.

[61] J. S. Cotler, D. K. Mark, H.-Y. Huang, F. Hernandez, J. Choi, A. L. Shaw, M. Endres, and S. Choi, Emergent quantum state designs from individual many-body wavefunctions, arXiv:2103.03536 (2021).

[62] J. Choi, A. L. Shaw, I. S. Madjarov, X. Xie, R. Finkelstein, J. P. Covey, J. S. Cotler, D. K. Mark, H.-Y. Huang, A. Kale, *et al.*, Preparing random states and benchmarking with many-body quantum chaos, Nature **613**, 468 (2023).

[63] H. Zhu, Multiqubit clifford groups are unitary 3-designs, Physical Review A **96**, 062336 (2017).

[64] C. Moore and M. Nilsson, Parallel quantum computation and quantum codes, SIAM journal on computing **31**, 799 (2001).

[65] J. Jiang, X. Sun, S.-H. Teng, B. Wu, K. Wu, and J. Zhang, Optimal space-depth trade-off of cnot circuits in quantum logic synthesis, in *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms* (SIAM, 2020) pp. 213–229.

[66] J. Haferkamp, Random quantum circuits are approximate unitary t-designs in depth $O(t^{5+o(1)})$, Quantum **6**, 795 (2022).

[67] J. L. Carter and M. N. Wegman, Universal classes of hash functions, in *Proceedings of the ninth annual ACM symposium on Theory of computing* (1977) pp. 106–112.

[68] N. Alon, O. Goldreich, J. Håstad, and R. Peralta, Simple constructions of almost k-wise independent random variables, Random Structures & Algorithms **3**, 289 (1992).

[69] J. Von Zur Gathen and J. Gerhard, *Modern computer algebra* (Cambridge university press, 2003).

[70] W. Eberly, Very fast parallel matrix and polynomial arithmetic, in *25th Annual Symposium onFoundations of Computer Science, 1984.* (IEEE, 1984) pp. 21–30.

[71] A. Schonhage, Schnelle multiplikation grosser zahlen, Computing **7**, 281 (1971).

[72] P. Barrett, Implementing the rivest shamir and adleman public key encryption algorithm on a standard digital signal processor, in *Conference on the Theory and Application of Cryptographic Techniques* (Springer, 1986) pp. 311–323.

[73] One can also write $\chi_H = P_{\mathrm{sym}}/D_{\mathrm{sym}}$ where $P_{\mathrm{sym}} = \frac{1}{k!}\sum_\pi \pi$ is the projector onto the symmetric subspace and $D_{\mathrm{sym}} = \binom{2^n+k-1}{2^n-1}$ is the symmetric subspace dimension [57].

[74] Here, $\pi x \equiv (x^{(\pi(1))}, x^{(\pi(2))}, \ldots, x^{(\pi(k))})$ denotes the permutation of the length-k list x by π.

[75] T. Giurgica-Tiron and A. Bouland, Pseudorandomness from subset states, arXiv preprint arXiv:2312.09206 (2023).

[76] F. G. Jeronimo, N. Magrafta, and P. Wu, Pseudorandom and pseudoentangled states from subset states, arXiv preprint arXiv:2312.15285 (2023).

[77] M. Zhandry, A note on quantum-secure prps, arXiv preprint arXiv:1611.05564 (2016).

[78] T. Schuster, M. Niu, J. Cotler, T. O'Brien, J. R. McClean, and M. Mohseni, Learning quantum systems via out-of-time-order correlators, Physical Review Research **5**, 043284 (2023).

[79] J. Cotler, T. Schuster, and M. Mohseni, Information-theoretic hardness of out-of-time-order correlators, Physical Review A **108**, 062608 (2023).

[80] The lower bound follows because random circuits require at least logarithmic depth to anti-concentrate [46]. Anti-concentration is necessary in order to form a design with

small relative error. We expect that this lower bound can be extended to apply to additive error designs using the techniques we introduce in the proof of Theorem 10.

[81] R. O'Donnell and J. Wright, Learning and testing quantum states via probabilistic combinatorics and representation theory, Curr. Dev. Math , 43 (2021).

Supplementary Material: Unitary designs in nearly optimal depth

CONTENTS

I. PRELIMINARIES

In this section, we establish the foundational concepts necessary for our analysis of designs and their distinguishability properties. We begin by reviewing the mathematical framework for averaging over the unitary group via the Haar measure, then proceed to define state and unitary designs with their respective error measures.

A. Haar averaging over the unitary group

We first review properties of the moments of Haar-random unitaries, which serve as the reference point against which we compare other unitary ensembles. Let $|x\rangle$ denote a computational basis state on a system of n qubits corresponding to the bitstring $x \in \{0,1\}^n$. The Haar measure provides the unique translation-invariant measure on the unitary group, defining a uniform distribution over all unitaries on n qubits.

Definition 1 (Averaging over the unitary group)**.** *Given a linear operator X acting on nk qubits, the k-th moment with respect to $U(2^n)$ is defined via the twirl over the unitary group:*

$$\Phi_H(X) = \int dU\, U^{\otimes k} X (U^\dagger)^{\otimes k}, \tag{4}$$

where we have left out the implicit dependence on k.

This definition captures how the operator X transforms when we apply k independent copies of a Haar-random unitary U. While individual Haar-random unitaries have no predictable structure, their statistical moments possess well-defined mathematical properties that can be characterized precisely.

The structure of these moments can be determined using representation theory. The key observation is that these moments must be invariant under any unitary change of basis applied to each copy separately. By applying Schur-Weyl duality [58, 59], this symmetry constraint determines the form of the moments:

Lemma 1 (Explicit form in terms of permutations)**.** *For any linear operator X acting on nk qubits, the k-th moment with respect to the unitary group can be written in the form*

$$\Phi_H(X) = \sum_{\sigma,\tau \in S_k} c_{\sigma,\tau} \cdot \mathrm{tr}(\sigma X) \cdot \tau. \tag{5}$$

The coefficients $c_{\sigma,\tau}$ depend on k and the Hilbert space dimension 2^n.

In principle, all of the coefficients $c_{\sigma,\tau}$ can be computed exactly using combinatorial formulas derived from the Weingarten calculus of the unitary group [24]. However, the main property of the moments that we will use in the following sections is their relationship to the symmetric group on k copies of the physical systems.

B. State k-designs

We now turn to state ensembles and their ability to mimic the statistical properties of Haar-random states under measurements on multiple copies. State designs provide a framework for constructing explicit state ensembles that approximate the behavior of Haar-random states for experiments involving a bounded number of copies. For quantum states, the approximation is typically characterized using trace distance $\|\cdot\|_1$.

Definition 2 (State k-design)**.** *An ensemble of states $\mathcal{S}$ is an ε-approximate quantum state k-design if it reproduces the twirl of the unitary group on k copies of any state on n qubits up to additive error ε, or equivalently,*

$$\|\chi_{\mathcal{S}} - \chi_H\|_1 \leq \varepsilon. \tag{6}$$

where we have used the abbreviated notation

$$\chi_{\mathcal{S}} = \mathop{\mathbb{E}}_{|\phi\rangle \sim \mathcal{S}} (|\phi\rangle\langle\phi|)^{\otimes k} \tag{7}$$

to denote the k-th moment over the state ensemble S.

This definition characterizes when an ensemble $\mathcal{S}$ cannot be distinguished from Haar-random states by any measurement performed on k copies of a random state. The moments of Haar-random states are maximally mixed over the symmetric subspace on the k copies [57].

1. Example: Binary phase state

To illustrate the construction of state designs, we review binary phase state ensembles, first introduced in [19] with statistical properties analyzed in [43]. These provide a concrete construction of pseudorandom quantum states using classical Boolean functions.

Definition 3 (Random binary phase state)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a uniformly random Boolean function. The corresponding* random binary phase state *on n qubits is defined as*

$$|\phi_f\rangle = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle . \tag{8}$$

The construction begins with the uniform superposition state and applies random phase factors determined by the Boolean function f.

Lemma 2 (Binary phase states are designs [43])**.** *The ensemble of random binary phase states from Definition 3 forms an ε-approximate state k-design with $\varepsilon = 4k^2/2^n$.*

C. Unitary k-designs

We now establish the framework for unitary designs, which are ensembles of unitary transformations that approximately reproduce the statistics of Haar-random unitaries. Unlike state designs, unitary designs concern dynamical processes that can be applied to arbitrary input states and must withstand more sophisticated experimental probes.

1. Additive Error and Parallel Security

The most commonly studied error measure is additive error, which is based on the differences between the moments in diamond norm. Recall that diamond distance concerns the maximum trace distance on the output states for any input states of a much bigger system size.

Definition 4 (Unitary k-design up to additive error)**.** *An ensemble of unitaries $\mathcal{E}$ is a* unitary k-design *if it reproduces the first k moments of the Haar measure. In addition, given some $\varepsilon > 0$, the ensemble $\mathcal{E}$ is an approximate unitary k-design up to* additive error ε *if*

$$\|\Phi_{\mathcal{E}} - \Phi_H\|_\diamond \leq \varepsilon, \tag{9}$$

where we have used the abbreviated notation

$$\Phi_{\mathcal{E}}(X) = \mathop{\mathbb{E}}_{U\sim\mathcal{E}} U^{\otimes k} X (U^\dagger)^{\otimes k} \tag{10}$$

to denote the k-th moment over the unitary ensemble $\mathcal{E}$.

Explicitly, the diamond norm is given by $\|\Phi - \Phi'\|_\diamond = \max_\rho \|\Phi(\rho) - \Phi'(\rho)\|_1$, where the maximization is over all states ρ on $nk + m$ qubits, where the number m of ancilla qubits may be arbitrarily large.

The diamond norm measures the maximum distinguishability of two quantum channels. The channels $\Phi_{\mathcal{E}}$ and Φ_H apply k copies of a random unitary U in parallel. It follows that the additive error measures the maximum distinguishability of the ensemble $\mathcal{E}$ and the Haar-ensemble in any quantum experiment that queries k copies of the unitary U in parallel.

Lemma 3 (Additive error is equivalent to parallel security)**.** *An ensemble $\mathcal{E}$ is an approximate unitary k-design up to additive error ε if and only if for any quantum algorithm making a single query to $U^{\otimes k}$, i.e. k parallel queries to U, the output states when U is sampled from $\mathcal{E}$ versus the Haar ensemble are ε-close in trace distance.*

2. Measurable Error and Adaptive Security

It is widely known in quantum complexity theory and quantum cryptography [35, 37] that indistinguishability under one query to $U^{\otimes k}$, i.e., k parallel queries to U, does not imply indistinguishability under general quantum experiments that can query k copies of U. A quantum experiment making k queries to U can apply the unitary in sequence and with arbitrary quantum operations in between each query. This is much more powerful as it enables the quantum experiment to learn some properties about U, then adaptively probe the unitary U based on the properties it has learned. The general formulation of any quantum experiment that makes k queries to U is written as follows.

Definition 5 (Quantum experiments with k queries to U)**.** *A quantum experiment with k queries consists of:*

1. *An initial state preparation $|\psi_0\rangle$ on registers $A \otimes A'$, where A has dimension 2^n and A' is an auxiliary register of dimension 2^m. Without loss of generality, we can set $|\psi_0\rangle = |0^n\rangle \otimes |0^m\rangle$.*
2. *For $i = 1, \ldots, k$:*
   - *Apply a unitary W_i to registers $A \otimes A'$.*
   - *Apply the unknown unitary U to register A.*
3. *Apply a final unitary W_{k+1} and measure to obtain classical outcome.*

To capture indistinguishability under the most powerful quantum experiments that make up to k queries to a unitary U, we consider a strong notion of approximation error: the maximum distinguishability between a random unitary ensemble and the Haar ensemble over all possible k-query quantum experiments. Whenever this error is large, there exists a quantum experiment that can be constructed to distinguish the two ensembles. We therefore refer to this as the *measurable error*. We now state the definition of measurable error formally.

Definition 6 (Unitary k-design up to measurable error)**.** *Let $\varepsilon > 0$. An ensemble of unitaries $\mathcal{E}$ is an approximate unitary k-design up to measurable error ε if for any quantum experiment with k queries to U, the output states when U is sampled from $\mathcal{E}$ versus the Haar ensemble are ε-close in trace distance, i.e.*

$$\sup_{W_1 \cdots W_{k+1}} \|\rho_{\mathcal{E}} - \rho_H\|_1 \leq \varepsilon, \tag{11}$$

where we have used the notation

$$\rho_{\mathcal{E}} = \mathop{\mathbb{E}}_{U \sim \mathcal{E}} \left[W_{k+1}[U \otimes \mathbb{1}_m] W_k \cdots W_2 [U \otimes \mathbb{1}_m] W_1 |0^{n+m}\rangle\langle 0^{n+m}| W_1^\dagger [U^\dagger \otimes \mathbb{1}_m] W_2^\dagger \cdots W_k^\dagger [U^\dagger \otimes \mathbb{1}_m] W_{k+1}^\dagger \right] \tag{12}$$

to denote the expected output state of a general quantum experiment that queries U k times.

3. Relative Error and Output Probabilities

One approach to bounding the distinguishability of two random unitary ensembles under general quantum experiments is to adopt an even more stringent definition of statistical closeness. For instance, we can consider the notion of approximate unitary designs based on relative error as defined in [32]:

Definition 7 (Unitary k-design up to relative error)**.** *Let $\varepsilon > 0$. Then an ensemble of unitaries $\mathcal{E}$ is an approximate unitary k-design up to relative error ε if*

$$(1 - \varepsilon)\Phi_H \preceq \Phi_{\mathcal{E}} \preceq (1 + \varepsilon)\Phi_H, \tag{13}$$

where $\mathcal{A} \preceq \mathcal{B}$ denotes that $\mathcal{B} - \mathcal{A}$ is completely positive.

The relative error can be thought of as a quantum analog of the "almost" k-wise independence condition for classical Boolean functions, which is sufficient to guarantee indistinguishability against a classical adversary [60]. In [39], it is shown that a bounded relative error is a sufficient condition for the indistinguishability of two ensembles under quantum experiments with access to k copies of a random unitary sampled from either ensemble.

Lemma 4 (Relative error implies measurable error [39])**.** *Suppose $\mathcal{E}$ is an approximate k-design up to relative error ε. Then for any quantum experiment with access to k copies of $U \sim \mathcal{E}$, the output states are 2ε-close in trace norm.*

Since measurable error is an upper bound on additive error, relative error serves as an upper bound for additive error as well (up to a constant factor 2). However, the converse is not true. In general, converting from additive to relative error incurs a factor which is exponential in n and k [32, 39]:

Lemma 5 (Comparing additive and relative error [32, 39])**.** *Let $\mathcal{E}$ be a unitary ensemble. If $\mathcal{E}$ is an approximate k-design up to relative error ε, then it is always an approximate design up to additive error $\varepsilon' = 2\varepsilon$. Conversely, if $\mathcal{E}$ is an approximate k-design up to additive error ε, it is guaranteed to be an approximate design up to relative error*

$$\varepsilon' = 2^{nk}\binom{2^n+k-1}{k}\varepsilon \leq \left(\frac{4^{nk}}{k!}\right)\left(1+\frac{k^2}{2^n}\right)\varepsilon, \tag{14}$$

where the first equality holds for any k, and the second inequality for any $k^2 \leq 2^n$.

The bound on the relative error in terms of the additive error [Eq. (14)] follows from Lemma 30 in [32], by replacing the lossy inequality $\binom{N+t-1}{t} \leq N^t$ in the proof of the lemma with either the exact expression, or the tighter inequality $\binom{N+t-1}{t} \leq N^t(1+t^2/N)/t!$ for $t^2 \leq N$ [39]. Here, $t \to k$ and $N \to 2^n$ in our notation.

While the relative error provides the strongest possible theoretical guarantee among the three error metrics, it does not correspond directly to physically observable quantities. Both the additive and measurable error have clear operational interpretations: the additive error quantifies the maximum distinguishability under parallel queries, while the measurable error captures the maximum distinguishability achievable by any quantum experiment. In contrast, the relative error characterizes the multiplicative deviation of the ensemble's moments from the Haar moments, which may not manifest as measurable differences in experiments. When the relative error significantly exceeds the measurable error for a given ensemble, the gap represents a theoretical structure that cannot be exploited by physical experiments. Rather, the relative error serves primarily as a mathematical tool for establishing theoretical properties rather than characterizing experimentally observable behavior.

An important exception is quantum experiments assisted by classical simulations. Classical simulations can enable a quantum experiment to be informed by quantities, such as exponentially small probability amplitudes, that can never be efficiently measured in a quantum experiment alone. This has enabled novel benchmarking and fidelity estimation strategies, such as classical shadow tomography [14], as well as new theoretical understandings of thermalization and chaos in many-body quantum systems via projected ensembles [61, 62]. However, these classical-simulation-assisted quantum experiments require one to be able to exactly simulate the quantum system of interest on a classical computer, including features of the system that would not be detectable in any efficient quantum experiment. Hence, these classical simulations require exponential time in general, but can be polynomial time in some cases, such as when the quantum circuit is Clifford as in classical shadows [14].

The relative error is uniquely suited to these quantum experiments assisted by classical simulations. Most often, the usefulness of relative error stems from its ability to bound exponentially small probability amplitudes. For example, one can bound moments of probabilities, such as

$$(1-\varepsilon)\mathop{\mathbb{E}}_{U\sim H}[\langle x|U\rho U^\dagger|x\rangle^k] \leq \mathop{\mathbb{E}}_{U\sim\mathcal{E}}[\langle x|U\rho U^\dagger|x\rangle^k] \leq (1+\varepsilon)\mathop{\mathbb{E}}_{U\sim H}[\langle x|U\rho U^\dagger|x\rangle^k] \tag{15}$$

for any ρ and k, in any approximate unitary k-design $\mathcal{E}$ with relative error ε. Such bounds are not possible for unitary designs with additive or measurable error, since the probability amplitudes are exponentially small and not physically observable in any quantum experiment that queries U.

In Section V, we demonstrate how repeated composition of designs with small additive error can yield designs with exponentially improved relative error guarantees. Specifically, we show that composing a specific unitary ensemble $p = 8k+1$ times achieves relative error. This provides a systematic approach for constructing relative error designs with only a moderate overhead in circuit depth.

4. Example: Exact unitary 2-designs

The multiqubit Clifford group provides a foundational example of an exact low-order design:

Lemma 6 (Multiqubit Clifford group is an exact 3-design [63])**.** *The multiqubit Clifford group $\mathcal{C}_n$ on n qubits forms an exact unitary 3-design. That is, for any operator X acting on $3n$ qubits,*

$$\Phi^{(3)}_{\mathcal{C}_n}(X) = \Phi^{(3)}_{H}(X), \tag{16}$$

x where $\Phi^{(3)}_{\mathcal{C}_n}(X) = \frac{1}{|\mathcal{C}_n|}\sum_{C\in\mathcal{C}_n} C^{\otimes 3}X(C^\dagger)^{\otimes 3}$.

Any Clifford unitary can be compiled in circuit depth $\mathcal{O}(\log n)$ using $\mathcal{O}(n^2)$ ancilla qubits [64, 65].

For the specific case of $k = 2$, even more resource-efficient constructions of exact designs are known. The ancilla count improves by a nearly quadratic factor compared to a random Clifford unitary.

Fact 1 (Compilation of exact unitary 2-designs [51])**.** *Exact unitary 2-designs on n qubits can be constructed in circuit depth $\mathcal{O}(\log n)$ using $\mathcal{O}(n \log n \log\log n)$ gates and $\tilde{\mathcal{O}}(n)$ ancilla qubits.*

It is not known how to construct exact designs for arbitrary k. However, there are several examples of ensembles which are known to approximate the moments of the Haar measure [32, 34, 39, 66].

5. Example: PFC ensemble

We review the Permutation-Function-Clifford (PFC) construction introduced in [35], which adapts the state design construction by sandwiching a random phase between random permutation and Clifford operators:

Definition 8 (PFC ensemble [35])**.** *Suppose g and f are drawn uniformly randomly from permutations and binary functions on $\{0,1\}^n$, respectively, and C is drawn uniformly from the Clifford group on n qubits. Then the Permutation-Function-Clifford (PFC) ensemble is given by the family of n-qubit unitaries:*

$$U = PFC = \left[\sum_{x\in\{0,1\}^n} |g(x)\rangle\langle x|\right]\left[\sum_{x'\in\{0,1\}^n} (-1)^{f(x')}|x'\rangle\langle x'|\right] C. \tag{17}$$

In [35], it was proven that the PFC ensemble forms an approximate unitary k-design up to additive error $\varepsilon = \mathcal{O}(\sqrt{k^2/2^n})$. However, it was not known whether the PFC ensemble forms an approximate design up to small measurable error. This open question was resolved in [37]:

Theorem 1 (PFC are designs [37])**.** *The Permutation-Function-Clifford (PFC) ensemble is an approximate unitary k-design up to measurable error $\varepsilon = 4k^2/2^n$.*

We provide a short alternate proof of Theorem 1 in Section IV C.

6. Example: LRFC ensemble

We also review the Luby-Rackoff-Function-Clifford (LRFC) ensemble introduced in [50], which is a permutation-free alternative to the PFC ensemble. This alternative can be useful, since random functions are much easier to construct and analyze compared to random permutations.

Definition 9 (LRFC ensemble [50])**.** *Suppose h_L and h_R are drawn uniformly randomly from functions on $\{0,1\}^{n/2} \to \{0,1\}^{n/2}$, f is drawn uniformly randomly from binary functions on $\{0,1\}^n$, and C is drawn uniformly from the Clifford group on n qubits. Then the Luby-Rackoff-Function-Clifford (LRFC) ensemble is given by the family of n-qubit unitaries:*

$$U = S_L S_R FC \equiv \left[\sum_{x\in\{0,1\}^n} |x_L \oplus h_L(x_R)\|x_R\rangle\langle x_L\|x_R|\right]\left[\sum_{x'\in\{0,1\}^n} |x'_L\|x'_R \oplus h_R(x'_L)\rangle\langle x'_L\|x'_R|\right] FC, \tag{18}$$

where F acts as in Definition 8, and $\|$ denotes the concatenation of two $\frac{n}{2}$-bit strings, $x \equiv x_L\|x_R$ and $x' \equiv x'_L\|x'_R$.

The S_L and S_R operations are random functions that shuffle the left $n/2$ qubits conditional on the value of the right $n/2$ qubits, and vice versa. The composition $S_L S_R$ is a permutation of the 2^n bitstrings, which we can view as replacing the random permutation P in the PFC ensemble. The permutation $S_L S_R$ is not uniformly random, however.

In [50], it was shown that the LRFC ensemble forms an approximate unitary k-design with small measurable error:

Theorem 2 (LRFC are designs [50])**.** *The Luby-Rackoff-Function-Clifford (LRFC) ensemble is an approximate unitary k-design up to measurable error $\varepsilon = 6k^2/\sqrt{2^n}$.*

This shows that the permutation $S_L S_R$ is indistinguishable from a random permutation P, when applied in composition with F and C. We provide a short alternate proof of Theorem 2 in Section IV D.

D. k-wise independent random functions

We now review the properties of classical k-wise independent functions. We are interested in families of functions which generate outputs that are close to those of uniformly random Boolean functions:

Definition 10 (k-wise independent function)**.** *Let $f_\alpha : \{0,1\}^n \to \{0,1\}^n$ be a function on bitstrings of length n which is parameterized by a random seed $\alpha \in \mathcal{A}$. Then f_α is known as a k-wise independent function if for all choices of distinct input values $x_1, x_2, ..., x_k \in \{0,1\}^n$ and output values $y_1, y_2, ..., y_k \in \{0,1\}^n$,*

$$\Pr_{\alpha\sim\mathcal{A}}[f_\alpha(x_1) = y_1, f_\alpha(x_2) = y_2, ..., f_\alpha(x_k) = y_k] = 2^{-nk}. \tag{19}$$

This definition is automatically satisfied by a truly random function, which sends each input bitstring to an independent and uniformly random output bitstring.

The standard construction of k-wise independent functions uses polynomial evaluation over finite fields. Let the set of inputs $\{0,1\}^n$ be identified with the finite field $\mathbb{F}_{2^n} = \mathrm{GF}(2^n)$. Each element $a \in \mathbb{F}_{2^n}$ can be represented as an n-bit vector $a_{n-1}a_{n-2}\dots a_1a_0$ associated with the polynomial $a(x) = \sum_{i=0}^{n-1} a_i x^i$ over $\mathbb{Z}_2$. The field operations are defined as follows: addition $a + b$ corresponds to bitwise XOR, while multiplication $a \cdot b$ is computed by multiplying the polynomials $a(x) \cdot b(x)$ modulo an irreducible polynomial $p(x)$ of degree n.

Theorem 3 (Polynomial-based k-wise independent functions [67, 68])**.** *Consider the function $f_\alpha : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined as follows. The seed α consists of k elements $(a_0, a_1, \dots, a_{k-1})$, where $\alpha_i \in \mathbb{F}_{2^n}$. The function f_α is defined by the evaluation of the polynomial whose coefficients are given by the seed:*

$$f_\alpha(x) = \sum_{i=0}^{k-1} a_i x^i. \tag{20}$$

When $a_0, \dots, a_{k-1}$ are chosen uniformly at random, f_α is a k-wise independent function.

This construction has the desired k-wise independence property because any k distinct inputs $x_1, \dots, x_k$ form a Vandermonde system, and the corresponding outputs are determined by a degree-$(k-1)$ polynomial uniquely determined by its values at these points. Since the polynomial coefficients are chosen uniformly at random, the outputs appear uniformly random for any choice of k inputs.

1. *Example: Derandomization of the binary phase state*

One can use k-wise independent functions to realize practical implementations of state and unitary designs, which avoid the need for truly random Boolean functions. This can be achieved through bounded independence, by instead using k-wise independent functions:

Definition 11 (k-wise independent phase state)**.** *Let $f_\alpha : \{0,1\}^n \to \{0,1\}$ be a $(2k)$-wise independent function parameterized by α. The corresponding k-wise independent phase state is*

$$|\phi_\alpha\rangle = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{f_\alpha(x)} |x\rangle . \tag{21}$$

Lemma 7 (k-wise independent phase states are state k-designs [43])**.** *For any k and classical construction of a $(2k)$-wise independent function, the ensemble of k-wise independent binary phase states given by Def. 11 yields an ε-approximate state k-design with $\varepsilon = 4k^2/2^n$.*

An analogous replacement can be applied to the PFC circuit [35] and LRFC circuit to generate unitary k-designs using k-wise independent functions and k-wise independent permutations. We refer to [35] for a discussion of k-wise independent permutations, as we do not use them in our work. In general, k-wise independent permutations are more difficult to implement than k-wise independent functions.

II. QUANTUM CIRCUIT IMPLEMENTATION OF k-WISE INDEPENDENT FUNCTIONS

To implement k-wise independent functions efficiently in quantum circuits, we need to analyze the classical circuit complexity of polynomial evaluation over finite fields. We focus on implementations using classical reversible Boolean circuits with only constant-local Boolean gates and without the ability to perform unbounded fan-in or fan-out. We can directly implement a classical reversible Boolean circuit on a quantum computer via the following correspondence.

Quantum gates. A quantum circuit is inherently reversible as every quantum gate is a unitary transformation that preserves information. When implementing classical functions on quantum computers, we must use reversible classical circuits, which can be directly translated to quantum circuits by replacing each reversible Boolean gate, such as CNOT or Toffoli gates, to the associated quantum gates acting on computational basis states.

Ancilla qubits. Classical irreversible circuits can be made reversible through the use of ancillary bits to store intermediate results. On quantum devices, these ancillary bits become ancillary qubits. The number of classical ancillary bits directly determines the number of quantum ancillary qubits required.

Circuit depth. The depth of a reversible classical circuit is the depth of the associated quantum circuit.

This section provides a detailed analysis of the reversible Boolean circuit resources required for such implementations, which directly translate to quantum circuit resources through the above correspondence.

A. Finite field arithmetic

The efficient implementation of k-wise independent functions relies on fast algorithms for arithmetic operations in finite fields. We begin by establishing the circuit complexity of basic field operations.

1. Field addition

Field addition in $\mathbb{F}_{2^n}$ has a remarkably simple implementation:

Lemma 8 (Field Addition [69])**.** *Let $a, b \in \mathbb{F}_{2^n}$ represented by n bits. The sum $a+b$ can be computed by a reversible classical Boolean circuit of depth $\mathcal{O}(1)$ with no ancillary bits. The field addition operation can be implemented either as $a, b \mapsto a+b, b$ or $a, b \mapsto a, a+b$ without any ancillary bits.*

Proof. Addition in $\mathbb{F}_{2^n}$ corresponds to bitwise XOR of the binary representations. So we can implement $a+b$ using n parallel XOR gates, each acting on corresponding bit positions. This uses $\mathcal{O}(1)$ depth and no ancillary bits. □

2. Field multiplication

Field multiplication is significantly more complex than addition, requiring polynomial multiplication followed by modular reduction. The state-of-the-art approach for large numbers uses the Schönhage-Strassen algorithm [69–71]:

Lemma 9 (Field Multiplication [69–71])**.** *Let $a, b \in \mathbb{F}_{2^n}$ represented by n bits. The product $a \cdot b$ can be computed by a reversible classical Boolean circuit of depth $\mathcal{O}(\log n)$ with $\mathcal{O}(n \log n \log\log n)$ ancillary bits. The field multiplication operation is implemented as $a, b, 0^n, 0^m \mapsto a, b, a \cdot b, 0^m$ with m ancillary bits.*

We first describe the standard irreversible Boolean circuit for performing field multiplication, then explain how to make the circuit reversible. The algorithm consists of two main phases:

Phase 1: Polynomial multiplication. We multiply $a(x), b(x)$ in $\mathbb{Z}_2[x]$ to obtain $c'(x) = a(x) \cdot b(x)$ with degree at most $(2n-2)$. This is achieved using a divide-and-conquer approach:

1. **Recursive decomposition:** Rewrite the two degree-$(n-1)$ polynomials $a(x)$ and $b(x)$ over $\mathbb{F}_2$ as degree-$(n/\lfloor\sqrt{n}\rfloor)$ polynomials over the smaller field $\mathbb{F}_{2^{\lfloor\sqrt{n}\rfloor}}$.

2. **Number-Theoretic Transform (NTT):** Apply the finite field analog of the Fast Fourier Transform to transform the polynomials into evaluation form. This step has circuit depth $\mathcal{O}(\log n)$ and size $\mathcal{O}(n \log n)$.

3. **Pointwise multiplication:** Perform parallel pointwise multiplication over $\mathbb{F}_{2^{\lfloor\sqrt{n}\rfloor}}$. This step is implemented recursively, leading to the recurrence relations:

$$D(n) = D(\lfloor\sqrt{n}\rfloor) + \mathcal{O}(\log n), \qquad \text{(circuit depth)} \tag{22}$$
$$S(n) = S(\lfloor\sqrt{n}\rfloor) + \mathcal{O}(n \log n), \qquad \text{(circuit size)} \tag{23}$$

where we have $D(n), S(n) = \mathcal{O}(1)$ for any small constant n.

4. **Inverse NTT:** Transform back to the coefficient representation with the same complexity as the forward transform.

Solving the recurrence relations yields total circuit depth $\mathcal{O}(\log n)$ and size $\mathcal{O}(n \log n \log\log n)$.

Phase 2: Modular reduction. We reduce $c'(x)$ modulo the irreducible polynomial $p(x)$ to obtain $c(x) = c'(x) \bmod p(x)$ with degree at most $n-1$. This can be implemented using Barrett reduction [72]. The setup is as follows. We work in the ring $\mathbb{F}_2[x]$ of polynomials with coefficients in $\mathbb{F}_2$. For polynomials $f(x), g(x) \in \mathbb{F}_2[x]$ with $g(x) \neq 0$, polynomial division gives us:

$$f(x) = q(x) \cdot g(x) + r(x) \tag{24}$$

where $q(x)$ is the quotient and $r(x)$ is the remainder with $\deg(r) < \deg(g)$. We define $\lfloor f(x)/g(x) \rfloor = q(x)$ as the quotient polynomial, ignoring the remainder. Barrett reduction uses the following identity:

Theorem 4 (Barrett identity for polynomials)**.** *For $f, g, h \in \mathbb{F}_2[x]$ with $g, h \neq 0$, the following identity holds:*

$$\lfloor f/g \rfloor = \lfloor (f \cdot \lfloor h/g \rfloor)/h \rfloor \tag{25}$$

provided that $\deg(f) \leq \deg(h)$.

Proof. Let $f = q \cdot g + r$ and $h = q' \cdot g + r'$ where $\deg(r) < \deg(g)$ and $\deg(r') < \deg(g)$. Then $\lfloor f/g \rfloor = q$ and $\lfloor h/g \rfloor = q'$. We have:

$$f \cdot \lfloor h/g \rfloor = f \cdot q' = q \cdot g \cdot q' + r \cdot q' = h \cdot q + (r \cdot q' - r' \cdot q). \tag{26}$$

We can bound the degree of the error term $r \cdot q' - r' \cdot q$ as follows. Since $h = q' \cdot g + r'$, we have $\deg(q') = \deg(h) - \deg(g)$. Similarly, $\deg(q) = \deg(f) - \deg(g)$. Therefore:

$$\deg(r \cdot q') \leq \deg(r) + \deg(q') \leq \deg(q') + \deg(g) - 1 < \deg(h), \tag{27}$$
$$\deg(r' \cdot q) \leq \deg(r') + \deg(q) \leq \deg(q) + \deg(g) - 1 < \deg(f) \leq \deg(h). \tag{28}$$

Hence, $\deg(r \cdot q' - r' \cdot q) < \deg(h)$. This implies that:

$$\lfloor f \cdot \lfloor h/g \rfloor / h \rfloor = \left\lfloor \frac{h \cdot q + (r \cdot q' - r' \cdot q)}{h} \right\rfloor = q, \tag{29}$$

where the last equality follows because $\deg(r \cdot q' - r' \cdot q) < \deg(h)$. Since $\lfloor f/g \rfloor = q$, this concludes the proof. □

Barrett reduction computes $c'(x) \bmod p(x)$ using the above identity with $f = c'(x)$, $g = p(x)$, and $h = x^{2n-2}$. Since $\deg(c'(x)) \leq 2n - 2 = \deg(x^{2n-2})$, the condition is satisfied. The modular reduction becomes:

$$c'(x) \bmod p(x) = c'(x) - \lfloor c'(x)/p(x) \rfloor \cdot p(x) = c'(x) - \lfloor (c'(x) \cdot \lfloor x^{2n-2}/p(x) \rfloor)/x^{2n-2} \rfloor \cdot p(x). \tag{30}$$

The computation proceeds as follows:

1. **Precomputation:** For the fixed polynomial $p(x)$ of degree n, precompute the Barrett constant:

$$\mu(x) = \lfloor x^{2n-2}/p(x) \rfloor \tag{31}$$

This polynomial has degree $(2n-2) - n = n - 2$. Since $p(x)$ is fixed, $\mu(x)$ can be precomputed once (on a classical computer) and reused.

2. **Polynomial multiplication:** Perform polynomial multiplication $c'(x) \cdot \mu(x)$ to obtain the polynomial $e(x)$ of degree at most $(2n-2)+(n-2) = 3n-4$. This multiplication can be implemented using the Schönhage-Strassen algorithm with circuit depth $\mathcal{O}(\log n)$ and size $\mathcal{O}(n \log n \log\log n)$.

3. **Quotient extraction:** Compute the quotient:

$$q(x) = \lfloor e(x)/x^{2n-2} \rfloor \tag{32}$$

   By the Barrett identity, $q(x)$ equals the true quotient $\lfloor c'(x)/p(x) \rfloor$ and has degree at most $(3n-4)-(2n-2) = n-2$. This operation extracts the coefficients of x^{2n-2} and higher monomials from $e(x)$, which can be implemented by right-shifting the $(3n-3)$ bits describing $e(x)$ by $(2n-2)$ positions.

4. **Remainder computation:** Compute the remainder:

$$r(x) = c'(x) - q(x) \cdot p(x) = c'(x) + q(x) \cdot p(x), \tag{33}$$

   where the second equality holds in $\mathbb{F}_2[x]$. This requires another polynomial multiplication $q(x) \cdot p(x)$, which uses a circuit depth of $\mathcal{O}(\log n)$ and a size of $\mathcal{O}(n \log n \log\log n)$.

Since the Barrett identity guarantees that $q(x)$ is the exact quotient, the remainder $r(x)$ automatically has degree at most $n-1$ and equals $c'(x) \bmod p(x)$. The Barrett reduction requires two polynomial multiplications (steps 2 and 4), both implementable using the Schönhage-Strassen algorithm. The total circuit depth for Barrett reduction is $\mathcal{O}(\log n)$ and the total size is $\mathcal{O}(n \log n \log\log n)$. The field multiplication (polynomial multiplication + Barrett reduction) requires circuit depth $\mathcal{O}(\log n)$ and size $\mathcal{O}(n \log n \log\log n)$ using a standard Boolean circuit.

Conversion to reversible circuits. The above describes a standard Boolean circuit, which is irreversible in general. To obtain a reversible Boolean circuit, we apply the standard conversion procedure:

1. Create an ancillary bit initialized to 0 for every output bit of each gate.
2. Implement the irreversible Boolean circuit by replacing each Boolean gate with a reversible gate that acts on the associated ancillary bit.
3. Use bitwise XOR to copy the n ancillary bits associated with the answer $a \cdot b$ to the final n output bits.
4. Run all reversible gates in reverse to return all ancillary bits to 0.

Hence, the circuit size of a standard Boolean circuit upper bounds the number of ancillary bits of the reversible Boolean circuit, while the circuit depth only increases by a constant factor. Together, the product $a \cdot b$ can be computed by a reversible classical Boolean circuit of depth $\mathcal{O}(\log n)$ with $\mathcal{O}(n \log n \log\log n)$ ancillary bits.

B. Polynomial evaluation circuit

With the field arithmetic primitives established, we can now analyze the evaluation of k-wise independent functions:

Lemma 10 (Low-depth and low-ancilla k-wise independent functions)**.** *A classical reversible Boolean circuit for evaluating $f_\alpha(x) = \sum_{i=0}^{k-1} a_i x^i$ for a given seed $\alpha = (a_0, \ldots, a_{k-1})$ and input $x \in \mathbb{F}_{2^n}$ can be implemented with either:*

1. ***Low depth:*** *$\mathcal{O}(\log k \cdot \log n)$ depth and $\mathcal{O}(kn \log n \cdot \log\log n)$ ancillary bits.*
2. ***Low ancilla:*** *$\mathcal{O}(k \cdot \log n)$ depth and $\mathcal{O}(n \log n \cdot \log\log n)$ ancillary bits.*

We present both low-depth and low-ancilla constructions below.

Low-depth construction:

The computation proceeds in three stages as follows.

Stage 1: Computing powers of x

The first stage computes all powers $x^0, x^1, \ldots, x^{k-1}$ using an approach that minimizes circuit depth:

Phase 1a (Sequential power computation): Compute exponents that are powers of 2 using repeated squaring:

$$x^1 = x \tag{34}$$
$$x^2 = x^1 \cdot x^1 \tag{35}$$
$$x^4 = x^2 \cdot x^2 \tag{36}$$
$$\vdots \tag{37}$$
$$x^{2^{\lfloor \log_2(k-1) \rfloor}} = \left(x^{2^{\lfloor \log_2(k-1) \rfloor - 1}}\right)^2 \tag{38}$$

This requires $\lfloor \log_2(k-1) \rfloor = \mathcal{O}(\log k)$ field multiplications performed sequentially. The powers are stored in $\lfloor \log_2(k-1) \rfloor \cdot n$ bits. Since each multiplication has depth $\mathcal{O}(\log n)$ by Lemma 9, the total circuit depth is $\mathcal{O}(\log k \cdot \log n)$. By reusing ancillary bits across sequential field multiplications, we need only $\mathcal{O}(n \log n \log\log n)$ ancillary bits.

Phase 1b (Parallel power computation): Use a binary tree to copy the power-of-2 exponents for later use. This requires depth $\mathcal{O}(\log k)$ and $\mathcal{O}(nk \log k)$ ancillary bits. For each remaining exponent $j \in \{3, 5, 6, 7, 9, \ldots, k-1\}$, we express j in binary as $j = \sum_i b_i 2^i$ and compute:

$$x^j = \prod_{i : b_i = 1} x^{2^i}. \tag{39}$$

All exponents j are computed in parallel. Each product requires at most $\mathcal{O}(\log k)$ field multiplications. All powers of x, $x^0, x^1, \ldots, x^{k-1}$, are stored in classical memory, which requires $k \cdot n$ bits. The total circuit depth is $\mathcal{O}(\log k \cdot \log n)$, and the number of ancillary bits is $\mathcal{O}(k \cdot n \log n \log\log n)$.

Stage 2: Coefficient multiplication

Compute $a_i \cdot x^i$ for all $i \in \{0, 1, \ldots, k-1\}$ in parallel. Each of the k parallel multiplications requires the use of $\mathcal{O}(n \log n \log\log n)$ ancillary bits by Lemma 9, for a total of $\mathcal{O}(k \cdot n \log n \log\log n)$ ancillary bits. Since all multiplications are performed in parallel, the circuit depth is $\mathcal{O}(\log n)$.

Stage 3: Binary tree summation

Sum the k terms $a_i \cdot x^i$ using a binary tree with $\lceil \log_2 k \rceil$ levels of parallel additions:

$$\text{Level 1:} \quad \lceil k/2 \rceil \text{ pairwise sums in parallel} \tag{40}$$
$$\text{Level 2:} \quad \lceil k/4 \rceil \text{ pairwise sums in parallel} \tag{41}$$
$$\vdots \tag{42}$$
$$\text{Final level:} \quad \text{Single sum} \tag{43}$$

By Lemma 8, each addition requires constant depth and no ancillary bits. The total circuit depth is $\mathcal{O}(\log k)$.

Final reversible implementation

We use bitwise XOR to copy the n ancillary bits associated with the answer $f_\alpha(x)$ to the final n output bits. By running the entire circuit in reverse, we return all ancillary bits to 0. This reversible Boolean circuit implements:

$$\alpha, x, 0^n, 0^m \mapsto \alpha, x, f_\alpha(x), 0^m, \tag{44}$$

where $m = \mathcal{O}(kn \log n \log\log n)$ is the total number of ancillary bits required.

Low-ancilla construction:

The low-ancilla approach trades depth for space by computing the function $f_\alpha(x) = \sum_{i=0}^{k-1} a_i x^i$ sequentially using the following algorithm:

$$\texttt{result} \leftarrow 0 \tag{45}$$

$$\texttt{current\_power} \leftarrow 1 \quad \text{(representing } x^0\text{)} \tag{46}$$

$$\texttt{for } i = 0 \texttt{ to } k-1: \tag{47}$$

$$\texttt{result} \leftarrow \texttt{result} + a_i \cdot \texttt{current\_power} \tag{48}$$

$$\texttt{current\_power} \leftarrow \texttt{current\_power} \cdot x \tag{49}$$

Each iteration requires one field multiplication ($a_i \cdot$ `current_power`), one field addition (`result` + $a_i \cdot$ `current_power`), and one field multiplication (`current_power` $\cdot x$). Each field arithmetic operation has depth $\mathcal{O}(\log n)$ by Lemma 8 and Lemma 9. With k sequential iterations, the total depth is $\mathcal{O}(k \log n)$.

The space complexity includes storage for `result`, `current_power`, and temporary ancillary bits for field operations. Since we reuse ancillary bits across sequential operations, the total requirement is $\mathcal{O}(n \log n \log\log n)$ ancillary bits. Similar to the low-depth construction, we use the bitwise XOR to copy the n bits associated with the answer $f_\alpha(x)$ to the final n output bits. By running the entire circuit in reverse, we return all ancillary bits to 0. This reversible Boolean circuit implements:

$$\alpha, x, 0^n, 0^m \mapsto \alpha, x, f_\alpha(x), 0^m, \tag{50}$$

where m is the total number of ancillary bits required for the chosen construction.

C. Summary of circuit resources

The complete quantum circuit implementation of a k-wise independent n-bit function uses either:

- **Low depth:** $\mathcal{O}(\log k \cdot \log n)$ depth and $\mathcal{O}(kn \log n \log\log n)$ ancillary qubits.
- **Low ancilla:** $\mathcal{O}(k \cdot \log n)$ depth and $\mathcal{O}(n \log n \log\log n)$ ancillary qubits.

These resource requirements provide flexibility for different quantum computing architectures, enabling efficient implementations of k-wise independent designs based on available resources.

III. STATE DESIGNS IN NEARLY OPTIMAL DEPTH

In this section, we provide details of our construction of approximate state designs. We first introduce our design construction based on blocked random phase states. We then discuss the key ingredient of our proof, the local distinct subspace projector, and provide full proof details. We discuss the application of our results to a simple construction of poly $\log\log n$-depth pseudorandom states in the final section.

A. Blocked random phase states

As discussed in the main text (Fig. 1), we consider a blocked variant of the random binary phase state,

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{\sum_a f_{a,a+1}(x_{a,a+1})} |x\rangle\,, \tag{51}$$

in which the phase $f(x) \equiv \sum_a f_{a,a+1}(x)$ is computed via a two-layer circuit of random classical functions. Here, we make a small change in notation compared to the main text, by replacing the index i for each patch of 2ξ qubits with the index $a, a+1$ (which labels the two patches of ξ qubits each, a and $a+1$, that combine to form i). This makes it explicit that adjacent functions overlap on patches of ξ qubits each. Each function $f_{a,a+1}$ acts on 2ξ qubits, and only depends on the values $x_{a,a+1}$ of the bitstring x on those qubits. The value of ξ is tunable and will be set depending on the desired n, k, ε of the state design.

To construct approximate state k-designs, we draw each $f_{a,a+1}$ from a $2k$-wise independent random function ensemble on 2ξ bits. We require $2k$-wise independence instead of k-wise independence to account for both the "ket" and "bra" of the quantum state. We will refer to the resulting ensemble, k-wise independent blocked random phase state. We prove that they form state designs:

Theorem 5 (Blocked random phase states are designs)**.** *The k-wise independent blocked random phase state ensemble with parameter ξ is an approximate state k-design up to additive error $\varepsilon = 3nk^2/2^\xi\xi + 2k^2/2^n = \mathcal{O}(nk^2/2^\xi\xi)$.*

The circuit depth of the resulting state ensemble is equal to twice the circuit depth of a k-wise independent function on 2ξ qubits. From Lemma 10 of Section II, we have:

Fact 2 (Circuit resources for blocked random phase states)**.** *The n-qubit k-wise independent blocked random phase state with parameter ξ can be implemented with either:*

1. ***Low depth:*** *$\mathcal{O}(\log k \cdot \log \xi)$ depth using $\mathcal{O}(kn \log \xi \cdot \log\log \xi)$ ancilla qubits.*

2. ***Low ancilla:*** *$\mathcal{O}(k \cdot \log \xi)$ depth using $\mathcal{O}(n \log \xi \cdot \log\log \xi)$ ancilla qubits.*

Both implementations use $2nk$ bits of randomness.

The number of bits of randomness follows because each k-wise independent function uses ξk bits of randomness [48]. The optimal number of bits of randomness for quantum state k-designs is nk (up to sub-leading additive factors) [29, 52]; a mere factor of two fewer than our ensemble. Intuitively, this lower bound follows because the Haar twirl χ_H has rank 2^{nk} (up to sub-leading multiplicative factors, for $k \ll 2^n$).

Combining Fact 2 and Theorem 5 yields the following:

Corollary 1 (Circuit resources for state k-designs)**.** *For any $k^2/\varepsilon \leq 2^n/3$, setting $\xi = \max(\log_2(3nk^2/\varepsilon), 3) \leq n$ yields approximate state k-designs with additive error ε using either:*

- ***Low depth:*** *$\mathcal{O}(\log k \cdot \log\log(nk/\varepsilon))$ depth and $\mathcal{O}(kn \log\log(nk/\varepsilon) \log\log\log(nk/\varepsilon))$ ancilla qubits.*

- ***Low ancilla:*** *$\mathcal{O}(k \cdot \log\log(nk/\varepsilon))$ depth and $\mathcal{O}(n \log\log(nk/\varepsilon) \log\log\log(nk/\varepsilon))$ ancilla qubits.*

Both use $2nk$ bits of randomness, which is merely a factor of two above the optimal nk bits for n-qubit state k-designs.

B. The local distinct subspace

Before proceeding to our proof of Theorem 5, let us first introduce a key technical object in our analysis: the local distinct subspace. We begin with the standard (non-local) distinct subspace [35], and then turn to its local variant.

Let $x = (x^{(1)}, x^{(2)}, \ldots, x^{(k)})$ be a length-k list of n-bit strings. The list labels a computational basis state $|x\rangle \equiv \bigotimes_{j=1}^k |x^{(j)}\rangle$ on the k-copy Hilbert space. The *distinct subspace* is spanned by x such that no two $x^{(j)}$ are equal:

Definition 12 (Distinct subspace [35])**.** *Let* $\text{dist} = \{x \,|\, x^{(i)} \neq x^{(j)} \text{ for } i \neq j\}$ *denote the set of distinct x. The* distinct subspace *is defined by the projector*

$$\Pi_{\text{dist}} = \sum_{x \in \text{dist}} |x\rangle\langle x| \,. \tag{52}$$

The subspace has dimension $\mathfrak{D} = (2^n)!/(2^n - k)!$ which obeys $1 - k^2/2^n \leq \mathfrak{D}/2^{nk} \leq 1$.

A crucial property of the distinct subspace is that *most* bitstrings are distinct when $k^2 \ll 2^n$. This is formalized by the lower bound on the dimension of the distinct subspace $\mathfrak{D}$ stated in the definition. The lower bound shows that the ratio of the number of distinct bitstrings, $\mathfrak{D}$, to the number of total bitstrings, 2^{nk}, is close to one when $k^2 \ll 2^n$.

To analyze our blocked state and unitary ensembles, we introduce a *local* variant of the distinct subspace. Let $x_a^{(j)}$ denote the ξ-bit string obtained by restricting an n-bit string $x^{(j)}$ to the ξ qubits on patch a. We let $x_a = (x_a^{(1)}, x_a^{(2)}, \ldots, x_a^{(k)})$ denote the corresponding length-k list of ξ-bit strings. The *local distinct subspace* is spanned by x such that x_a is distinct for every patch a.

Definition 13 (Local distinct subspace)**.** *For any system of n qubits divided into patches of ξ qubits each. Let* loc-dist $= \{x \,|\, x_a^{(i)} \neq x_a^{(j)}$ for all a and $i \neq j\}$ *denote the set of locally distinct x. The* local distinct subspace *is defined by the projector*

$$\Pi_{\text{dist}}^{\text{loc}} \equiv \sum_{x \in \text{loc-dist}} |x\rangle\langle x| \,. \tag{53}$$

The local distinct subspace has dimension $\mathfrak{D}_{\text{loc}} = ((2^\xi)!/(2^\xi - k)!)^{n/\xi}$ which obeys $1 - nk^2/2^\xi\xi \leq \mathfrak{D}_{\text{loc}} \leq 1$.

The local distinct subspace is contained within the global distinct subspace, $\Pi_{\text{dist}}^{\text{loc}} = \Pi_{\text{dist}}^{\text{loc}}\Pi_{\text{dist}}$.

One might worry that requiring each bitstring to be locally distinct imposes too strong of a restriction, and that most bitstrings will lie outside the local distinct subspace. Fortunately, this is not the case, as expressed in the lower bound on $\mathfrak{D}_{\text{loc}}$ stated in the definition. To derive the formula for $\mathfrak{D}_{\text{loc}}$, we note that the local distinct subspace projector is a tensor product of projectors onto the distinct subspace of each patch a, $\Pi_{\text{dist}}^{\text{loc}} = \bigotimes_a \Pi_{\text{dist}}^a$, where $\Pi_{\text{dist}}^a \equiv \sum_{x_a \in \text{dist}_a} |x_a\rangle\langle x_a|$. The subspace dimension is therefore given by $\mathfrak{D}_{\text{loc}} = \prod_{a=1}^m \mathfrak{D}_a$ where $m \equiv n/\xi$ is the total number of patches and $\mathfrak{D}_a = (2^\xi)!/(2^\xi - k)!$ is the distinct subspace dimension of each patch. From the bound

$$1 - k^2/2^\xi \leq \mathfrak{D}_a \leq 1, \tag{54}$$

we have $1 - mk^2/2^\xi \leq \mathfrak{D}_{\text{loc}} \leq 1$. Hence, most bitstrings are locally distinct when $(n/\xi)k^2 < nk^2 \ll 2^\xi$, which only requires ξ be logarithmic in n and k.

C. Proof of Theorem 5: The blocked random phase state has small additive error

Let us now turn to the proof of Theorem 5 and show that the blocked random phase state is a state k-design. Our proof consists of only a small number of very straightforward steps, as discussed in the main text. We describe each step in detail to facilitate understanding.

We consider three state ensembles. Let

$$\chi_B \equiv \mathop{\mathbb{E}}_{F_{a,a+1}} \Big[\Big(\prod_a F_{a,a+1} \Big)^{\otimes k} \cdot |+^n\rangle\langle+^n|^{\otimes k} \cdot \Big(\prod_a F_{a,a+1} \Big)^{\otimes k} \Big] \tag{55}$$

denote the twirl of the blocked random phase state,

$$\chi_F \equiv \mathop{\mathbb{E}}_{F} \Big[F^{\otimes k} \cdot |+^n\rangle\langle+^n|^{\otimes k} \cdot F^{\otimes k} \Big] \tag{56}$$

denote the twirl of the (global) random phase state, and

$$\chi_H \equiv \mathop{\mathbb{E}}_{U} \Big[U^{\otimes k} \cdot |+^n\rangle\langle+^n|^{\otimes k} \cdot (U^\dagger)^{\otimes k} \Big] = \frac{(2^n - 1)!}{(2^n + k - 1)!} \sum_{\pi \in S_k} \pi, \tag{57}$$

denote the Haar twirl. Our consideration of the random phase state χ_F is purely for pedagogical sake. In the formula for χ_H, we apply a standard equation for the Haar twirl[73].

The twirls of the blocked random phase state and global random phase state are easy to compute. Let us decompose $|+^n\rangle\langle+^n|^{\otimes k} = \frac{1}{2^{nk}} \sum_{x,\tilde{x}} |\tilde{x}\rangle\langle x|$ in the computational basis on k copies. When averaged, the global random phase F enforces that $\tilde{x}$ and x are related by a permutation $\pi \in S_k$,

$$\chi_F = \mathop{\mathbb{E}}_{f} \left[\frac{1}{2^{nk}} \sum_{x,\tilde{x}} (-1)^{\sum_j f(x^{(j)}) + \sum_j f(\tilde{x}^{(j)})} |\tilde{x}\rangle\langle x| \right] = \frac{1}{2^{nk}} \sum_{x,\tilde{x}} \delta_{\tilde{x} \in \{\pi x | \pi \in S_k\}} \cdot |\tilde{x}\rangle\langle x| \,.$$

The relation[74] $\tilde{x} = \pi x$ guarantees that the phase vanishes, $\sum_j f(\tilde{x}^{(j)}) + \sum_j f(x^{(j)}) = 0$, for every random function f. If this condition does not hold, the average over f will cause the term to vanish. The twirl of the blocked random phase state is similarly easy to compute, albeit with several more indices,

$$\chi_B = \mathop{\mathbb{E}}_{f_{a,a+1}} \left[\frac{1}{2^{nk}} \sum_{x,\tilde{x}} (-1)^{\sum_{j,a} f_{a,a+1}(x_{a,a+1}^{(j)}) + \sum_{j,a} f_{a,a+1}(\tilde{x}_{a,a+1}^{(j)})} |\tilde{x}\rangle\langle x| \right] = \frac{1}{2^{nk}} \sum_{x,\tilde{x}} \Big(\prod_a \delta_{\tilde{x}_{a,a+1} \in \{\pi_a x_{a,a+1} | \pi_a \in S_k\}} \Big) \cdot |\tilde{x}\rangle\langle x| \,.$$

The total phase is a sum of the local phases from each patch $a, a+1$ of each copy j. For the term to not vanish after averaging over every $f_{a,a+1}$, we require $\tilde{x}_{a,a+1} = \pi_a x_{a,a+1}$ for some permutation $\pi_a \in S_k$ on each patch a. Note that this condition is equivalent to $\tilde{x}_a = \pi_a x_a$ and $\tilde{x}_{a+1} = \pi_a x_{a+1}$ for every a, if we consider the support of x on each patch a and $a+1$ individually.

With formulas for all three states in hand, we can now project onto the local distinct subspace. Note that all three states commute with the local distinct subspace projector. Hence, we have

$$\left\|\chi_B - \Pi^{\text{loc}}_{\text{dist}}\, \chi_B\, \Pi^{\text{loc}}_{\text{dist}}\right\|_1 \leq 1 - \text{tr}\left(\Pi^{\text{loc}}_{\text{dist}}\, \chi_B\right) \tag{58}$$

and similar for χ_F and χ_H. Since χ_B and χ_F have uniform support over the computational basis states, we have

$$1 - \text{tr}\left(\Pi^{\text{loc}}_{\text{dist}}\, \chi_B\right) = 1 - \text{tr}\left(\Pi^{\text{loc}}_{\text{dist}}\, \chi_F\right) = 1 - \mathfrak{D}_{\text{loc}}/2^{nk} \leq nk^2/2^\xi \xi. \tag{59}$$

This implies that the projection to the local distinct subspace incurs only a small trace-norm error, as discussed in the main text. For the Haar-random state χ_H, we have

$$1 - \text{tr}\left(\Pi^{\text{loc}}_{\text{dist}}\, \chi_H\right) = 1 - \text{tr}\left(\Pi^{\text{loc}}_{\text{dist}}\right) \frac{(2^n-1)!}{(2^n+k-1)!} = 1 - \mathfrak{D}_{\text{loc}} \frac{(2^n-1)!}{(2^n+k-1)!} \leq nk^2/2^\xi \xi + k^2/2^n. \tag{60}$$

This follows immediately from Eq. (57) because the trace of all $\pi \neq \mathbb{1}$ with the distinct projector are zero. The inequality holds because $\mathfrak{D}_{\text{loc}}$ is only slightly less than 2^{nk} and the ratio of factorials is only slightly less than $1/2^{nk}$ (for $k^2 \leq 2^n$). Hence, the Haar-random state can also be projected to the local distinct subspace with only a small trace-norm error.

To complete the proof, we just observe that the three states are equal on the local distinct subspace. Consider χ_B and χ_F. For χ_B, the twirl yielded $\tilde{x}_a = \pi_a x_a$ and $\tilde{x}_{a+1} = \pi_a x_{a+1}$ for each a. When x_a is distinct, there is a unique π_a that can satisfy either condition. This implies that the first permutation π_1 (which obeys $\tilde{x}_1 = \pi_1 x_1$ and $\tilde{x}_2 = \pi_1 x_2$) must equal the second permutation π_2 (which obeys $\tilde{x}_2 = \pi_2 x_2$ and $\tilde{x}_3 = \pi_2 x_3$). Iterating $m = n/\xi$ times, one finds that *all* permutations are in fact equal, $\pi_a = \pi_1 \equiv \pi$. This produces an identical state as the global random phase,

$$\Pi^{\text{loc}}_{\text{dist}}\, \chi_B\, \Pi^{\text{loc}}_{\text{dist}} = \frac{1}{2^{nk}} \sum_{\pi \in S_k} \sum_{x \in \text{loc-dist}} |\pi x\rangle\langle x| = \Pi^{\text{loc}}_{\text{dist}}\, \chi_F\, \Pi^{\text{loc}}_{\text{dist}}. \tag{61}$$

Here, we replace the sum over $\tilde{x}$ with a sum over π, since for every distinct x, each $\pi \in S_k$ contributes a unique $\tilde{x} = \pi x$. Turning to χ_H, we insert the definition of $\Pi^{\text{loc}}_{\text{dist}}$ into the formula for χ_H [Eq. (57)], which gives

$$\Pi^{\text{loc}}_{\text{dist}}\, \chi_H\, \Pi^{\text{loc}}_{\text{dist}} = \frac{(2^n-1)!}{(2^n+k-1)!} \sum_{\pi \in S_k} \sum_{x \in \text{loc-dist}} |\pi x\rangle\langle x|\,. \tag{62}$$

As promised, this is equal to the projected χ_B and χ_F up to only a small difference in normalization. Observing Eq. (59) and Eq. (60), the difference in normalization can be at most $nk^2/2^\xi \xi + k^2/2^n$. This implies that the trace-norm error is bounded by the same amount, $\|\Pi^{\text{loc}}_{\text{dist}}\, \chi_B\, \Pi^{\text{loc}}_{\text{dist}} - \Pi^{\text{loc}}_{\text{dist}}\, \chi_H\, \Pi^{\text{loc}}_{\text{dist}}\|_1 \leq nk^2/2^\xi \xi + k^2 2^n$. Combining with Eq. (59) and Eq. (60), we have $\|\chi_B - \chi_H\|_1 \leq 3nk^2/2^\xi \xi + 2k^2/2^n = \mathcal{O}(nk^2/2^\xi \xi)$ as desired. □

D. Second approach to nearly optimal state designs via state-function gluing lemma

In this section, we provide a second, alternative approach to proving Theorem 5. Instead of analyzing the entire blocked random phase circuit at once, our alternative approach analyzes only three adjacent blocks of the circuit at a time. This yields moderately simpler notation. It also provides a more versatile intermediary result, showing that any two random states can be "glued" together by a random function acting on small subsets of both systems.

In order to analyze the moments of this ensemble, we formulate a procedure to "glue" together state designs on neighboring blocks using random phase operators. The main technical ingredient is an adaptation of the distinct subspace analysis in which we consider a projection onto the locally distinct subspace of the region acted on by the phase operators. We then bound the statistical closeness to a Haar-random state after introducing each new block. This procedure yields an error that is exponentially small in the block size, so that plugging in known implementations of classical k-wise independent functions yields a depth which is doubly logarithmically in the system size.

Lemma 11 (Gluing state designs with phase operators)**.** *Suppose $\mathcal{S}_A, \mathcal{S}_B$ are ε_A- and ε_B-approximate state k-designs on A and B, respectively, where $|A|, |B| \geq \xi$ and $k = o(2^{\xi/2})$. Then the ensemble formed by applying a random phase operator F_α on ξ qubits each of A and of B is an ε-approximate state k-design with*

$$\varepsilon = \varepsilon_A + \varepsilon_B + \mathcal{O}(k^2/2^\xi). \tag{63}$$

Proof. Let $\mathcal{S}_{FAB}$ and $\mathcal{S}_F$ denote the state ensembles generated by applying random phase operators on ξ qubits each of states from $\mathcal{S}_A, \mathcal{S}_B$, and on Haar-random states on the two regions, respectively. Recall that we have

$$\begin{aligned} \|\chi_{\mathcal{S}_{FAB}} - \chi_H\|_1 &\leq \|\chi_{\mathcal{S}_{FAB}} - \chi_{\mathcal{S}_F}\|_1 + \|\chi_{\mathcal{S}_F} - \chi_H\|_1 \\ &\leq \varepsilon_A + \varepsilon_B + \|\chi_{\mathcal{S}_F} - \chi_H\|_1, \end{aligned} \tag{64}$$

where we have used the fact that the trace norm is non-increasing under the application of any quantum channel to replace the first term. To analyze the second term, we apply projections onto the locally distinct subspaces corresponding to Ξ_A and Ξ_B, the respective regions of A, B that the phase operators act on. We have:

$$\begin{aligned} \|\chi_{\mathcal{S}_F} - \chi_H\|_1 \leq& \left\|\chi_{\mathcal{S}_F} - \left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] \chi_{\mathcal{S}_F} \left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right]\right\|_1 \\ &+ \left\|\left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] \chi_{\mathcal{S}_F} \left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] - \chi_H\right\|_1 \\ \leq& \left\|\left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] \chi_{\mathcal{S}_F} \left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] - \chi_H\right\|_1 + \mathcal{O}(k^2/2^\xi). \end{aligned} \tag{65}$$

In addition, since the projection operators are diagonal in the computational basis, they commute with the action of the phase operators. We can therefore write the twirl over the phases via

$$\begin{aligned} &\left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] \chi_{\mathcal{S}_F} \left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] \\ &= \mathop{\mathbb{E}}_\alpha F_\alpha^{\otimes k} \left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] \left[\chi_{H(A)} \otimes \chi_{H(B)}\right] \left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] F_\alpha^{\otimes k} \\ &= \mathop{\mathbb{E}}_\alpha F_\alpha^{\otimes k} \left[\frac{1}{(k!)^2 Z_A Z_B} \sum_{\substack{a \in \{0,1\}^{k(|A|-\xi)} \\ \vec{x} \in \mathrm{dist}(2^\xi, k)}} \sum_{\pi \in S_k} |a, \vec{x}\rangle\langle \pi(a, \vec{x})| \otimes \sum_{\substack{b \in \{0,1\}^{k(|B|-\xi)} \\ \vec{x}' \in \mathrm{dist}(2^\xi, k)}} \sum_{\pi' \in S_k} |\vec{x}', b\rangle\langle \pi'(\vec{x}', b)|\right] F_\alpha^{\otimes k}, \end{aligned} \tag{66}$$

where the normalization factors are given by the dimensions of the corresponding symmetric subspaces

$$Z_A = \binom{2^{|A|} + k - 1}{k}, \quad Z_B = \binom{2^{|B|} + k - 1}{k}. \tag{67}$$

We now observe that the twirl over the random phases eliminates contributions from terms where $\pi \neq \pi'$. The entire projected component is therefore maximally mixed on a subspace of the global symmetric subspace, so the final term in the RHS of Eq. 65 is bounded by

$$\begin{aligned} \mathrm{RHS} &= 1 - \mathrm{Tr}\left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] \chi_{\mathcal{S}_F} \left[\Pi_{\mathrm{dist}(\Xi_A)} \otimes \Pi_{\mathrm{dist}(\Xi_B)}\right] \\ &= 1 - 2^{k(|A|-\xi)} 2^{k(|B|-\xi)} \binom{2^\xi}{k}^2 \binom{2^{|A|} + k - 1}{k}^{-1} \binom{2^{|B|} + k - 1}{k}^{-1} \\ &= 1 - \frac{2^{k(|A|-\xi)} 2^\xi (2^\xi - 1) \cdots (2^\xi - k + 1)}{(2^{|A|} + k - 1)(2^{|A|} + k - 2) \cdots 2^{|A|}} \frac{2^{k(|B|-\xi)} 2^\xi (2^\xi - 1) \cdots (2^\xi - k + 1)}{(2^{|B|} + k - 1)(2^{|B|} + k - 2) \cdots 2^{|B|}} \\ &\leq \mathcal{O}(k^2/2^\xi) + \mathcal{O}(k^2/2^{|A|}) + \mathcal{O}(k^2/2^{|B|}), \end{aligned} \tag{68}$$

where in the last step we have used the restriction on k to obtain the asymptotic expansion in terms of $|A|, |B|$, and ξ. Plugging back into Eq. 64 and collecting the error terms from each step yields

$$\|\chi_{\mathcal{S}_{FAB}} - \chi_H\|_1 \leq \varepsilon_A + \varepsilon_B + \mathcal{O}(k^2/2^\xi), \tag{69}$$

up to leading order in k and ξ. □

We can then plug the approximation error given in Lemma 7 into the above result repeatedly in order to obtain a bound on the blocked phase state construction. From Lemma 7, applying the first layer of phase gates yields approximate state designs on each block, up to error $\mathcal{O}(k^2/2^\xi)$. The result follows from starting with the leftmost block, then applying Lemma 11 for each additional block, up to $n/2\xi - 1$. This gives an alternative proof of Theorem 5.

E. Application to pseudorandom states

Although the main focus of our work concerns state and unitary designs, our results also yield simple constructions and proofs of pseudorandom states and unitaries. A pseudorandom state (PRS) is an ensemble of quantum states that is indistinguishable from the Haar-random state ensemble by any bounded-time quantum experiment. Here, a bounded-time quantum experiment is any experiment that involves a bounded number of queries to the unknown state as well as bounded-time quantum circuits in between queries. We refer to earlier works for a comprehensive and pedagogical introduction [19, 37, 39]. To be more specific, we say that a PRS on n qubits has security against any $t(n)$-time adversary if the PRS cannot be distinguished from Haar-random by any $t(n)$-time experiment, where $t(n)$ is any function of n.

The canonical example of a PRS is the pseudorandom binary phase state. This is identical to the binary phase state in Eq. (51), except that $f(x)$ is taken to be a quantum-secure pseudorandom function (PRF) instead of a classical k-wise independent function. By definition, a quantum-secure PRF is indistinguishable from a truly random function by any bounded-time quantum experiment. Hence, the proof that the pseudorandom binary phase state is a PRS amounts to showing that the truly random binary phase state is indistinguishable from Haar-random. This is identical to the proof that the random binary phase states form an approximate state k-design for any bounded $k = \mathcal{O}(t(n))$ and additive error $1/\varepsilon = \mathcal{O}(t(n))$. Therefore, the proof of Lemma 7 (originally proven in [43] using substantially different techniques) also implies that the pseudorandom binary phase state is a PRS with security against any sub-exponential time adversary.

We can now apply an identical logic to the blocked random phase state. Replacing each local function $f_{a,a+1}$ with a PRF on 2ξ qubits yields the simplest construction yet of low-depth pseudorandom states. We take each PRF to be indistinguishable from random by any $o(\exp(\xi))$-time adversary [49]. Our proof of Theorem 5 shows that the random ensemble is an approximate state k-design for any $k, 1/\varepsilon = o(\exp(\xi))$. Hence, the original pseudorandom ensemble is indistiguishable from a Haar-random state by any $o(\exp(\xi))$-time adversary. We set $\xi = \omega(\log n)$, in which case $o(\exp(\xi))$-time security implies security against any polynomial-time adversary since $\operatorname{poly} n = o(\exp(\xi))$. Our ensemble can be compiled in circuit depth $\operatorname{poly}\log n$ in 1D circuits and $\operatorname{poly}\log\log n$ in all-to-all connected circuits [39]. These scalings are similar to existing extremely low-depth PRS constructions [39]; the primary benefit is that our construction and proof are much simpler.

IV. UNITARY DESIGNS IN NEARLY OPTIMAL DEPTH

In this section, we provide the full details of our construction of approximate unitary k-designs in circuit depth $\mathcal{O}(\log k \log\log nk/\varepsilon)$. We first introduce our design construction based on the blocked LRFC circuit ensemble. We then describe our novel approach to bounding the measurable error of random unitary ensembles. We apply this approach to provide short proofs that the PFC ensemble, LRFC ensemble, and blocked LRFC ensemble have small measurable error. We review the application of our proofs to pseudorandom unitaries in the final section.

A. Blocked Luby-Rackoff-Function-Clifford (LRFC) circuits

As introduced in the main text (Fig. 1), we consider a blocked variant of the LRFC circuit ensemble:

Definition 14 (Blocked LRFC circuit)**.** *Consider the circuit shown in Fig. 1(b) of the main text, in which:*

- *For every patch a, $h_{a,a+1}$ is drawn uniformly randomly from functions on $\{0,1\}^\xi \to \{0,1\}^\xi$, and instantiates the shuffle gate $S_{a,a+1}\,|x_a\|x_{a+1}\rangle = |x_a\|x_{a+1} \oplus h_{a,a+1}(x_a)\rangle$.*
- *For every patch a, $f_{a,a+1}$ is drawn uniformly randomly from binary functions on $\{0,1\}^{2\xi} \to \{0,1\}$, and instantiates the random function $F_{a,a+1}\,|x_{a,a+1}\rangle = (-1)^{f_{a,a+1}(x_{a,a+1})}\,|x_{a,a+1}\rangle$.*
- *For every odd patch a, C_a is drawn uniformly randomly from the Clifford group on ξ qubits.*

. The blocked Luby-Rackoff-Function-Clifford (LRFC) ensemble is given by the family of n-qubit random unitaries:

$$U = S_o \cdot F_e \cdot F_o \cdot S_e \cdot C_o, \tag{70}$$

where $S_o = \bigotimes_{a\in even} S_{a,a+1}$ is a tensor product of random shuffles of odd patches conditional on even patches, $F_e = \bigotimes_{a\in even} F_{a,a+1}$ is a tensor product of random functions on each even pairs of patches, $F_o = \bigotimes_{a\in odd} F_{a,a+1}$ is similar

for odd pairs of patches, $S_e = \bigotimes_{a\in odd} S_{a,a+1}$ shuffles even patches conditional on odd patches, and $C_o = \bigotimes_{a\in odd} C_a$ is a tensor product of Clifford unitaries on odd patches.

As in our discussion of state designs, we make a small change in notation compared to the main text, by replacing the index i for each patch of 2ξ qubits with the index $a, a+1$ labeling two patches of ξ qubits each. The value of ξ is tunable and will depend on the desired n, k, ε of the final unitary design.

In the following subsections, we will prove that the blocked LRFC ensemble forms an approximate unitary design with small measurable error:

Theorem 6 (Blocked LRFC circuits are designs)**.** *The blocked LRFC ensemble is an approximate unitary k-design up to measurable error $\varepsilon = 3nk^2/2^\xi\xi$.*

We describe in detail our approach to proving this result in the remainder of this section; the final proof is found in Section IV E.

From Theorem 6, we can construct approximate unitary designs in nearly optimal depth by drawing each small random function $h_{a,a+1}$ and $f_{a,a+1}$ from a $2k$-wise independent random function on ξ or 2ξ bits, respectively. We will also draw each random unitary C_a from any exact unitary 2-design on ξ qubits. The circuit depth of the resulting unitary ensemble is equal to twice the depth of a 2ξ-bit random function plus twice the depth of a ξ-bit random function plus the depth of a ξ-bit exact unitary 2-design. From our earlier review and analysis (Sections II), this yields designs in the following circuit depths:

Fact 3 (Circuit resources for blocked LRFC circuits)**.** *The k-wise independent blocked LRFC circuit can be implemented with either:*

1. ***Low depth:*** *$\mathcal{O}(\log k \cdot \log \xi)$ depth using $\mathcal{O}(nk \cdot \log \xi \cdot \log\log \xi)$ ancilla qubits.*
2. ***Low ancilla:*** *$\mathcal{O}(k \cdot \log \xi)$ depth using $\mathcal{O}(n \cdot \log \xi \cdot \log\log \xi)$ ancilla qubits.*

Both implementations use $3nk + (5/2)n$ bits of randomness.

Combining Fact 3 and Theorem 6 yields the following:

Corollary 2 (Circuit resources for unitary k-designs)**.** *For any $k^2/\varepsilon \leq 2^n/3$, setting $\xi = \log_2(3nk^2/\varepsilon) \leq n$ yields approximate unitary k-designs with measurable error ε using either:*

- ***Low depth:*** *$\mathcal{O}(\log k \cdot \log\log(nk/\varepsilon))$ depth and $\mathcal{O}(kn \log(nk/\varepsilon) \log\log(nk/\varepsilon))$ ancilla qubits.*
- ***Low ancilla:*** *$\mathcal{O}(k \log\log(nk/\varepsilon))$ depth and $\mathcal{O}(n \log(nk/\varepsilon) \log\log(nk/\varepsilon))$ ancilla qubits.*

The randomness requirement is $3nk + (5/2)n$ bits.

The number of bits of randomness follows because F_e and F_o together use $2nk$ bits of randomness [48]. The shuffles S_e and S_o use nk bits of randomness, since their functions act on half as many bits. Finally, the tensor product of exact unitary 2-designs C uses $(n/2\xi)5\xi = (5/2)n$ bits of randomness [51]. The optimal number of bits of randomness for a unitary k-design is $2nk$ (up to sub-leading additive factors), since applying the Haar twirl to one side of the EPR state yields a mixed state with rank 2^{2nk} (up to sub-leading multiplicative factors). Hence, our ensemble is a mere factor of 3/2 away from optimal in this regard, when k is large.

B. A simple and general approach for bounding the measurable error

As discussed in the main text, to prove Theorem 6, we develop a new and general approach for bounding the measurable error of random unitary ensembles. Our approach provides a convenient alternative to the path-recording framework introduced by [37] (see Section IV H for an expanded comparison). In this subsection, we provide a high-level overview of our approach. We then demonstrate it in full detail in the following subsection, by giving a short self-contained proof that the PFC ensemble has small measurable error. We then apply the same approach to prove that the LRFC and blocked LRFC ensembles have small measurable error as well. Our proofs for the three ensembles are nearly identical to one another, illustrating the versatility of our approach.

Our approach melds and refines ideas from several recent works on pseudorandom states and unitaries [35, 37, 39, 50, 75, 76]. It consists of three key steps:

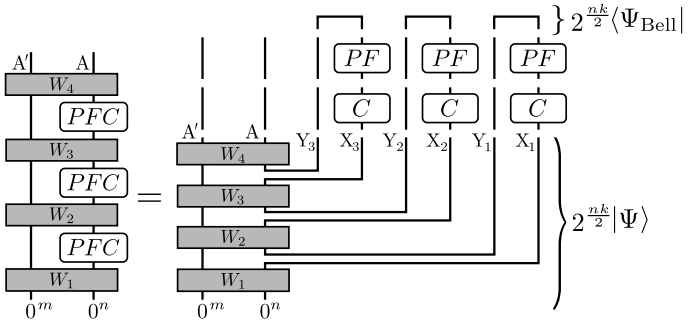

FIG. 4. A visual depiction of our expression Eq. (71) for the output $|\psi_W^U\rangle$ of any quantum experiment querying $U = PFC$. On the left, the unitary acts k times in sequence on an n-qubit register A, interleaved with arbitrary quantum operations, W_j, involving ancilla qubits A'. On the right, X_j denotes the register that the j-th unitary acts on, for $j = 1, \ldots, k$, and Y_j denotes the register that X_j is entangled with in $|\Psi_{\text{Bell}}\rangle$.

1. We first reformulate any quantum experiment involving sequential applications of a random unitary as an experiment involving parallel applications and post-selection [39] (Fig. 4).

2. We then prove that one can insert a projector onto the distinct subspace [35, 75, 76] (or, a local variant of it) in between key components of the parallel random unitaries [35, 37, 50] in the post-selected experiment.

3. We complete the proof by showing that the random unitary ensemble of interest acts identically to a Haar-random unitary on the (local) distinct subspace [35, 37, 50, 75, 76].

Several of these ideas are implicit in the path-recording framework of [37]. We adopt similar notation to [37] to help highlight these connections. At the same time, we deviate from [37] in important ways, including our use of post-selection and the introduction of several simple operator identities that enable a direct analysis.

Let us first discuss Step 1. Following Definition 5, the output state of any experiment querying U can be expressed $W_{k+1}UW_kU\cdots W_2UW_1\,|0^{n+m}\rangle$, where U acts on an n-qubit subsystem A and each W_i acts on an arbitrarily large system AA'. As shown in Fig. 4, we can re-arrange this expression so that the k sequential applications of U act instead as k parallel applications on ancilla qubits. This requires $2k$ new ancilla registers of n qubits each, with one register X_i for each input to a copy of U and one register Y_i for each output. The registers are connected by an initial EPR state (between each Y_i and X_{i+1}) and a final EPR projection (between each X_i and Y_i). The entire reformulation is best viewed in tensor network notation; nonetheless, in equations, we have

$$|\psi_U\rangle = 2^{nk}(\mathbb{1}_{AA'} \otimes \langle\Psi_{\text{Bell}}|_{XY})(\mathbb{1}_{ABY} \otimes \boldsymbol{U}_X)\,|\Psi\rangle_{ABXY}\,, \tag{71}$$

where $|\Psi\rangle$ is an initial state determined by the choice of W_i (see Fig. 4), $\langle\Psi_{\text{EPR}}|$ is the tensor product of k EPR projectors on each X_i and Y_i (with $X \equiv \cup_i X_i$, $Y \equiv \cup_i Y_i$), and $\boldsymbol{U} \equiv U^{\otimes k}$. We suppress the dependence of $|\psi_U\rangle$ and $|\Psi\rangle$ on W for brevity. The reformulation incurs a post-selection overhead of 2^{nk} and hence is not physical. Nonetheless, it is convenient for analysis due to the parallelism in U.

We leave the details of Steps 2 and 3 to the following subsection. For now, we simply recall several definitions. The operator $\Pi_{\text{dist}} = \sum_{x\in\text{dist}} |x\rangle\langle x|$ projects onto the distinct subspace, where $x = (x_1, \ldots, x_k)$ with all x_j distinct. The number $\mathfrak{D} = (2^n)!/(2^n - k + 1)!$ denotes the distinct subspace dimension, $1 - k^2/2^n \leq \mathfrak{D}/2^{nk} \leq 1$.

C. Proof of Theorem 1: The PFC ensemble has small measurable error

Let $\delta = k^2/2^n$, $U = PFC$ and $\boldsymbol{P} \equiv P^{\otimes k}$, $\boldsymbol{F} \equiv F^{\otimes k}$, $\boldsymbol{C} \equiv C^{\otimes k}$. The expected output state is given by

$$\rho = \mathop{\mathbb{E}}_{U\sim PFC}\left[\,|\psi_U\rangle\langle\psi_U|_{AA'}\,\right] = \mathop{\mathbb{E}}_{C}\left[\text{tr}_{XY}\left(B'_{XY}\boldsymbol{C}_X\,|\Psi\rangle\langle\Psi|_{AA'XY}\,\boldsymbol{C}_X^\dagger\right)\right] \tag{72}$$

where $B'_{XY} \equiv 4^{nk}\,\mathbb{E}_{P,F}\left[(\boldsymbol{PF})^\dagger_X\,|\Psi_{\text{Bell}}\rangle\langle\Psi_{\text{Bell}}|_{XY}\,(\boldsymbol{PF})_X\right]$ is the twirled Bell state multiplied by 4^{nk}. We also define an analogous operator $B_{XY} \equiv \sum_{\pi\in S_k} \pi_X \otimes \pi_Y$, where π permutes the k registers of X or Y. (B is equal to the twirl of the Bell state over a Haar-random U up to small relative error [39]; however, we do not use this in our proof.)

Our proof uses five facts. The first two are fundamental and correspond to Steps 3 and 2 in the proof approach overview, respectively. The final three are for technical convenience.

(1.) B' and $(2^{nk}/\mathfrak{D})B$ are equal on the distinct subspace, $B'(\Pi_{\text{dist}} \otimes \Pi_{\text{dist}}) = (2^{nk}/\mathfrak{D})B(\Pi_{\text{dist}} \otimes \Pi_{\text{dist}})$. This follows by expanding the EPR projector as $2^{nk} |\Psi_{\text{Bell}}\rangle\langle\Psi_{\text{Bell}}| (\Pi_{\text{dist}} \otimes \Pi_{\text{dist}}) = \sum_{\tilde{x}} \sum_{x \in \text{dist}} |\tilde{x}, \tilde{x}\rangle\langle x, x|$. The twirl over F yields,

$$\mathop{\mathbb{E}}_{F} \left[\boldsymbol{F} |\tilde{x}, \tilde{x}\rangle\langle x, x| \boldsymbol{F}^\dagger \right] = \mathop{\mathbb{E}}_{f} \left[(-1)^{\sum_i f(\tilde{x}_i) + \sum_i f(x_i)} |\tilde{x}, \tilde{x}\rangle\langle x, x| \right] = \sum_{\pi} \delta_{\tilde{x} = \pi x} \cdot |\pi x, \pi x\rangle\langle x, x| , \tag{73}$$

where $\pi \in S_k$ is any permutation, and we abbreviate $\pi x \equiv (x_{\pi(1)}, \ldots, x_{\pi(k)})$. Note that we can exchange the order of F and P since the average over a random function commutes with any permutation. The condition $\tilde{x} = \pi x$ ensures that $f(\tilde{x}) + f(x) = 0$; otherwise the sign vanishes upon averaging. The remaining average over P yields

$$\mathop{\mathbb{E}}_{P} \left[\boldsymbol{P} |\pi x, \pi x\rangle\langle x, x| \boldsymbol{P}^\dagger \right] = (\pi \otimes \pi) \cdot \mathop{\mathbb{E}}_{P} \left[\boldsymbol{P} |x, x\rangle\langle x, x| \boldsymbol{P}^\dagger \right] = (1/\mathfrak{D}) \sum_{y \in \text{dist}} |\pi y, \pi x\rangle\langle y, x| , \tag{74}$$

since a random permutation maps any distinct bitstring x to a uniformly random distinct bitstring y. Combining these expressions, we have $B'(\Pi_{\text{dist}} \otimes \Pi_{\text{dist}}) = (2^{nk}/\mathfrak{D}) \sum_{x,y \in \text{dist}} |\pi y, \pi x\rangle\langle y, x| = (2^{nk}/\mathfrak{D})B(\Pi_{\text{dist}} \otimes \Pi_{\text{dist}})$ as desired.

(2.) The twirl of Π_{dist} over any 2-design is near the identity, $\left\| \mathbb{1} - \mathbb{E}_C \left[\boldsymbol{C}^\dagger \Pi_{\text{dist}} \boldsymbol{C} \right] \right\|_\infty \leq \delta$ [35]. Intuitively, this follows because C scrambles states into random superpositions of bitstrings, and most bitstrings are distinct. In detail, we can upper bound $\mathbb{1} - \Pi_{\text{dist}} \leq \sum_{1 \leq i < j \leq k} \Pi_{ij}$ where $\Pi_{ij} = \sum_{z \in \{0,1\}^n} |z, z\rangle\langle z, z|$. The twirl over C then yields $\mathbb{E}_C[\boldsymbol{C} \Pi_{ij} \boldsymbol{C}^\dagger] = (\mathbb{1} + \mathcal{S}_{ij})(2^n + 1)$, where $\mathcal{S}_{ij}$ is the swap operator. Hence, the norm is less $\sum_{i<j} \frac{2}{2^n+1} \leq k^2/2^n = \delta$.

(3.) B and B' commute with $\Pi_{\text{dist}} \otimes \mathbb{1}$ and $\mathbb{1} \otimes \Pi_{\text{dist}}$. B also commutes with $\boldsymbol{C}$.

(4.) For any positive semi-definite matrices P, Q, R where P and Q commute, we have $\text{tr}(PQR) \leq \|Q\|_\infty \text{tr}(PR)$. This follows from Holder's inequality, $\text{tr}(PQR) = \text{tr}(Q\sqrt{P}R\sqrt{P}) \leq \|Q\|_\infty \|\sqrt{P}R\sqrt{P}\|_1 = \|Q\|_\infty \text{tr}(PR)$.

(5.) $\text{tr}(B(\mathbb{1} \otimes \Pi_{\text{dist}}) |\Psi\rangle\langle\Psi|) = \mathfrak{D}/2^{nk}$. This is shown below the current proof.

We can now prove the claim. We insert $\mathbb{1} = \Pi_{\text{dist}} \otimes \Pi_{\text{dist}} + (\mathbb{1} - \Pi_{\text{dist}} \otimes \Pi_{\text{dist}})$ to decompose ρ into two terms,

$$\rho = \rho_{\text{dist}} + \delta\rho \equiv \mathop{\mathbb{E}}_{C} \left[\text{tr}_{XY}(B'(\Pi_{\text{dist}} \otimes \Pi_{\text{dist}}) \boldsymbol{C} |\Psi\rangle\langle\Psi| \boldsymbol{C}^\dagger) \right] + \mathop{\mathbb{E}}_{C} \left[\text{tr}_{XY}(B'(\mathbb{1} - \Pi_{\text{dist}} \otimes \Pi_{\text{dist}}) \boldsymbol{C} |\Psi\rangle\langle\Psi| \boldsymbol{C}^\dagger) \right],$$

where each operator acts on the same subsystems as before. We bound the second term as follows,

$$\begin{aligned}
\|\delta\rho\|_1 = \text{tr}(\delta\rho) &= \mathop{\mathbb{E}}_{C} \left[\text{tr}(B'(\mathbb{1} - \Pi_{\text{dist}} \otimes \Pi_{\text{dist}}) \boldsymbol{C} |\Psi\rangle\langle\Psi| \boldsymbol{C}^\dagger) \right] && \text{(since } \delta\rho \text{ is positive)} \\
&= 1 - (2^{nk}/\mathfrak{D}) \text{tr} \left(B \cdot \mathop{\mathbb{E}}_{C} \left[\boldsymbol{C}^\dagger \Pi_{\text{dist}} \boldsymbol{C} \right] \otimes \Pi_{\text{dist}} \cdot |\Psi\rangle\langle\Psi| \right) && \text{(since } \text{tr}(\rho) = 1 \text{ and (1.))} \\
&\leq 1 - (2^{nk}/\mathfrak{D})(1 - \delta) \text{tr} \left(B(\mathbb{1} \otimes \Pi_{\text{dist}}) |\Psi\rangle\langle\Psi| \right) && \text{(from (2.), (3.), (4.))} \\
&= 1 - (2^{nk}/\mathfrak{D})(1 - \delta)(\mathfrak{D}/2^{nk}) = \delta. && \text{(from (5.))}
\end{aligned}$$

Meanwhile, the first term is close to a fixed density matrix ρ_a,

$$\begin{aligned}
\rho_{\text{dist}} &= (2^{nk}/\mathfrak{D}) \text{tr}_{XY} \left(B \cdot \mathop{\mathbb{E}}_{C} \left[\boldsymbol{C}^\dagger \Pi_{\text{dist}} \boldsymbol{C} \right] \otimes \Pi_{\text{dist}} \cdot |\Psi\rangle\langle\Psi| \right) && \text{(from (1.))} \\
&= (2^{nk}/\mathfrak{D}) \text{tr}_{XY} \left(B(\mathbb{1} \otimes \Pi_{\text{dist}}) |\Psi\rangle\langle\Psi| \right) + \Delta \equiv \rho_a + \Delta, && \text{(from (2.), (3.), (4.))}
\end{aligned}$$

where $\|\Delta\|_1 \leq \delta(2^{nk}/\mathfrak{D}) \text{tr}(B(\mathbb{1} \otimes \Pi_{\text{dist}}) |\Psi\rangle\langle\Psi|) = \delta$ from (2.), (3.), (4.), (5.).

This completes the proof: We have $\|\rho - \rho_a\|_1 \leq 2\delta$ when C is drawn from any 2-design. Since both the Clifford and Haar ensembles are 2-designs, we have $\|\rho - \rho_H\|_1 \leq \|\rho_H - \rho_a\|_1 + \|\rho - \rho_a\|_1 \leq 4\delta = 4k^2/2^n$. □

Proof of (5.): We proceed by induction. Let Π^j_{dist} be the distinct subspace projector on $(XY)_{\leq j}$, and $\rho_j = \text{tr}_{AA'(XY)_{>j}}(|\Psi\rangle\langle\Psi|)$ the reduced density matrix. The key property we use is that ρ_j is maximally mixed on Y_j.

Base case ($k = 1$): Here, $B = \mathbb{1} \otimes \mathbb{1}$ and $\Pi_{\text{dist}} = \mathbb{1}$. Hence, $\text{tr}(B(\mathbb{1} \otimes \Pi_{\text{dist}}) |\Psi\rangle\langle\Psi|) = 1$.

Inductive step: We expand $B = \sum_\pi \pi \otimes \pi$ and use the following identity: $\mathrm{tr}_j(\pi \Pi^j_{\mathrm{dist}}) = (2^n - j + 1)\Pi^{j-1}_{\mathrm{dist}}$ if $\pi(j) = j$, and $\mathrm{tr}_j(\pi \Pi^j_{\mathrm{dist}}) = 0$ otherwise. This allows us to trace over Y_j, and, since this enforces $\pi(j) = j$, X_j as well,

$$\sum_{\pi \in S_j} \mathrm{tr}_{(XY)_{\le j}}\big((\pi \otimes \pi)(\mathbb{1} \otimes \Pi^j_{\mathrm{dist}})\rho_j\big) = \frac{2^n - j + 1}{2^n} \sum_{\pi' \in S_{j-1}} \mathrm{tr}_{(XY)_{\le j-1}}\big((\pi' \otimes \pi')(\mathbb{1} \otimes \Pi^{j-1}_{\mathrm{dist}})\rho_{j-1}\big), \tag{75}$$

where π' is π restricted to the first $j-1$ elements. Iterating k times yields $((2^n)!/(2^n - k + 1)!)/2^{nk} = \mathfrak{D}/2^{nk}$. □

D. Proof of Theorem 2: The LRFC ensemble has small measurable error

To adapt our proof to the LRFC ensemble, we will project to slightly smaller subspaces than in the PFC ensemble. We let Π^L_{dist} project to the distinct subspace on the left $n/2$ qubits, and Π^R_{dist} on the right $n/2$ qubits. The left and right distinct subspace have dimensions $\mathfrak{D}_{L,R} = 2^{n/2} \cdot (2^{n/2})!/(2^{n/2} - k + 1)! \ge 2^{nk}(1 - \delta')$ where $\delta' = k^2/\sqrt{2^n}$.

We now proceed similar to PFC. Let $U = S_L S_R F C$ and $\boldsymbol{L} \equiv S_L^{\otimes k}$, $\boldsymbol{R} \equiv S_R^{\otimes k}$, $\boldsymbol{F} \equiv F^{\otimes k}$, $\boldsymbol{C} \equiv C^{\otimes k}$. The expected output state is $\rho = \mathbb{E}_C \mathrm{tr}_{XY}\big(B'' \boldsymbol{C} |\Psi\rangle\langle\Psi| \boldsymbol{C}^\dagger\big)$, where

$$B''_{XY} \equiv 4^{nk} \mathop{\mathbb{E}}_{LRF} \left[(\boldsymbol{LRF})^\dagger_X |\Psi_{\mathrm{Bell}}\rangle\langle\Psi_{\mathrm{Bell}}|_{XY} (\boldsymbol{LRF})_X\right] = 4^{nk} \mathop{\mathbb{E}}_{LRF} \left[(\boldsymbol{FR})^\dagger_X (\boldsymbol{L})^\dagger_Y |\Psi_{\mathrm{Bell}}\rangle\langle\Psi_{\mathrm{Bell}}|_{XY} (\boldsymbol{FR})_X (\boldsymbol{L})_Y\right]. \tag{76}$$

In the second step, we commute F and R, and pull L to the opposite side of the EPR pair using $\boldsymbol{L}_X |\Psi_{\mathrm{Bell}}\rangle = \boldsymbol{L}^T_Y |\Psi_{\mathrm{Bell}}\rangle$ and $L^T = L$, for future convenience. We also define $B_{XY} \equiv \sum_{\pi \in S_k} \pi \otimes \pi$ as before. We again use five facts.

(1'.) B'' and B are equal on the modified distinct subspace, $(\Pi^{LR}_{\mathrm{dist}})_{XY} \equiv (\Pi^L_{\mathrm{dist}})_X \otimes (\Pi^R_{\mathrm{dist}})_Y$. We expand $2^{nk} |\Psi_{\mathrm{Bell}}\rangle\langle\Psi_{\mathrm{Bell}}| (\Pi^{LR}_{\mathrm{dist}})_{XY} = \sum_{\tilde{x}} \sum_{x_L, x_R \in \mathrm{dist}} |\tilde{x}, \tilde{x}\rangle\langle x, x|$, abbreviating $x \equiv x_L \| x_R$. The twirl over F sets $\tilde{x} = \pi x$ for $\pi \in S_k$ as before. Meanwhile, the twirl over L yields

$$\mathop{\mathbb{E}}_L \left[\boldsymbol{L}^\dagger_Y |\pi x, \pi x\rangle\langle x, x| \boldsymbol{L}_Y\right] = (\pi \otimes \pi) \cdot \mathop{\mathbb{E}}_L \left[\boldsymbol{L}^\dagger_Y |x, x\rangle\langle x, x| \boldsymbol{L}_Y\right] = (1/2^{(n/2)k}) \sum_{y_L} |\pi x, \pi(y_L \| x_R)\rangle\langle x, (y_L \| x_R)|, \tag{77}$$

since $y_L \equiv x_L + f_L(x_R)$ is a uniformly random set of k $\frac{n}{2}$-bit strings when x_R is distinct. We can then twirl over R in an identical manner,

$$(\pi \otimes \pi) \cdot \mathop{\mathbb{E}}_R \left[\boldsymbol{R}^\dagger_X |x, (y_L \| x_R)\rangle\langle x, (y_L \| x_R)| \boldsymbol{R}_X\right] = (1/2^{(n/2)k}) \sum_{y_R} |\pi(x_L \| y_R), \pi(y_L \| x_R)\rangle\langle (x_L \| y_R), (y_L \| x_R)|. \tag{78}$$

In total, this shows $B''(\Pi^{LR}_{\mathrm{dist}})_{XY} = \sum_\pi \sum_{x_L, x_R \in \mathrm{dist}} \sum_{y_L, y_R} |\pi(x_L \| y_R), \pi(y_L \| x_R)\rangle\langle (x_L \| y_R), (y_L \| x_R)| = B(\Pi^{LR}_{\mathrm{dist}})_{XY}$.

(2'.) The twirl of $(\Pi^L_{\mathrm{dist}})_X$ over any 2-design is near the identity, $\left\|\mathbb{1} - \mathbb{E}_C \left[\boldsymbol{C}^\dagger \Pi^L_{\mathrm{dist}} \boldsymbol{C}\right]\right\|_\infty \le \delta'$. This follows from a near-identical computation as before.

(3'.) B and B'' commute with $(\Pi^L_{\mathrm{dist}})_Y$ and $(\Pi^R_{\mathrm{dist}})_X$. B also commutes with $\boldsymbol{C}$.

(4.) For any positive semi-definite matrices P, Q, R where P and Q commute, we have $\mathrm{tr}(PQR) \le \|Q\|_\infty \mathrm{tr}(PR)$.

(5'.) $\mathrm{tr}\big(B(\mathbb{1}_X \otimes (\Pi^R_{\mathrm{dist}})_Y) |\Psi\rangle\langle\Psi|\big) = \mathfrak{D}_R/2^{nk}$. This follows from an identical computation as before.

We can now prove the claim. We insert $\mathbb{1} = (\Pi^L_{\mathrm{dist}})_X \otimes (\Pi^R_{\mathrm{dist}})_Y + (\mathbb{1} - (\Pi^L_{\mathrm{dist}})_X \otimes (\Pi^R_{\mathrm{dist}})_Y)$ to decompose ρ,

$$\rho = \rho_{\mathrm{dist}} + \delta\rho \equiv \mathop{\mathbb{E}}_C \left[\mathrm{tr}_{XY}(B''(\Pi^L_{\mathrm{dist}} \otimes \Pi^R_{\mathrm{dist}}) \boldsymbol{C} |\Psi\rangle\langle\Psi| \boldsymbol{C}^\dagger)\right] + \mathop{\mathbb{E}}_C \left[\mathrm{tr}_{XY}(B''(\mathbb{1} - \Pi^L_{\mathrm{dist}} \otimes \Pi^R_{\mathrm{dist}}) \boldsymbol{C} |\Psi\rangle\langle\Psi| \boldsymbol{C}^\dagger)\right],$$

where each operator acts on the same subsystems as before. We bound the second term as follows,

$$\begin{aligned}
\|\delta\rho\|_1 = \mathrm{tr}(\delta\rho) &= \mathop{\mathbb{E}}_C \left[\mathrm{tr}(B''(\mathbb{1} - \Pi^L_{\mathrm{dist}} \otimes \Pi^R_{\mathrm{dist}}) \boldsymbol{C} |\Psi\rangle\langle\Psi| \boldsymbol{C}^\dagger)\right] && \text{(since } \delta\rho \text{ is positive)} \\
&= 1 - \mathrm{tr}\left(B \cdot \mathop{\mathbb{E}}_C \left[\boldsymbol{C}^\dagger \Pi^L_{\mathrm{dist}} \boldsymbol{C}\right] \otimes \Pi^R_{\mathrm{dist}} \cdot |\Psi\rangle\langle\Psi|\right) && \text{(since } \mathrm{tr}(\rho) = 1 \text{ and (1'.))} \\
&\le 1 - (1 - \delta') \mathrm{tr}\left(B(\mathbb{1} \otimes \Pi^R_{\mathrm{dist}}) |\Psi\rangle\langle\Psi|\right) && \text{(from (2'.), (3'.), (4.))} \\
&= 1 - (1 - \delta')(\mathfrak{D}_R/2^{nk}) \le 2\delta'. && \text{(from (5'.))}
\end{aligned}$$

Meanwhile, the first term is close to a fixed density matrix ρ_a,

$$\begin{aligned}\rho_{\text{dist}} &= \operatorname{tr}_{XY}\big(B \cdot \mathop{\mathbb{E}}_{C}\left[\boldsymbol{C}^\dagger \Pi_{\text{dist}}^L \boldsymbol{C}\right] \otimes \Pi_{\text{dist}}^R \cdot |\Psi\rangle\langle\Psi|\big) && \text{(from (1'.))}\\ &= \operatorname{tr}_{XY}\big(B(\mathbb{1}\otimes\Pi_{\text{dist}}^R)|\Psi\rangle\langle\Psi|\big) + \Delta \equiv \rho_a + \Delta, && \text{(from (2'.), (3'.), (4.))}\end{aligned}$$

where $\|\Delta\|_1 \le \delta' \operatorname{tr}\big(B(\mathbb{1}\otimes\Pi_{\text{dist}}^R)|\Psi\rangle\langle\Psi|\big) = \delta'(\mathfrak{D}_R/2^{nk}) \le \delta'$ from (2'.), (3'.), (4.), (5'.).

This completes the proof: We have $\|\rho - \rho_a\|_1 \le 3\delta'$ when C is drawn from any 2-design. Since both the Clifford and Haar ensembles are 2-designs, we have $\|\rho - \rho_H\|_1 \le \|\rho_H - \rho_a\|_1 + \|\rho - \rho_a\|_1 \le 6\delta' = 6k^2/\sqrt{2^n}$. □

E. Proof of Theorem 6: The blocked LRFC circuit has small measurable error

Finally, we can address the blocked LRFC circuit. Similar to our proof of nearly optimal state designs, we will project onto a tensor product of *local* distinct subspaces Π_{dist}^a on each patch a of ξ qubits. Motivated by our analysis of the LRFC ensemble, we will divide these patches into two alternating subsets: even patches, which are shuffled by S_e in the second circuit layer, and odd patches, which are shuffled by S_o in the fifth layer. We let

$$\Pi_{\text{dist}}^{\text{loc}(o)} = \bigotimes_{a\in\text{odd}} \Pi_{\text{dist}}^a \quad \text{and} \quad \Pi_{\text{dist}}^{\text{loc}(e)} = \bigotimes_{a\in\text{even}} \Pi_{\text{dist}}^a \tag{79}$$

denote the local distinct subspace projectors on the odd and even patches, respectively. These will play an analogous role to Π_{dist}^L and Π_{dist}^R in our LRFC proof. The subspaces have dimensions $\mathfrak{D}_e = \mathfrak{D}_o = 2^{(n/2)k}\cdot(\mathfrak{D}_a)^{m/2} \ge 2^{nk}(1 - k^2/2^\xi)^{m/2} \ge 2^{nk}(1-\tilde\delta)$ where $\tilde\delta \equiv (m/2)k^2/2^\xi$, where $\mathfrak{D}_a = (2^\xi)!/(2^\xi - k + 1)!$ is the dimension of each patch.

With this setup in hand, our proof proceeds nearly identically to PFC and LRFC. Let $U = S_o F_o F_e S_e C_e$ and $\boldsymbol{S}_{e,o} \equiv S_{e,o}^{\otimes k}$, $\boldsymbol{F}_{e,o} \equiv F_{e,o}^{\otimes k}$, $\boldsymbol{C}_e \equiv C_e^{\otimes k}$. The expected output is $\rho = \mathbb{E}_C \operatorname{tr}_{XY}\big(\tilde B \boldsymbol{C}|\Psi\rangle\langle\Psi|\boldsymbol{C}^\dagger\big)$, where

$$\tilde B_{XY} \equiv 4^{nk} \mathop{\mathbb{E}}_{LRF}\left[(\boldsymbol{F}_o\boldsymbol{F}_e\boldsymbol{S}_e)_X^\dagger (\boldsymbol{S}_o)_Y^\dagger |\Psi_{\text{Bell}}\rangle\langle\Psi_{\text{Bell}}|_{XY} (\boldsymbol{F}_o\boldsymbol{F}_e\boldsymbol{S}_e)_X (\boldsymbol{S}_o)_Y\right], \tag{80}$$

using a similar manipulation $(\boldsymbol{S}_e)_X|\Psi_{\text{Bell}}\rangle = (\boldsymbol{S}_e)_Y|\Psi_{\text{Bell}}\rangle$ as in the LRFC proof. We define $B_{XY} \equiv \sum_{\pi\in S_k} \pi\otimes\pi$ as before. Our five facts are modified as follows.

(1".) $\tilde B$ and B are equal on the local distinct subspace, $(\Pi_{\text{dist}}^{\text{loc}})_{XY} \equiv (\Pi_{\text{dist}}^{\text{loc}(o)})_X \otimes (\Pi_{\text{dist}}^{\text{loc}(e)})_Y$. To see this, we note that $(\Pi_{\text{dist}}^{\text{loc}(o)})_X$ commutes with $(\boldsymbol{F}_e\boldsymbol{F}_o\boldsymbol{S}_o)_X$ and $(\Pi_{\text{dist}}^{\text{loc}(e)})_Y$ commutes with $(\boldsymbol{S}_e)_Y$. We can then expand $2^{nk}|\Psi_{\text{Bell}}\rangle\langle\Psi_{\text{Bell}}|(\Pi_{\text{dist}}^{\text{loc}})_{XY} = \sum_{\tilde x}\sum_{x\in\text{loc-dist}}|\tilde x,\tilde x\rangle\langle x,x|$, where the sum is over x that are distinct on every patch.

Let us first analyze the twirl over F_e and F_o. The key result is that this is equivalent to the twirl over an n-qubit random function, when restricted to the local distinct subspace:

$$\mathop{\mathbb{E}}_{F}\left[\boldsymbol{F}|\tilde x,\tilde x\rangle\langle x,x|\boldsymbol{F}^\dagger\right] = \mathop{\mathbb{E}}_{f_{a,a+1}\,\forall a}\left[(-1)^{\sum_{j,a} f_{a,a+1}(\tilde x_{a,a+1}^{(j)}) + \sum_{j,a} f_{a,a+1}(x_{a,a+1}^{(j)})}|\tilde x,\tilde x\rangle\langle x,x|\right] = \sum_\pi \delta_{\tilde x=\pi x}\cdot|\pi x,\pi x\rangle\langle x,x|\,. \tag{81}$$

For comparison, see Eq. (73) for the twirl over an n-qubit random function. Here, $x_{a,a+1}^{(j)}$ denotes the support of the j-th bitstring on patches $a, a+1$, and the sum runs over all patches $a = 1,\dots,m$. The random functions $f_{a,a+1}$ for even a come from F_e and for odd a from F_o. The average over each random function forces $\tilde x$ and x to be permutations of one another within each pair of nearest-neighbor patches, $\tilde x_{a,a+1}^{(j)} = \pi_a x_{a,a+1}^{(j)}$. This is equivalent to $\tilde x_a^{(j)} = \pi_a x_a^{(j)}$ and $\tilde x_{a+1}^{(j)} = \pi_a x_{a+1}^{(j)}$ for each a. However, since each x^a is distinct, this can be true only if $\pi_{a-1} = \pi_a$ for every a. This implies that *all* the permutations are in fact equal, $\pi_a = \pi_1 \equiv \pi$ for all a, which yields the final expression.

We can now turn to the twirl over S_e and S_o. The key result is that these twirls send each local distinct bitstring x to a uniformly random bitstring y. Together with Eq. (81), this implies that the blocked LRF circuit acts identically to a global n-qubit LRF circuit, when restricted to the local distinct subspace. We begin with S_o:

$$(\pi\otimes\pi)\cdot\mathop{\mathbb{E}}_{S_o}\left[(\boldsymbol{S}_o)_Y^\dagger|x,x\rangle\langle x,x|(\boldsymbol{S}_o)_Y\right] = (1/2^{(n/2)k})\sum_{y_o}|\pi x,\pi(y_o\|x_e)\rangle\langle x,(y_o\|x_e)|\,,$$

since $y_o \equiv \bigotimes_{a\in\text{odd}}(x_a + h_{a,a+1}(x_{a+1}))$ is a uniformly random set of k $\frac{n}{2}$-bit strings when each x_{a+1} is distinct. Here, we let x_e denote the concatenation of all bitstrings on even patches, and x_o the concatenation on all odd patches,

$x \equiv x_o \| x_e$. We can now twirl over S_e in an identical manner,

$$(\pi \otimes \pi) \cdot \mathop{\mathbb{E}}_{S_e} \left[(\boldsymbol{S}_e)^\dagger_X \left| \pi x, \pi(y_o \| x_e) \right\rangle\!\left\langle x, (y_o \| x_e) \right| (\boldsymbol{S}_e)_X \right] = (1/2^{(n/2)k}) \sum_{y_e} \left| \pi(x_o \| y_e), \pi(y_o \| x_e) \right\rangle\!\left\langle (x_o \| y_e), (y_o \| x_e) \right|,$$

where $y_e \equiv \bigotimes_{a \in \text{even}} (x_a + h_{a,a+1}(x_{a+1}))$ is again uniformly random since each x_{a+1} is distinct. In total, this shows $B''(\Pi^{\text{loc}}_{\text{dist}})_{XY} = \sum_\pi \sum_{x_o, x_e \in \text{loc-dist}} \sum_{y_o, y_e} \left| \pi(x_o \| y_e), \pi(y_o \| x_e) \right\rangle\!\left\langle (x_o \| y_e), (y_o \| x_e) \right| = B(\Pi^{\text{loc-dist}}_{\text{dist}})_{XY}$, as desired.

(2".) The twirl of $(\Pi^{\text{loc}(o)}_{\text{dist}})_X$ over a tensor product of local 2-designs is near identity, $\left\| \mathbb{1} - \mathbb{E}_C \left[\boldsymbol{C}_e^\dagger \Pi^{\text{loc}(o)}_{\text{dist}} \boldsymbol{C}_e \right] \right\|_\infty \le \tilde{\delta}$. This also holds for the twirl over any ensemble that is invariant under composition with local 2-designs (such as a Haar-random unitary on all n qubits).

To show this, we can upper bound $\mathbb{1} - \Pi^{\text{loc}(o)}_{\text{dist}} \le \sum_{a \in \text{odd}} \sum_{1 \le i < j \le k} \Pi^a_{ij}$ where $\Pi^a_{ij} = \sum_{z_a \in \{0,1\}^\xi} |z_a, z_a\rangle\!\langle z_a, z_a|$. The twirl obeys $0 \preceq \mathbb{E}_C[\boldsymbol{C} \Pi^a_{ij} \boldsymbol{C}^\dagger] \preceq 2/(2^\xi + 1)$. Hence, the norm is less $\sum_a \sum_{i<j} \frac{2}{2^n+1} \le (m/2)k^2/2^n = \tilde{\delta}$.

(3".) B and $\tilde{B}$ commute with $(\Pi^{\text{loc}(e)}_{\text{dist}})_Y$ and $(\Pi^{\text{loc}(o)}_{\text{dist}})_X$. B also commutes with $\boldsymbol{C}$.

(4.) For any positive semi-definite matrices P, Q, R where P and Q commute, we have $\operatorname{tr}(PQR) \le \|Q\|_\infty \operatorname{tr}(PR)$.

(5".) $\operatorname{tr}\Big(B(\mathbb{1}_X \otimes (\Pi^{\text{loc}(e)}_{\text{dist}})_Y) \left| \Psi \right\rangle\!\left\langle \Psi \right| \Big) = \mathfrak{D}_e / 2^{nk}$. This again follows from an identical computation as before.

The remainder of the proof is identical to the LRFC ensemble. We insert $\mathbb{1} = (\Pi^{\text{loc}(o)}_{\text{dist}})_X \otimes (\Pi^{\text{loc}(e)}_{\text{dist}})_Y + (\mathbb{1} - (\Pi^{\text{loc}(o)}_{\text{dist}})_X \otimes (\Pi^{\text{loc}(e)}_{\text{dist}})_Y)$ to decompose ρ into two terms,

$$\rho = \rho_{\text{dist}} + \delta\rho \equiv \mathop{\mathbb{E}}_C \left[\operatorname{tr}_{XY} (\tilde{B}(\Pi^{\text{loc}(o)}_{\text{dist}} \otimes \Pi^{\text{loc}(e)}_{\text{dist}}) \boldsymbol{C} \left| \Psi \right\rangle\!\left\langle \Psi \right| \boldsymbol{C}^\dagger) \right] + \mathop{\mathbb{E}}_C \left[\operatorname{tr}_{XY} (\tilde{B}(\mathbb{1} - \Pi^{\text{loc}(o)}_{\text{dist}} \otimes \Pi^{\text{loc}(e)}_{\text{dist}}) \boldsymbol{C} \left| \Psi \right\rangle\!\left\langle \Psi \right| \boldsymbol{C}^\dagger) \right].$$

We bound the second term via

$$\begin{aligned}
\|\delta\rho\|_1 = \operatorname{tr}(\delta\rho) &= \mathop{\mathbb{E}}_C \left[\operatorname{tr}(B''(\mathbb{1} - \Pi^{\text{loc}(o)}_{\text{dist}} \otimes \Pi^{\text{loc}(e)}_{\text{dist}}) \boldsymbol{C} \left| \Psi \right\rangle\!\left\langle \Psi \right| \boldsymbol{C}^\dagger) \right] && \text{(since } \delta\rho \text{ is positive)} \\
&= 1 - \operatorname{tr}\left(B \cdot \mathop{\mathbb{E}}_C \left[\boldsymbol{C}^\dagger \Pi^{\text{loc}(o)}_{\text{dist}} \boldsymbol{C} \right] \otimes \Pi^{\text{loc}(e)}_{\text{dist}} \cdot \left| \Psi \right\rangle\!\left\langle \Psi \right| \right) && \text{(since } \operatorname{tr}(\rho) = 1 \text{ and (1".))} \\
&\le 1 - (1 - \tilde{\delta}) \operatorname{tr}\left(B(\mathbb{1} \otimes \Pi^{\text{loc}(e)}_{\text{dist}}) \left| \Psi \right\rangle\!\left\langle \Psi \right| \right) && \text{(from (2".), (3".), (4.))} \\
&= 1 - (1 - \tilde{\delta})(\mathfrak{D}_e / 2^{nk}) \le 2\tilde{\delta}. && \text{(from (5".))}
\end{aligned}$$

Meanwhile, the first term is close to a fixed density matrix ρ_a,

$$\begin{aligned}
\rho_{\text{dist}} &= \operatorname{tr}_{XY}\left(B \cdot \mathop{\mathbb{E}}_C \left[\boldsymbol{C}^\dagger \Pi^{\text{loc}(o)}_{\text{dist}} \boldsymbol{C} \right] \otimes \Pi^{\text{loc}(e)}_{\text{dist}} \cdot \left| \Psi \right\rangle\!\left\langle \Psi \right| \right) && \text{(from (1".))} \\
&= \operatorname{tr}_{XY}\left(B(\mathbb{1} \otimes \Pi^{\text{loc}(e)}_{\text{dist}}) \left| \Psi \right\rangle\!\left\langle \Psi \right| \right) + \Delta \equiv \rho_a + \Delta, && \text{(from (2".), (3".), (4.))}
\end{aligned}$$

where $\|\Delta\|_1 \le \delta' \operatorname{tr}\Big(B(\mathbb{1} \otimes \Pi^{\text{loc}(e)}_{\text{dist}}) \left| \Psi \right\rangle\!\left\langle \Psi \right| \Big) = \delta'(\mathfrak{D}_R e 2^{nk}) \le \tilde{\delta}$ from (2".), (3".), (4.), (5".).

This completes the proof: We have $\|\rho - \rho_a\|_1 \le 3\tilde{\delta}$ when C is drawn from any 2-design. Since both the Clifford and Haar ensembles are 2-designs, we have $\|\rho - \rho_H\|_1 \le \|\rho_H - \rho_a\|_1 + \|\rho - \rho_a\|_1 \le 6\tilde{\delta} = 3mk^2/2^\xi$. □

F. Second approach to nearly optimal unitary designs via unitary-function gluing lemma

It is possible to arrive at a similar construction and error bound by gluing together designs on different subsystems using only phase gates, similar to the approach in Sec. III. This construction achieves the same scaling in n and k, but uses a different analysis technique.

We consider a modified low-depth variant of the LRFC ensemble in which left- and right-shuffle, phase, and Clifford operators are applied to each of the even patches, then an additional layer of random phases are applied to the odd patches:

Definition 15 (Second blocked LRFC ensemble)**.** *Consider a system of n qubits divided into nearest-neighbor patches of ξ qubits each (Fig. 1). For each patch a, suppose $h_{a,a+1}$ is drawn uniformly randomly from functions on $\{0,1\}^\xi \to \{0,1\}^\xi$, and $f_{a,a+1}$ is drawn uniformly randomly from binary functions on $\{0,1\}^{2\xi} \to \{0,1\}$. Also, for each odd a, suppose C_a is drawn uniformly randomly from the Clifford group on ξ qubits. Then the low-depth Luby-Rackoff-Function-Clifford (LRFC) ensemble is given by the family of n-qubit random unitaries:*

$$U = F_e \cdot S_o \cdot S_o \cdot F_o \cdot C_o, \tag{82}$$

where $F_o = \bigotimes_{a\in odd} F_{a,a+1}$, $L_o = \bigotimes_{a\in odd} R_{a,a+1}$, $R_o = \bigotimes_{a\in odd} R_{a,a+1}$, and $C_o = \bigotimes_{a\in odd} C_a$ are tensor products of unitary operators acting on the odd pairs of patches, similar to Def. 14, while F_e is a tensor product of phase operators acting on the even pairs of patches.

We proceed to formulate a similar gluing bound as in the state case, in which we obtain an error which scales with the number of blocks, as well as inversely exponential in the number of qubits in the patch. Plugging in the circuit implementations of the k-wise independent functions again yields a depth which is doubly logarithmic in system size.

Lemma 12 (Gluing unitary designs with phase operators)**.** *Let $|A|, |B| \geq \xi$ and $k < 2^\xi$. Suppose $\mathcal{E}_A, \mathcal{E}_B$ are ε_A- and ε_B-approximate k-designs on A and B, respectively, up to measurable error. Then the ensemble formed by applying a random phase operator F_α on ξ qubits each of A and of B is an ε-approximate k-design with measurable error*

$$\varepsilon = \varepsilon_A + \varepsilon_B + \mathcal{O}(k^2/2^\xi). \tag{83}$$

Proof. Let $\mathcal{E}_{FAB}$ and $\mathcal{E}_F$ denote the unitary ensembles generated by applying random phase operators on overlapping blocks with unitaries sampled from $\mathcal{E}_A, \mathcal{E}_B$ and with Haar-random unitaries on A, B, respectively. Then for any choice of $W_1, W_2, \cdots, W_{k+1}$ we have that

$$\begin{aligned} \|\rho_{\mathcal{E}_{FAB}} - \rho_H\|_1 &\leq \|\rho_{\mathcal{E}_{FAB}} - \rho_{\mathcal{E}_\mathcal{F}}\|_1 + \|\rho_{\mathcal{E}_\mathcal{F}} - \rho_H\|_1 \\ &\leq \varepsilon_A + \varepsilon_B + \|\rho_{\mathcal{E}_\mathcal{F}} - \rho_H\|_1, \end{aligned} \tag{84}$$

where in the second step we have used both the assumption on $\mathcal{E}_A, \mathcal{E}_B$ as well as the fact that the action of any instance of a random phase operator can be absorbed into the following W_i. To analyze the second term, we rewrite the output state in the form

$$\rho_{\mathcal{E}_\mathcal{F}} = \mathop{\mathbb{E}}_{U_A, U_B \sim H} \left[\mathrm{tr}_{XY}\, \mathcal{F} (U_A \otimes U_B)^{\otimes k} |\Psi_W\rangle\langle\Psi_W| (U_A^\dagger \otimes U_B^\dagger)^{\otimes k} \right], \tag{85}$$

where $\mathcal{F}$ is the unnormalized Bell state twirled over the random phases. Recall that the twirl over F eliminates terms which are not of form $|\pi(xx')\rangle\langle xx'|_{\Xi_A \Xi_B}$. We again consider a projection onto both of the local distinct subspaces corresponding to Ξ_A and Ξ_B, the regions which the phase operator acts on:

$$\begin{aligned} (\rho_{\mathcal{E}_\mathcal{F}})_{\mathrm{dist}} &= \left[\Pi_{\mathrm{dist}}^{\Xi_A} \otimes \Pi_{\mathrm{dist}}^{\Xi_B}\right] \Psi_{\mathcal{E}_\mathcal{F}} \left[\Pi_{\mathrm{dist}}^{\Xi_A} \otimes \Pi_{\mathrm{dist}}^{\Xi_B}\right] \\ &= \mathop{\mathbb{E}}_{U_A, U_B \sim H} \left[\mathrm{tr}_{XY}\, \mathcal{F} \left[\Pi_{\mathrm{dist}}^{\Xi_A} \otimes \Pi_{\mathrm{dist}}^{\Xi_B}\right] (U_A \otimes U_B)^{\otimes k} |\Psi_W\rangle\langle\Psi_W| (U_A^\dagger \otimes U_B^\dagger)^{\otimes k} \left[\Pi_{\mathrm{dist}}^{\Xi_A} \otimes \Pi_{\mathrm{dist}}^{\Xi_B}\right] \right] \\ &= \mathop{\mathbb{E}}_{U_A, U_B \sim H} \left[\mathrm{tr}_{XY}\, \mathcal{F} (U_A^\dagger \otimes U_B^\dagger)^{\otimes k} \left[\Pi_{\mathrm{dist}}^{\Xi_A} \otimes \Pi_{\mathrm{dist}}^{\Xi_B}\right] (U_A \otimes U_B)^{\otimes k} |\Psi_W\rangle\langle\Psi_W| \right], \end{aligned} \tag{86}$$

where we have used the fact that the restrictions of the symmetric subspace commute with each other and with the $U_A \otimes U_B$, similar to Sec. IV C. We then observe that the twirl on the restricted subspace is the same as the restriction of the Haar twirl over the entire system:

$$\mathop{\mathbb{E}}_{U_A, U_B} \mathcal{F} (U_A^\dagger \otimes U_B^\dagger)^{\otimes k} \left[\Pi_{\mathrm{dist}}^{\Xi_A} \otimes \Pi_{\mathrm{dist}}^{\Xi_B}\right] (U_A \otimes U_B)^{\otimes k} = \mathop{\mathbb{E}}_{U_{AB} \sim H} \mathcal{F} (U_{AB}^\dagger)^{\otimes k} \left[\Pi_{\mathrm{dist}}^{\Xi_A} \otimes \Pi_{\mathrm{dist}}^{\Xi_B}\right] U_{AB}^{\otimes k}. \tag{87}$$

Applying the same argument as in Eq. 68 of the proof of Lemma 11 to bound the dimension of the local distinct subspace, and using the fact that the trace norm is monotonic under physical operations, yields

$$\|(\rho_{\mathcal{E}_\mathcal{F}})_{\mathrm{dist}} - \rho_H\|_1 \leq k^2/2^\xi. \tag{88}$$

To finish the proof, we bound the difference between the terms

$$\begin{aligned}\left\|\rho_{\mathcal{E}_{\mathcal{F}}}-(\rho_{\mathcal{E}_{\mathcal{F}}})_{\text{dist}}\right\|_1 &= \mathop{\mathbb{E}}_{U_A,U_B\sim H}\operatorname{tr}\left[\mathcal{F}(U_A\otimes U_B)^{\otimes k}\left[\mathbb{1}-\left(\Pi_{\text{dist}}^{\Xi_A}\otimes\Pi_{\text{dist}}^{\Xi_B}\right)\right](U_A^\dagger\otimes U_B^\dagger)^{\otimes k}|\Psi_W\rangle\langle\Psi_W|\right]\\ &= 1-\operatorname{tr}\left(\rho_{\mathcal{E}_{\mathcal{F}}}\right)_{\text{dist}} = 1-\operatorname{tr}\left(\Pi_{\text{dist}}^{\Xi_A}\otimes\Pi_{\text{dist}}^{\Xi_B}\right)\Psi_H\\ &\leq k^2/2^\xi,\end{aligned} \tag{89}$$

Collecting error terms up to leading order in k,ξ yields the bound in Eq. 83. □

Applying this gluing formula repeatedly for each additional block in the system yields the following bound for the blocked LRFC construction:

Theorem 7 (Second blocked LRFC is a design)**.** *Let $\mathcal{E}_{n,\xi}$ be the family of blocked k-wise independent LRFC circuits on n qubits with blocks of size $\xi\leq n$. Then $\mathcal{E}_{n,\xi}$ forms an ε-approximate k-design with*

$$\varepsilon=\mathcal{O}(nk^2/2^\xi\xi). \tag{90}$$

Proof. From Lemma 7, applying the initial layers of Clifford, right shuffle, phase, and left shuffle gates yields approximate k-designs on each block, up to error $\mathcal{O}(k^2/2^\xi)$. The result follows by starting from the leftmost block and repeatedly applying the result of Lemma 7 after adding of the additional $n/2\xi-1$ blocks. □

As a corollary, we immediately obtain the same scaling as the main result of this section:

Corollary 3 (Unitary designs in $\log k\log\log nk/\varepsilon$ depth)**.** *Let $\mathcal{E}_n$ be an ensemble of k-wise independent blocked LRFC circuits on n qubits with block size $\xi=\mathcal{O}(\log n)$. Then $\mathcal{E}_n$ is an ε-approximate design with $\varepsilon=\mathcal{O}(nk^2/2^\xi\xi)$. In addition, each $U\sim\mathcal{E}_n$ can be implemented with a circuit of depth $\mathcal{O}(\log k\cdot\log\log nk/\varepsilon)$ with $k\cdot\tilde{\mathcal{O}}(n)$ ancillas.*

Proof. This follows from substituting the constructions in Lemma 10 and [51] for k-wise independent functions and exact unitary 2-designs, respectively, into the result of Theorem 7, then choosing fixed $\varepsilon>0$ and letting $\xi=\mathcal{O}(\log n)$ for large n. □

G. Third approach to nearly optimal unitary designs via relative error gluing lemma

Here, we present a formal proof of the alternative construction of unitary k-designs discussed in the main text, which builds heavily on the existing results of [39] and [50]. The unitary ensemble corresponds to a two-layer circuit in which each small random unitary is drawn randomly from the LRFC ensemble on 2ξ qubits.

Definition 16 (Third blocked LRFC ensemble)**.** *Consider a system of n qubits divided into patches of size ξ. Then the third LRFC ensemble is given by the family of n-qubit random unitaries:*

$$U=(LRFC)_e\cdot(LRFC)_o, \tag{91}$$

where $(LRFC)_e$ and $(LRFC)_o$ are tensor products of unitaries drawn from the LRFC ensemble on even and odd pairs of patches, respectively.

Since the unitaries applied in each of the patches for both layers is drawn from an approximate design, it is possible to show that this construction also forms a design by applying the relative error gluing result (Theorem 1 of [39]) to neighboring patches:

Theorem 8 (Third blocked LRFC is a design)**.** *The third blocked LRFC ensemble on n qubits forms an approximate unitary k-design with measurable error $\mathcal{O}(nk^2/2^\xi)$.*

Proof. From Theorem 2, the LRFC ensemble on each individual patch forms an approximate k-design up to measurable error $\mathcal{O}(k^2/2^\xi)$. Hence, the third blocked LRFC ensemble is indistinguishable from the blocked Haar-random circuit up to measurable error $nk^2/2^\xi\xi$. From Theorem 1 of [39]), the blocked Haar-random circuit is a unitary k-design with relative error $nk^2/2^\xi$. This implies that it is a design with measurable error $2nk^2/2^\xi$ (Lemma 4). □

H. Application to pseudorandom unitaries

As previously discussed in the case of state designs, our simple constructions and proofs of random unitary ensembles with small measurable error also have application to the study of pseudorandom unitaries (PRUs). A PRU is a unitary ensemble that is indistinguishable from Haar-random by any bounded-time quantum experiment. We refer again to Refs. [37, 39] for a pedagogical introduction.

The existence of pseudorandom unitaries has remained an open question until very recently. This was resolved by [37], which proved that the PFC ensemble forms a PRU whenever P and F are instantiated with a pseudorandom permutation (PRP) [77] and pseudorandom function (PRF) [49]. This built upon earlier work, which introduced the PFC ensemble and proved that it formed a PRU with a weaker parallel form of security [35]. Following this progress, the LRFC ensemble was introduced and also proven to form a PRU when each function is pseudorandom [50].

So far, both proofs of the existence of PRUs (for the PFC ensemble [37] and the LRFC ensemble [50]) work within the so-called path-recording framework introduced by [37]. Once instantiated, this framework is quite powerful. For example, it allows one to prove that (slight variants of) the PFC and LRFC ensembles are secure even against adversaries that can query both a random unitary U and its inverse $U^\dagger$ many times. Such experiments are much more powerful than standard experiments that only query U [39, 78, 79]. At the same time, however, the path-recording framework can yield somewhat lengthy proofs. This arises both from a large amount of initial notation, and the repeated manipulation of large sums of bitstrings throughout the analysis. Given the fundamental importance of PRUs, one might wonder whether a more direct proof is possible.

This is in fact provided by our work. Our proofs that the PFC, LRFC, and blocked LRFC ensembles have small measurable error immediately imply that each ensemble is a PRU (when its functions and permutations are instantied pseudorandomly). By definition, a PRP and PRF are indistinguishable from a truly random permutation and function by any bounded-time experiment. Our analysis then proves that the truly random ensembles are indistinguishable from Haar-random unitaries. Together, this implies that the pseudorandom ensembles are each PRUs. Our proofs for each ensemble are extremely short and direct (see Sections IV C, IV D, and IV E). They are also self-contained, relying only on basic properties of unitary 2-designs and the permutation group. We hope that this alternative approach can complement existing methods for future work on PRUs and unitary designs.

V. UNITARY DESIGNS WITH SMALL RELATIVE ERROR

In this section, we present a variant of the blocked LRFC circuit that forms an approximate unitary k-design with small relative error. The circuit has depth $\mathcal{O}(k \log k \log\log nk/\varepsilon)$, which is larger by only a factor of k compared to our earlier results. As aforementioned, the best previous construction of unitary designs with relative error required circuit depths $\mathcal{O}(k \operatorname{poly}\log k \log nk/\varepsilon)$ [38, 39]. This features an exponentially worse scaling in the number of qubits n and the inverse error $1/\varepsilon$ compared to our new results. In what follows, we first describe our construction and then provide a proof that it achieves small relative error.

A. Blocked amplified LRFC circuits

To describe our relative error unitary ensemble, consider the circuit formed by applying p independently random LRFC unitaries on the same 2ξ qubits in succession. We term this the $(\text{LRFC})^p$ ensemble. Our relative error unitary ensemble corresponds to the two-layer circuit in which each block is drawn independently randomly from the $(\text{LRFC})^p$ ensemble on 2ξ qubits.

Definition 17 (Blocked amplified LRFC circuit)**.** *Consider a system of n qubits divided into patches of size ξ. The p-layer blocked amplified LRFC circuit is given by the family of n-qubit random unitaries:*

$$U = (LRFC)_e^p (LRFC)_o^p, \tag{92}$$

where $(LRFC)_e^p$ is a tensor product of $(LRFC)^p$ random unitaries on every even patch of qubits, and $(LRFC)_o^p$ is a tensor product of $(LRFC)^p$ random unitaries on every old patch of qubits.

The "amplification" in the name of our ensemble comes from the *amplification of approximation error* result for unitary designs [32], which states that the additive error decreases multiplicatively when designs are composed. For completeness, we reproduce the result in the following subsection, before using it to show that the blocked amplified LRFC ensemble is a relative error design for $p = \mathcal{O}(k)$ and $\xi \leq n/2$:

Theorem 9 (Blocked amplified LRFC circuits are relative error designs)**.** *For any $k \leq 2^{\xi/4}$ and $p \geq 8k+1$. The (LRFC)^p ensemble forms an approximate unitary k-design on n qubits with relative error $\varepsilon = \mathcal{O}(nk^2/2^\xi)$.*

The circuit depth of this construction is p times the depth of the original blocked LRFC construction from Fact 3:

Fact 4 (Circuit depth of blocked amplified LRFC circuit)**.** *The blocked amplified LRFC circuit can be implemented in depth $\mathcal{O}(p \cdot \log k \cdot \log \xi)$.*

Hence, by taking $p = 8k+1$ and $\xi = \mathcal{O}(nk^2/\varepsilon)$, we can achieve approximate unitary k-designs with relative error ε in depth $\mathcal{O}(k \cdot \log k \cdot \log\log(nk/\varepsilon))$. This improves the scalings with n and ε compared to known results [38, 39].

B. Proof of Theorem 9: The blocked amplified LRFC ensemble has small relative error

Our proof is extremely short. From Lemma 13 and Lemma 14 below, the (LRFC)^p circuit on 2ξ qubits forms a design with relative error $\varepsilon = 2k^2/2^\xi$ for $p \geq 8k+1$. We then apply the relative error gluing lemma (Theorem 1 of [39]) to obtain a design on n qubits with relative error $(n/\xi)2k^2/2^\xi + nk^2/2^\xi$. This completes the proof. □

Lemma 13 (Error decays)**.** *If $\Phi_\mathcal{E}$ has additive error ε, then $\Phi_\mathcal{E} \circ \Phi_\mathcal{E}$ has additive error at most ε^2.*

Proof. We write $\Phi_\mathcal{E} = \Phi_H + \delta\Phi$, where $\Phi_H \circ \delta\Phi = \delta\Phi \circ \Phi_H = 0$ by definition. Squaring gives, $\Phi_\mathcal{E} \circ \Phi_\mathcal{E} = \Phi_H + \delta\Phi \circ \delta\Phi$. By assumption, we have $\|\delta\Phi(\rho)\|_1 \leq \varepsilon$ for any ρ. We can break $\delta\Phi(\rho) = \rho_+ - \rho_-$ into a positive and negative part, which have normalizations $\varepsilon_\pm \equiv \|\rho_\pm\|_1 = \mathrm{tr}(\rho_\pm)$. Since ρ_+ and ρ_- have support on orthogonal subspaces, we have $\varepsilon_+ + \varepsilon_- = \|\delta\Phi(\rho)\|_1 \leq \varepsilon$ from our previous bound. To proceed, we write $\delta\Phi(\delta\Phi(\rho)) = \delta\Phi(\rho_+) - \delta\Phi(\rho_-)$. Since $\rho_\pm$ are positive density matrices with traces $\varepsilon_\pm$, we have $\|\delta\Phi(\rho_\pm)\|_1 \leq \varepsilon\|\rho_\pm\|_1 = \varepsilon\varepsilon_\pm$. This yields $\|\delta\Phi(\delta\Phi(\rho))\|_1 \leq \varepsilon(\varepsilon_+ + \varepsilon_-) \leq \varepsilon^2$, which completes the proof. □

Lemma 14 (Amplification)**.** *For any $k \leq 2^{n/8}$ and $p \geq 8k+1$. The* (LRFC)^p *ensemble is an approximate unitary k-design with relative error $\varepsilon = 2k^2/\sqrt{2^n}$.*

Proof. From Theorem 2, the LRFC ensemble forms an approximate unitary k-design with additive error $4k^2/2^{n/2}$. Iterating Lemma 13 $p-1$ times, we find that the p-th composition of the LRFC ensemble with itself forms an approximate unitary k-design with additive error $\varepsilon_{\mathrm{add}} = (k^2/2^{n/2})^p$. From Lemma 5, any approximate unitary k-design with additive error $\varepsilon_{\mathrm{add}}$ is also an approximate unitary k-design with *relative* error $\varepsilon = (4^{nk}/k!)(1+k^2/2^n)\varepsilon_{\mathrm{add}}$. Setting $p \geq 8k+1$ and using $k! \geq 1$ yields $\varepsilon \leq 4^{nk}(1+k^2/2^n)(k^{16k+2}/4^{2nk+n/4}) = (k^2/\sqrt{2^n})(1+k^2/2^n)(k^8/2^n)^{2k}$. When $k \leq 2^{n/8}$, the final term is less than one and the second term is less than two. □

VI. IMPROVED LOWER BOUNDS ON STATE AND UNITARY DESIGNS

In this section, we provide the proof of our improved lower bounds on the circuit depths required for state and unitary designs. The full statement of our theorem is as follows.

Theorem 10. (Lower bound for state and unitary designs with additive error) *For any $1 < k = o(2^n)$. Any random state or unitary ensemble over n qubits that forms a k-design with additive error ε requires circuit depth at least:*

- $d = \Omega(k + \log n/\varepsilon)$*, for 1D circuits with $\mathcal{O}(n)$ ancilla qubits and $d = o(n)$,*
- $d = \Omega(k + \log\log n/\varepsilon)$*, for all-to-all circuits with $\mathcal{O}(n)$ ancilla qubits and $d = o(\log n)$.*
- $d = \Omega(\log k + \log\log n/\varepsilon)$*, for all-to-all circuits with any number of ancilla qubits and $d = o(\log n)$.*

We assume that every all-to-all circuit in the ensemble has the same architecture. The restriction to $k = o(2^n)$ is necessary since the a Haar-random unitary forms an exact k-design for any k and can be compiled in depth $\mathcal{O}(2^{2n})$ in any circuit geometry [32]. The restriction to $d = o(n)$ (in 1D) and $d = o(\log n)$ (in all-to-all systems) is necessary since the Clifford group forms an exact unitary 3-design and can be compiled in depth $\mathcal{O}(n)$ in 1D and $\mathcal{O}(\log n)$ in all-to-all circuits.

Before providing the proof of Theorem 10, let us first review the best known previous lower bounds for state and unitary designs. For clarity, we provide separate discussions regarding the dependence on each of k, n, and ε.

- For the k-dependence, the best existing lower bound is Proposition 8 of Ref. [32], which states that any additive error state or unitary design requires a circuit of size at least $\Omega(nk/(\log nk))$. This lower bound is widely believed to be optimal, and has been proven to be optimal up to poly-logarithmic factors [34].

  Our lower bound on the k-dependence simply re-phrases this known lower bound on the circuit size in terms of the circuit depth. We provide full details in our proof below.

- For the n-dependence, the only existing lower bound is Proposition 1 of Ref. [39]. This applies to state/unitary designs with relative error, and yields depth lower bounds of $d = \Omega(\log n)$ in 1D circuits and $d = \Omega(\log \log n)$ in all-to-all connected circuits. No lower bound existed for state/unitary designs with additive error.

  To this end, the primary achievement of our lower bounds is to show that these same circuit depths are also needed for designs with additive error, and not just relative error. This extension is highly non-trivial, since many features of relative error designs are incredibly fine-grained and not efficiently measurable in experiments.

- For the ε-dependence, a basic argument involving a SWAP test on half the system leads to a lower bound of $d = \Omega(\log 1/\varepsilon)$ in 1D circuits. This applies to both state and unitary designs with additive error. In all-to-all circuit geometries, the only existing lower bound is Proposition 2 of Ref. [39]. This applies only to unitary designs, and yields a depth lower bound of $d = \Omega(\log \log 1/\varepsilon)$ for any unitary design with additive error.

  Our Theorem 10 extends the lower bound for all-to-all-connected circuits to state designs.

We note that more restricted circuit classes may feature stronger lower bounds that are not reflected above. For example, any unitary ensemble in which each unitary is composed of independent Haar-random gates requires circuit depth at least $d = \Omega(\log n)$ to form relative error designs[80] and $d = \Omega(\log 1/\varepsilon)$ to form additive error designs [47], even in all-to-all connected circuit geometries.

Let us now turn to the proof of Theorem 10. As discussed above, the dependence on k follows from Proposition 8 in Ref. [32]. Hence, the bulk of our proof will focus on the n and ε dependence.

Proof of Theorem 10, k-dependence. From the analysis in Proposition 8 of [32], any ensemble $\mathcal{S}$ that forms an state k-design with additive error $\varepsilon < 1/4$ must contains at least $\Omega(nk/\log(nk))$ gates. If the number of ancilla qubits is bounded by $\mathcal{O}(n)$, then the circuit size can grow at most linearly in the circuit depth d, $\mathcal{O}(n \cdot d)$. Hence, we require $d = \Omega(k/\log(nk))$. If the number of ancilla qubits is unbounded, on the other hand, the light-cone can grow exponentially in the circuit depth (for circuits with arbitrary long-range two-qubit gates). Hence, the total number of gates can grow as $\mathcal{O}(n \cdot \exp(d))$, which implies that the circuit depth must be at least $\Omega(\log k)$. □

Proof of Theorem 10, n- and ε-dependence. Let $\mathcal{S}$ denote the state ensemble. We write $|\psi\rangle = U|0^n\rangle$ for each $|\psi\rangle \sim \mathcal{S}$, where U is a circuit of depth at most d. We let L denote the maximum size of any light-cone in U. We have $L \leq 2^d$ for all-to-all connected circuits and $L \leq 2d$ for 1D circuits.

To set up our proof, let us first divide the n qubits into isolated patches as follows. Each patch will correspond to the forward light-cone of a given qubit. We additionally will demand that the backwards light-cones of any two different patches do not overlap. Mechanistically, we place the patches as follows. We set the first patch by choosing any qubit and letting the first patch consist of all L qubits in its light-cone. We then trace the backwards light-cone of the first patch (which has size less than L^2), then trace the forwards light-cone of this (which has size less than L^3), and then finally trace the backwards light-cone of this (which has size less than L^4). We then set the second patch by choosing any qubit that is outside this backwards-forwards-backwards light-cone. There are at least $n - L^4$ possible choices. The second patch is equal to the forwards light-cone of this qubit. We then set the third patch by tracing out the backwards-forwards-backwards light-cone of the union of the first and second patch, and setting the third patch to be the forwards light-cone of any qubit outside of this. There are at least $n - 2L^4$ possible such choices. Iterating in this manner, we can place at least $M \equiv n/L^4$ patches across the entire system whose backwards light-cones do not overlap. Each patch contains L qubits and the forward light-cone of at least one qubit.

With this setup in hand, we can now prove our lower bound. We consider the following quantum experiment. We draw two copies of a state $|\psi\rangle$ from either the ensemble $\mathcal{S}$ or the Haar ensemble H. We then perform random single-qubit rotations, $v = \bigotimes_{i=1}^n v_i$, on each qubit of the system. Averaging over these rotations yields the state,

$$\mathop{\mathbb{E}}_{v}\left[\left(v\,|\psi\rangle\langle\psi|\,v^\dagger\right)^{\otimes 2}\right] \tag{93}$$

We then measure (i.e. dephase) the state in the computational basis. This yields the state,

$$\sum_{x,y\in\{0,1\}^n} \langle x\otimes y|\mathop{\mathbb{E}}_{v}\left[\left(v\,|\psi\rangle\langle\psi|\,v^\dagger\right)^{\otimes 2}\right]|x\otimes y\rangle\cdot|x\otimes y\rangle\langle x\otimes y|\,. \tag{94}$$

Note that one could place the expectation over v either inside or outside the inner product in the first term. We then forget all information about the measurement outcomes except for whether the bitstring x and the bitstring y agreed on all of their bits in each individual patch. Let $z(x,y) \in \{0,1\}^M$ denote the resulting bitstring, where z_a indicates where x and y are equal on all bits in patch a. That is, $z_a = 1$ if $x_i = y_i$ for all qubits i in patch a, and $z_a = 0$ if $x_i \neq y_i$ for any qubit i in patch a. We can represent the resulting state as,

$$\chi_\psi \equiv \sum_{z\in\{0,1\}^M} p_\psi(z)\,|z\rangle\langle z|\,, \tag{95}$$

where $p_\psi(z) = \sum_{x,y:z(x,y)=z} p_\psi(x,y)$, and $p_\psi(x,y)$ denotes the first term in the sum in Eq. (93). Finally, we conclude the experiment by counting whether the total number of collisions, $s = |z|$, is greater or less than a fixed threshold s^*. That is, we measure the observable,

$$A = \sum_{z:|z|>s^*} |z\rangle\langle z| - \sum_{z:|z|\leq s^*} |z\rangle\langle z|\,, \tag{96}$$

where a positive measurement outcome will be associated to the ensemble $\mathcal{S}$, and a negative measurement outcome to the Haar ensemble. We will set the variable s^* later on in the proof.

The state χ_ψ in Eq. (95) was obtained from $|\psi\rangle$ by a sequence of quantum channels. Hence, if the ensemble $\mathcal{S}$ forms an approximate 2-design with additive error ε, we must have

$$\|\chi_\mathcal{S} - \chi_H\|_1 \leq \varepsilon, \tag{97}$$

where $\chi_\mathcal{S} = \mathbb{E}_{\psi\sim\mathcal{S}}\left[\chi_\psi\right]$ and $\chi_H = \mathbb{E}_{\psi\sim H}\left[\chi_\psi\right]$. By Holder's inequality, we must also have,

$$|\mathrm{tr}(A\chi_\mathcal{S}) - \mathrm{tr}(A\chi_H)| \leq \varepsilon. \tag{98}$$

The strategy of our proof is to lower bound the left hand side above. This immediately lower bounds the achievable additive error ε of any state or unitary design.

Let us first consider the Haar ensemble. The second moment of the Haar ensemble is given by,

$$\mathop{\mathbb{E}}_{\psi\sim H}\left[|\psi\rangle\langle\psi|^{\otimes 2}\right] = \frac{1}{2^n(2^n-1)}\mathbb{1} + \frac{1}{2^n(2^n-1)}\mathcal{S}, \tag{99}$$

where $\mathcal{S}$ is the SWAP operator. This leads to an (expected) output distribution

$$\mathop{\mathbb{E}}_{\psi\sim H}\left[p_\psi(x,y)\right] = \frac{1}{2^n(2^n-1)} + \frac{1}{2^n(2^n-1)}\delta_{x=y}. \tag{100}$$

The total variational (i.e. 1-norm) distance between this distribution and the maximally mixed distribution is,

$$\sum_{x,y}\left|\mathop{\mathbb{E}}_{\psi\sim H}\left[p_\psi(x,y)\right] - \frac{1}{4^n}\right| = 2(4^n-2^n)\left(\frac{1}{4^n} - \frac{1}{2^n(2^n+1)}\right) = \frac{2}{2^n}\frac{1-1/2^n}{1+1/2^n} \leq \frac{2}{2^n}, \tag{101}$$

which is exponentially small in n. Hence, for the purposes of this proof we can treat $\mathbb{E}_{\psi\sim H}\left[p_\psi(x,y)\right]$ as maximally mixed. This yields a collision distribution,

$$\tilde{p}_H(z) = (1-1/2^L)^{|z|}(1/2^L)^{M-|z|}, \tag{102}$$

in which each patch features a collision with an independent probability $q_H = 1/2^L$. Here, we let $\tilde{p}_H(z)$ denote the collision distribution drawn from the flat distribution over x and y, which is close to the exact Haar collision distribution $p_H(z)$ up to total variation distance $\sum_z |\tilde{p}_H(z) - p_H(z)| \leq 2/2^n$.

We can now turn to the ensemble $\mathcal{S}$. Let us first notice a key fact: For each fixed state $|\psi\rangle$, the distribution $p_\psi(z)$ is a tensor product distribution. This follows because the patches are backwards-light-cone-separated, and in going from $p_\psi(x,y)$ to $p_\psi(z)$ we have traced out all qubits that are outside every patch. (We note that this does not necessarily hold after averaging over $|\psi\rangle$, since the ensemble $\mathcal{S}$ might feature long-range correlations between the random gates in different patches.) Hence, we can write

$$p_\psi(z) = \prod_{a=1}^{M}(1-q_\psi^a)^{z_a}(q_\psi^a)^{1-z_a}, \tag{103}$$

where q_ψ^a is the probability to observe a collision in patch a.

Our next step is to lower bound each q_ψ^a. To do so, we follow a similar approach to the proof of Proposition 1 in Ref. [39]. Let

$$\rho_a = \mathrm{tr}_{\bar{a}}(U\,|0^n\rangle\langle 0^n|\,U^\dagger) \tag{104}$$

denote the reduced density matrix of the system on patch a after U is applied. The quantity q_ψ^a measures the collision probability when ρ_a is measured in a random single-qubit basis,

$$q_\psi^a = \mathop{\mathbb{E}}_{v}\left[\sum_{x_a\in\{0,1\}^L} \langle x_a|\, v_a\rho_a v_a^\dagger\,|x_a\rangle^2\right], \tag{105}$$

where v_a is the restriction of the random single-qubit rotations v to patch a. A standard formula for the twirl over a tensor product of single-qubit 2-designs [12] allows one to compute

$$q_\psi^a = \sum_{k=0}^{n} 3^{-k}\,\mathrm{tr}_a\left(\rho_a\cdot\mathcal{P}_k\{\rho_a\}\right), \tag{106}$$

where $\mathcal{P}_k$ is a super-operator that projects onto Pauli operators with weight k.

Now that we have an explicit formula for q_ψ^a, we can proceed with our lower bound. For each patch a, we re-write the initial state of the system as a sum of three operators,

$$|0^n\rangle\langle 0^n| = \frac{1}{2^n}\mathbb{1} + \rho_1^a + \rho_>^a, \tag{107}$$

where ρ_1^a consists solely the single-qubit Z-stabilizer whose light-cone is in a, and $\rho_>^a$ consists of all other non-identity stabilizers. Note that $U\rho_1^aU^\dagger$ contains operators at most of weight L, all of which have support entirely in patch a. We then consider the total support of ρ_a on all weights between 1 and L,

$$P_L^a \equiv \sum_{k=1}^{L}\mathrm{tr}_a(\rho_a\cdot\mathcal{P}_k\{\rho_a\}), \tag{108}$$

where again, $\rho_a = \mathrm{tr}_{\bar{a}}(U\,|0^n\rangle\langle 0^n|\,U^\dagger)$. We can now insert the decomposition Eq. (107) into this expression. Since ρ_1^a and $\rho_>^a$ are orthogonal before the application of U, i.e. $\mathrm{tr}(\rho_1^a\rho_>^a)=0$, they are also orthogonal after the application of U. Moreover, they remain orthogonal after tracing out $\bar{a}$ and projecting to weights $k\le L$, since ρ_1 only has support on a and such weights. This allows us to lower bound P_L by focusing solely on the ρ_1^a term,

$$P_L^a = \mathrm{tr}_a((\rho_1^a)^2) + \sum_{k=0}^{L}\mathrm{tr}_a(U\rho_>^aU^\dagger\cdot\mathcal{P}_k\{U\rho_>^aU^\dagger\}) \ge \frac{1}{2^L}, \tag{109}$$

since the second term is non-negative and the first term is equal to $1/2^L$, since ρ_1^a contains a single stabilizer. Note that the identity term in Eq. (107) does not contribute to P_L^a, since it does not have weight between 1 and L. This lower bound on P_L^a in turn lower bounds the expected collision probability,

$$q_\psi^a = \sum_{k=0}^{n} 3^{-k}\,\mathrm{tr}_a\left(\rho_a\cdot\mathcal{P}_k\{\rho_a\}\right) \ge \frac{1}{2^L} + 3^{-L}P_L^a \ge \frac{1}{2^L}\left(1+\frac{1}{3^L}\right), \tag{110}$$

where the first bound follows because every term in the sum is positive. This completes our lower bound on q_ψ^a.

We can now specify the observable A and analyze its behavior. Consider a fictional Bernoulli process $p_f(z)$ in which each patch has an independent probability of collision, $q_f = (1/2^L)(1+1/3^L)$. This is equal to our lower bound on the collision probabilities q_ψ^a. We will construct A as the optimal observable to distinguish this fictional Bernoulli process from the Haar-random collision distribution, which corresponds to a Bernoulli process with collision probabilities, $q_H = 1/2^L$. The optimal observable is given by,

$$A = \sum_{z\in\{0,1\}^M}\mathrm{sgn}\big(p_f(z)-\tilde{p}_H(z)\big)\cdot|z\rangle\langle z|\,. \tag{111}$$

To determine the value of the sign function, we can compute the ratio of the two probability distributions,

$$\frac{p_f(z)}{\tilde{p}_H(z)} = \left(\frac{1-(1/2^L)(1+1/3^L)}{1-1/2^L}\right)^{|z|}\left(\frac{(1/2^L)(1+1/3^L)}{1/2^L}\right)^{M-|z|}. \tag{112}$$

We define s^* as the value of $|z|$ at which this ratio is equal to one. For $|z| > s*$, we have $p_f(z) > \tilde{p}_H(z)$, and for $|z| \leq s*$, we have $p_f(z) \leq \tilde{p}_H(z)$. This confirms our formula for A in Eq. (96).

We will now show that A allows one to distinguish $p_f(z)$ and $p_H(z)$. In the next paragraph, we will use this result to show that A also allows one to distinguish $p_{\mathcal{S}}(z)$ and $\tilde{p}_H(z)$ for any sufficiently low-depth ensemble $\mathcal{E}$. We have

$$\langle A\rangle_f - \langle A\rangle_H \geq \sum_{z\in\{0,1\}^M} \left|p_f(z) - \tilde{p}_H(z)\right| - 2/2^n, \tag{113}$$

where the latter term accounts for the difference between the exact Haar distribution $p_H(z)$ and $\tilde{p}_H(z)$, which is small. The first term is equal to the total variation distance $\mathrm{TVD}(p_f, \tilde{p}_H)$ between the two distributions. Since both distributions are a tensor power of the same distribution across all patches, we can apply the standard inequalities (see e.g. Section 13 of Ref. [81]),

$$\mathrm{TVD}\big(p_1^{\otimes M}, p_2^{\otimes M}\big) \geq \frac{1}{2} d_H\big(p_1^{\otimes M}, p_2^{\otimes M}\big)^2 = 1 - \left(1 - \frac{1}{2} d_H(p_1,p_2)^2\right)^M \geq 1 - \left(1 - \frac{1}{2}\mathrm{TVD}(p_1,p_2)^2\right)^M, \tag{114}$$

where $d_H(p_1, p_2)$ is the Hellinger distance. From this, we find

$$\langle A\rangle_f - \langle A\rangle_H + 2/2^n \geq \mathrm{TVD}(p_f, \tilde{p}_H) \geq 1 - (1-|q_f - q_H|^2)^M = 1 - \left(1 - \left(\frac{1}{2^L 3^L}\right)^2\right)^M. \tag{115}$$

Let $x \equiv (1/(2^L 3^L))^2$. We can bound $(1-x)^M \leq e^{-Mx} \leq 1 - Mx/(2\log 2)$, where the second inequality holds for $xM \leq \log 2$. This yields,

$$\langle A\rangle_f - \langle A\rangle_H \geq \frac{M}{\log 2}\left(\frac{1}{2^L 3^L}\right)^2 - 2/2^n. \tag{116}$$

This is our final lower bound on $\langle A\rangle_f - \langle A\rangle_H$.

Let us now turn to the ensemble $\mathcal{E}$. We will show that $\langle A\rangle_{\mathcal{S}} \geq \langle A\rangle_f$, hence $\langle A\rangle_f - \langle A\rangle_H$ obeys the same lower bound as in Eq. (116). To see this, consider $\langle A\rangle_\psi$ for an individual state $|\psi\rangle \sim \mathcal{S}$. As discussed, the distribution $p_\psi(z)$ is a tensor product of binary variables with probabilities at least q_ψ^a in each patch. Consider the expectation value $\langle A\rangle(\{q_\psi^a\})$ as a function of these probabilities. We have

$$\begin{aligned}
\partial_{q_\psi^a}\langle A\rangle(\{q_\psi^a\}) &= \partial_{q_\psi^a}\left(2\sum_{z:|z|>s^*} p_\psi(z) - 1\right) \\
&= 2\partial_{q_\psi^a}\left((1-q_\psi^a)\sum_{|z_{\bar{a}}|>s^*} p_\psi(z_{\bar{a}}) + q_\psi^a \sum_{|z_{\bar{a}}|>s^*-1} p_\psi(z_{\bar{a}})\right) \\
&= 2\left(\sum_{|z_{\bar{a}}|>s^*-1} p_\psi(z_{\bar{a}}) - \sum_{|z_{\bar{a}}|>s^*} p_\psi(z_{\bar{a}})\right) \geq 0.
\end{aligned} \tag{117}$$

Hence, $\langle A\rangle(\{q_\psi^a\})$ is monotonically increasing as a function of each q_ψ^a. The inequality $q_\psi^a \geq q_f$ then implies $\langle A\rangle_{\mathcal{S}} = \mathbb{E}_{\psi\sim\mathcal{E}}[\langle A\rangle_\psi] \geq \mathbb{E}_{\psi\sim\mathcal{E}}[\langle A\rangle_f] = \langle A\rangle_f$, as desired.

This completes our proof. From all of the above, we have

$$\varepsilon \geq \langle A\rangle_{\mathcal{S}} - \langle A\rangle_H \geq \frac{M}{\log 2}\left(\frac{1}{2^L 3^L}\right)^2 - 2/2^n = \frac{1}{\log 2}\frac{n/L^4}{36^L} - 2/2^n, \tag{118}$$

for any approximate unitary 2-design with additive error ε. We have assumed that $d = o(n)$ in 1D circuits and $d = o(\log n)$ in all-to-all connected circuits. Since $L \leq 2d$ in 1D and $L \leq 2^d$ in all-to-all circuits, these assumptions imply $L = o(n)$. Hence, the negative term in Eq. (118) is small compared to the positive term and can be neglected. Thus, the inequality can be satisfied if an only if $L = \Omega(\log(n/\varepsilon))$. In 1D circuits, this yields $d = \Omega(\log(n/\varepsilon))$. In all-to-all connected circuits, this yields $d = \Omega(\log\log(n/\varepsilon))$ as desired. □