

Strong random unitaries and fast scrambling

Thomas Schuster^{1,2}, Fermi Ma³, Alex Lombardi⁴,
Fernando Brandão^{5,1}, and Hsin-Yuan Huang^{1,2}

¹California Institute of Technology

²Google Quantum AI

³UC Berkeley, New York University

⁴Princeton University

⁵AWS Center for Quantum Computing

October 1, 2025

Abstract

Understanding how fast physical systems can resemble Haar-random unitaries is a fundamental question in physics. Many experiments of interest in quantum gravity and many-body physics, including the butterfly effect in quantum information scrambling and the Hayden-Preskill thought experiment, involve queries to a random unitary U alongside its inverse $U^\dagger$, conjugate U^* , and transpose U^T . However, conventional notions of approximate unitary designs and pseudorandom unitaries (PRUs) fail to capture these experiments. In this work, we introduce and construct *strong unitary designs* and *strong PRUs* that remain robust under all such queries. Our constructions achieve the optimal circuit depth of $\mathcal{O}(\log n)$ for systems of n qubits. We further show that strong unitary designs can form in circuit depth $\mathcal{O}(\log^2 n)$ in circuits composed of independent two-qubit Haar-random gates, and that strong PRUs can form in circuit depth $\text{poly}(\log n)$ in circuits with no ancilla qubits. Our results provide an operational proof of the fast scrambling conjecture from black hole physics: every observable feature of the fastest scrambling quantum systems reproduces Haar-random behavior at logarithmic times.

1 Introduction

Understanding how fast a quantum system can scramble information is a fundamental question with implications throughout quantum science. In quantum computing, quantum information scrambling by random circuits enables efficient device benchmarking [1–4], quantum state tomography [5–7], and quantum advantage demonstrations [8–10]. In quantum cryptography [11–13], scrambling is characterized by the computational indistinguishability of quantum circuits from Haar-random unitaries, and enables new cryptographically secure protocols. In fundamental physics, scrambling and the emergence of Haar-random unitary behaviors provide powerful theoretical tools for modeling complex phenomena across diverse areas, from quantum many-body dynamics [14–16] to quantum chaos and thermalization [17–19] to quantum gravity and black hole physics [20–24].

Across all of these contexts, a central question concerns the minimum time required to scramble quantum information. This question is crucial for quantum technologies: the shorter the time required,

the more experimentally applicable random unitary protocols become. In physics, this question is captured by the *fast scrambling conjecture*, proposed by Sekino and Susskind [20], which states¹:

Conjecture 1 (Fast scrambling conjecture, Sekino and Susskind [20]). The minimum time to *scramble* information in quantum systems of n qubits under all-to-all connectivity is $\Theta(\log n)$.

In their original formulation, scrambling was characterized through entanglement growth: for every n -qubit pure state $|\psi\rangle$, every sufficiently small subsystem of the time-evolved state $U|\psi\rangle\langle\psi|U^\dagger$ should achieve near-maximal entanglement entropy in $\mathcal{O}(\log n)$ time. However, the modern physical understanding of quantum information scrambling encompasses numerous signatures beyond entanglement growth, including, in physical studies, the decay of out-of-time-order correlators [25], information recovery protocols like the Hayden-Preskill thought experiment [21], and the saturation of operator size distributions and operator entanglement entropies to their Haar-random values [26].

In recent years, *indistinguishability from Haar-random* has emerged as a powerful conceptual framework for characterizing scrambling: a system scrambles if its dynamics U become operationally indistinguishable from Haar-random evolution in any physical experiment. Operational indistinguishability is commonly defined through *approximate unitary k -designs* [27–39] and *pseudorandom unitaries* (PRUs) [11, 40–42]. The former guarantees that U is indistinguishable from a Haar-random unitary within any quantum experiment that queries U up to k times, while the latter concerns any polynomial-time quantum experiment. These general operational frameworks offer a crucial advantage of also capturing any future scrambling diagnostics yet to be discovered. This naturally motivates the following operational formulation of the fast scrambling conjecture:

Conjecture 2 (Operational fast scrambling conjecture). The minimum circuit depth to form n -qubit unitary k -designs (for constant k) and PRUs under all-to-all connectivity is $\Theta(\log n)$.

The past decade has seen remarkable progress in understanding the depths needed to form unitary designs and PRUs [11, 32–43]. Unfortunately, standard notions of designs and PRUs possess two critical limitations, which undermine the utility of the fast scrambling conjecture formulated above.

Limitation 1: Forward-only access. Standard unitary designs and PRUs only guarantee indistinguishability under forward queries to U . However, many scrambling diagnostics require access to the inverse $U^\dagger$, conjugate U^* , or transpose U^T operations. For example, out-of-time-order correlators require time-reversal operations using $U^\dagger$ to be efficiently measured [44], while efficient information recovery in the Hayden-Preskill protocol requires complex conjugation U^* [45]. Similarly, recent work in quantum cryptography [46] suggests that the strongest notion of PRUs should allow access to all of U , $U^\dagger$, U^* , U^T (as well as their controlled versions), reflecting the fact that a user with knowledge of the gates composing U should be able to implement all these transformations.

Standard designs and PRUs fail to capture these essential features. In fact, they do not even satisfy an $\Omega(\log n)$ depth lower bound: recent work [39, 47] shows that standard unitary designs and PRUs can be constructed in $\Theta(\log \log n)$ depth, exponentially faster than the conjectured minimum scrambling time of $\Theta(\log n)$. This demonstrates that forward-only indistinguishability is insufficient to capture the complete range of scrambling behaviors often desired in physics and cryptography.

Limitation 2: Unphysical use of ancillary systems. All existing PRU constructions [36, 40, 42] over n qubits require $m = \text{poly}(n)$ ancilla qubits initialized to $|0^m\rangle$ and returned to $|0^m\rangle$ to achieve pseudorandomness on the original n qubits. While this use of ancilla qubits is acceptable for cryptographic applications, it creates a fundamental mismatch when modeling physical quantum dynamics. Physical scrambling processes, whether in black holes or many-body quantum systems,

¹The fast scrambling conjecture also posits that optimal scrambling is achieved in black hole systems. Verifying this claim remains experimentally inaccessible with current technology and is beyond the scope of this work.

operate on fixed Hilbert spaces and do not involve auxiliary degrees of freedom with fine-tuned initialization and finalization conditions. As a result, standard cryptographic PRUs do not necessarily provide appropriate evidence for physical scrambling processes.

In this work, we address both of these limitations. First, we introduce *strong unitary k -designs* and *strong pseudorandom unitaries* (PRUs), which are indistinguishable from Haar-random in any experiment that queries the unitary U or its inverse $U^\dagger$, conjugate U^* , or transpose U^T . Second, we initiate the study of *ancilla-free PRUs*, which are PRUs with efficient ancilla-free circuit implementations. These definitions motivate a strengthened version of the fast scrambling conjecture:

Conjecture 3 (Strong fast scrambling conjecture). The minimum depth to form n -qubit **strong** unitary designs and PRUs under all-to-all connectivity is $\Theta(\log n)$, achievable **without ancilla**.

This conjecture captures the strongest possible operational meaning of fast scrambling: quantum dynamics that remain indistinguishable from Haar-random under any efficient quantum experiment involving any combination of operations, realized using only the physical degrees of freedom.

Our main results provide compelling evidence for, and an almost full resolution to, the strong fast scrambling conjecture:

1. **Strong unitary designs.** We provide the first proof of existence for strong unitary designs and establish that the minimum depth to form them is precisely $\Theta(\log n)$. This proves that every property measurable in finitely many queries scrambles in logarithmic time.
2. **Strong PRUs.** We provide the first proof of existence for strong PRUs secure against all operations U , $U^\dagger$, U^* , U^T and establish that the minimum depth to form them is precisely $\Theta(\log n)$ under a well-established cryptographic assumption: subexponential hardness of learning with errors (LWE) [48]. This represents a significant advance over prior work [42], which requires $\text{poly}(n)$ depth and only achieved security against U and $U^\dagger$. Our result proves that every property measurable by polynomial-time experiments scrambles in logarithmic time.
3. **Ancilla-free constructions:** We show that both strong unitary designs and strong PRUs can be implemented without using any ancilla qubits in $\text{poly}(\log n)$ depth. While slightly larger than the conjectured $\Theta(\log n)$, this provides the first ancilla-free PRU construction for any security notion, including standard forward-only PRUs. These constructions are secure under the subexponential hardness² of learning with errors [48].
4. **Generic emergence.** We prove that all-to-all random circuits consisting of independent Haar-random two-qubit gates form strong unitary designs in $\mathcal{O}(\log^2 n)$ depth, providing evidence that fast scrambling is a generic phenomenon rather than requiring careful engineering.

All of our results immediately extend to quantum experiments with access to controlled versions of $U, U^\dagger, U^*, U^T$, following the general reduction laid out in [49, 50].

Our constructions of strong unitary designs and strong PRUs introduce several new random unitary ensembles and techniques for working with strong random unitaries. Our main technical contributions are threefold. *First*, we introduce the Luby-Rackoff-Function-Clifford (LRFC) ensemble and prove that it forms both strong unitary designs and strong PRUs. The LRFC ensemble adapts the Permutation-Function-Clifford (PFC) ensemble of [40], replacing the random permutation with a Luby-Rackoff construction to achieve exponentially lower circuit depths while maintaining security against all queries to U , $U^\dagger$, U^* , and U^T . *Second*, inspired by [36], we prove a gluing theorem for strong unitary designs and strong PRUs. This powerful technique allows us to reduce the circuit

²In order to construct polynomial-depth ancilla-free PRUs, it suffices to assume the polynomial hardness of LWE.

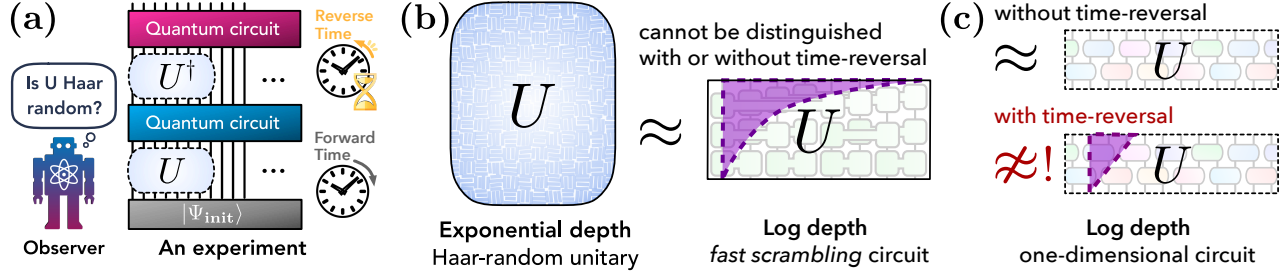


Figure 1: Illustration of our main results. **(a)** A strong approximate unitary k -design is a random unitary ensemble that is indistinguishable from Haar in any quantum experiment that queries U or its inverse (i.e. time-reversal), conjugate, or transpose k times. A strong pseudorandom unitary (PRU) is similarly indistinguishable in any polynomial-time experiment. **(b)** We construct strong unitary designs and PRUs on n qubits in depth $\mathcal{O}(\log n)$. Our constructions use long-range two-qubit gates to scramble quantum information over all n qubits as fast as possible. **(c)** In comparison, low-depth one-dimensional quantum circuits can only scramble information over local regions. This allows them to form conventional designs [35, 36] and PRUs [36], but not strong designs or strong PRUs.

depth of our strong constructions to the optimal value of $\mathcal{O}(\log n)$, which we prove is the minimum possible for any strong unitary design or strong PRU, and to establish strong unitary designs in depth $\mathcal{O}(\log^2 n)$ using all-to-all random circuits with Haar-random two-qubit gates. *Third*, to construct ancilla-free PRUs, we combine a new classical-to-quantum circuit compilation technique with our gluing theorems to construct standard PRUs in $\text{poly}(\log n)$ depth over 1D geometries and strong PRUs in $\text{poly}(\log n)$ depth over all-to-all geometries, both without using any ancilla qubits.

Organization of this paper. Our manuscript is organized as follows. In Section 2, we define strong unitary designs and summarize our main results on their circuit depth. We also illustrate the failure of standard definitions of approximate unitary designs to capture experiments involving the time-reverse $U^\dagger$ and conjugate U^* . In Section 3, we define strong PRUs and summarize our main results on their circuit depth. In Section 4, we provide detailed descriptions of our constructions and proofs of strong unitary designs and PRUs. These involve three key ingredients as described above: the LRFC random unitary ensemble, a gluing construction for optimizing the circuit depth of strong random unitaries, and an adapted gluing construction for local random circuits. In Section 5, we discuss the relation between strong random unitaries and fast quantum information scrambling. We conclude in Section 6 with discussions and open questions.

2 Strong approximate unitary designs

Approximate unitary designs seek to mimic Haar-random unitaries in applications that involve a random unitary only a finite number of times. Let us first review their standard definitions and then provide our strong definition and summarize our main results on strong unitary designs.

Background. An exact unitary k -design on n qubits is a random unitary ensemble $\mathcal{E}$ whose k -th moment, $\Phi_{\mathcal{E}}(\cdot) \equiv \mathbb{E}_{U \sim \mathcal{E}}[U^{\otimes k}(\cdot)U^{\dagger, \otimes k}]$, equals the k -th moment of the Haar ensemble on $U(2^n)$: $\Phi_{\mathcal{E}} = \Phi_H$. While exact designs provide the strongest possible guarantees, efficient realizations beyond $k \leq 3$ are exceedingly rare.

To address this limitation, several notions of *approximate unitary k -designs* have been introduced. We begin with the strongest such notion, the so-called *relative error* [32]. A unitary ensemble $\mathcal{E}$ is an

approximate unitary k -design with relative error ε if its moment obeys $(1 - \varepsilon)\Phi_H \preceq \Phi_{\mathcal{E}} \preceq (1 + \varepsilon)\Phi_H$, where $\mathcal{A} \preceq \mathcal{B}$ indicates that $\mathcal{B} - \mathcal{A}$ is a completely positive map. Physically, the relative error guarantees that a random unitary $U \sim \mathcal{E}$ cannot be distinguished from Haar-random in any quantum experiment that queries it up to k times [36]. It also provides even stronger guarantees on properties that cannot be efficiently measured in any quantum experiment [39].

Remarkably, unitary k -designs with relative error ε over n qubits can form in extremely low circuit depths of $\tilde{\mathcal{O}}(k \log n / \varepsilon)$ [35, 36], growing only logarithmically in the number of qubits n . This holds even in one-dimensional systems with small light-cones. The dependence on n , k , and ε was further improved exponentially to $\mathcal{O}(k \log k \cdot \log \log(n/\varepsilon))$, to achieve relative error, and $\mathcal{O}(\log k \cdot \log \log(n/\varepsilon))$, to achieve a more physical notion of measurable error, for systems with long-range two-qubit gates [39].

The existence of such low-depth unitary designs is counter-intuitive, as they appear to capture many features of Haar-random unitaries [35, 36] without developing other characteristic features such as large light-cones, high entanglement, decay of out-of-time-order correlations, and good quantum encoding properties. Notably, these latter features are precisely the standard diagnostics of *quantum information scrambling* in many-body quantum physics and quantum gravity [15, 20, 25, 26, 51–56].

A resolution to this apparent paradox was provided in [36]: these scrambling-related features cannot be detected efficiently in any quantum experiment that queries only the forward evolution U . Consequently, they do not form barriers to realizing low-depth unitary designs. However, many scrambling diagnostics *can* be efficiently detected in quantum experiments that involve the inverse $U^\dagger$, conjugate U^* , or transpose U^T of the unitary U . These are precisely the experiments traditionally studied in quantum information scrambling [10, 54, 57–61]. For example, estimating out-of-time-order correlators to study butterfly effects requires time-reversal operations $U^\dagger$ [54, 57, 57], while the decoding protocol for the Hayden-Preskill thought experiment involves complex conjugation U^* [45]. This motivates a stronger notion of approximate unitary designs that captures experiments involving not just U , but also $U^\dagger$, U^* , and U^T .

Strong unitary designs. We define a *strong ε -approximate unitary k -design* as any random unitary ensemble $\mathcal{E}$ that cannot be distinguished from Haar-random in any quantum experiment that makes any k queries to the unitary U or its inverse $U^\dagger$, conjugate U^* , or transpose U^T . To be precise, if we denote the output of a general quantum experiment as $|\psi_W^U\rangle = W_{k+1}U^{\circ k}W_kU^{\circ k-1}\dots U^{\circ 1}W_1|0\rangle$, where each $\circ_j \in \{\cdot, \dagger, T, *\}$ represents forward evolution, inverse, transpose, or conjugate respectively, and W_j are arbitrary quantum operations applied between successive queries, then we demand

$$\left\| \mathbb{E}_{U \sim \mathcal{E}} \left[|\psi_W^U\rangle\langle\psi_W^U| \right] - \mathbb{E}_{U \sim H} \left[|\psi_W^U\rangle\langle\psi_W^U| \right] \right\|_1 \leq \varepsilon \quad (2.1)$$

for all choices of W_j and $\circ_j$. This generalizes the notion of adaptive security for pseudorandom unitaries [11, 42] and measurable error for unitary designs [39] to incorporate all variants of the unitary. We refer to Appendix A.1 for further discussion, including strong versions of other design approximation metrics.

With this definition, a fundamental question arises: what circuit depths are required for strong unitary designs to form? A basic light-cone argument, which we formalize later, shows that strong unitary designs cannot form until information can propagate between any pair of qubits in the system. This requires the light-cone of the evolution to encompass all n qubits, demanding depth $\Omega(\log n)$ in general quantum circuits and dynamics. Can this extremely fast speed of scrambling actually be achieved? The *fast scrambling conjecture* from black hole physics posits that all-to-all connected quantum systems can achieve logarithmic scrambling times [20]. However, existing progress toward proving this conjecture has focused on specific scrambling diagnostics, such as the decay of out-of-time-order correlators or the encoding properties of random unitaries [26, 62–71]. A fully general

operational proof of this conjecture has remained an open question.

Our main result establishes that strong unitary designs can indeed form in optimal circuit depth $\mathcal{O}(\log n)$ in all-to-all-connected architectures. This proves that every property of a random unitary measurable in a constant number of queries scrambles in logarithmic time.

Theorem 1 (Fast formation of strong unitary designs). *Strong ε -approximate unitary k -designs can be realized in the following circuit depths:*

1. $d = \mathcal{O}(\log n + \log k \cdot \log \log(nk/\varepsilon))$ using all-to-all structured circuits with $\tilde{\mathcal{O}}(nk)$ ancilla qubits.
2. $d = \mathcal{O}(\log n + k \cdot \log \log(nk/\varepsilon))$ using all-to-all structured circuits with $\tilde{\mathcal{O}}(n)$ ancilla qubits.

For all-to-all random circuits consisting of independent Haar-random two-qubit gates without ancilla qubits, $d = \mathcal{O}(k \cdot \text{poly log } k \cdot \log(n/\varepsilon) + \log n \cdot \log(n/\varepsilon))$.

The structured circuits achieve the optimal $\mathcal{O}(\log n)$ scaling in system size when k and ε are held constant, while the random circuits achieve an $\mathcal{O}(\log^2 n)$ scaling. The upper bounds for structured circuits are nearly optimal across all parameters, as confirmed by our lower bounds:

Proposition 1. (Depth lower bounds for strong unitary designs) *For any $\varepsilon < 1/4$, any circuit ensemble over n qubits that forms a strong ε -approximate unitary k -design requires circuit depth d :*

1. $d = \Omega(\log n + \log k)$ for any all-to-all circuits with any number of ancilla qubits.
2. $d = \Omega(\log n + k/\log(nk))$ for any all-to-all circuits with at most $\mathcal{O}(n)$ ancilla qubits.

In contrast, for any 1D circuits with any number of ancilla qubits, $d = \Omega(n + k/\log(nk))$.

The two items confirm near-optimality of our all-to-all constructions, while we also show an exponential separation between all-to-all connectivity and finite-dimensional geometries. We provide detailed constructions and proof techniques in Section 4 and complete proofs in Appendix A. In Appendix A.6, we also establish a surprising result showing that local random circuits require $\Omega(n)$ depth to realize strong unitary designs with *relative error*, regardless of connectivity.

3 Strong pseudorandom unitaries

Pseudorandom unitaries (PRUs) seek to mimic Haar-random unitaries in efficient quantum experiments. Let us first review their standard definition and then provide our strong definition and summarize our main results on strong PRUs.

Background. A random unitary ensemble $\mathcal{E}$ is a PRU if no efficient quantum algorithm can distinguish a random unitary $U \sim \mathcal{E}$ from a Haar-random unitary under polynomially many queries to U [11]. More precisely, $\mathcal{E}$ is a PRU with security against any $t(n)$ -time quantum adversary if it cannot be distinguished from Haar-random in any $t(n)$ -time quantum experiment, where $t(n)$ is some function of the number of qubits n .

The premier example is the Permutation-Function-Clifford (PFC) ensemble [40], $U = PFC$, formed by multiplying a pseudorandom permutation P , a pseudorandom function F , and a random Clifford unitary C . Under standard cryptographic assumptions, the PFC ensemble achieves security against subexponential-time quantum adversaries [42]. However, it requires circuit depth $\text{poly}(n)$ to implement, even on all-to-all-connected geometries, due to the circuit depth of the pseudorandom permutation [36, 73].

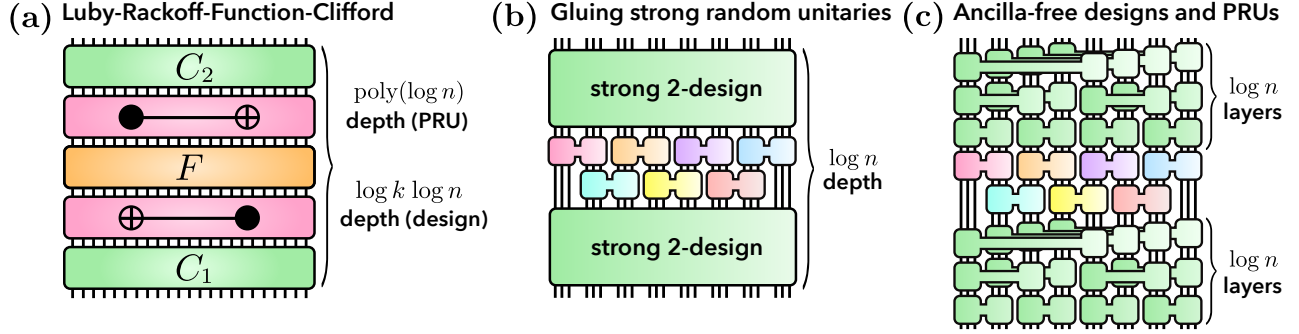


Figure 2: Our constructions of strong unitary k -designs and strong PRUs. **(a)** The Luby-Rackoff-Function-Clifford (LRFC) ensemble sandwiches classical shuffle and phase gates (pink and orange) between random Clifford unitaries (green). It forms a strong unitary design and a strong PRU in the stated circuit depths. **(b)** To further reduce these depths, we consider a glued construction, with two layers of small 2ξ -qubit random unitaries (various colors) sandwiched between strong n -qubit unitary 2-designs (green). This forms a strong unitary k -design when $\xi = \Omega(\log(nk/\epsilon))$ and a strong PRU when $\xi = \omega(\log n)$. We instantiate each small unitary with the LRFC ensemble. **(c)** To obtain ancilla-free constructions, we replace each n -qubit 2-design with a fast scrambling circuit of depth $\log n$ composed of 2ξ -qubit 2-designs. For ancilla-free strong unitary designs consisting of Haar-random two-qubit gates, each small unitary is drawn from a random circuit on 2ξ qubits. For ancilla-free strong PRUs, each small unitary is implemented by reusing neighboring qubits as ancillae.

Recent work has achieved exponential improvements in the circuit depths of standard PRUs. Ref. [36] reduces the depth to $\text{poly}(\log n)$ while maintaining security against polynomial-time quantum adversaries. The same work also discusses PRU realizations in even smaller circuit depths $\text{poly}(\log \log n)$ using the LRFC ensemble introduced in our work.³ We will show that the LRFC ensemble forms a strong PRU in circuit depth $\text{poly}(\log n)$, which yields circuit depth $\text{poly}(\log \log n)$ for the two-layer LRFC ensemble considered in Ref. [36].

Similar to standard unitary designs, existing PRUs exhibit a fundamental limitation: they only guarantee security against experiments that query the forward evolution U . However, as discussed for strong unitary designs, many important quantum phenomena require experiments involving the inverse $U^\dagger$, conjugate U^* , or transpose U^T to be detected. Prior work partially addressed this by extending the PFC ensemble to achieve security against experiments querying both U and $U^\dagger$, using the construction $U = DPFC$ with an additional random Clifford D [42]. However, this approach still omits conjugate and transpose operations, and requires $\text{poly}(n)$ circuit depth to implement. In our results that follow, we establish security under all queries to $U, U^\dagger, U^*, U^T$ and exponentially reduce the circuit depth from $\text{poly}(n)$ to $\mathcal{O}(\log n)$.

Strong pseudorandom unitaries. We define a *strong PRU* as any random unitary ensemble $\mathcal{E}$ that cannot be distinguished from Haar-random in any efficient quantum experiment involving any combination of queries to the unitary U or its inverse $U^\dagger$, conjugate U^* , or transpose U^T . Formally, $\mathcal{E}$ is a strong PRU with $t(n)$ -time security if it remains indistinguishable from Haar-random in any $t(n)$ -time quantum experiment, regardless of which operations are queried.

Our main result establishes that strong PRUs can form in optimal circuit depth $\mathcal{O}(\log n)$ in all-to-all-connected architectures. This proves that every efficiently observable property of quantum

³The LRFC construction was developed by several of the authors of this work at the time of publication of Ref. [36] but the security proof remained unpublished until now.

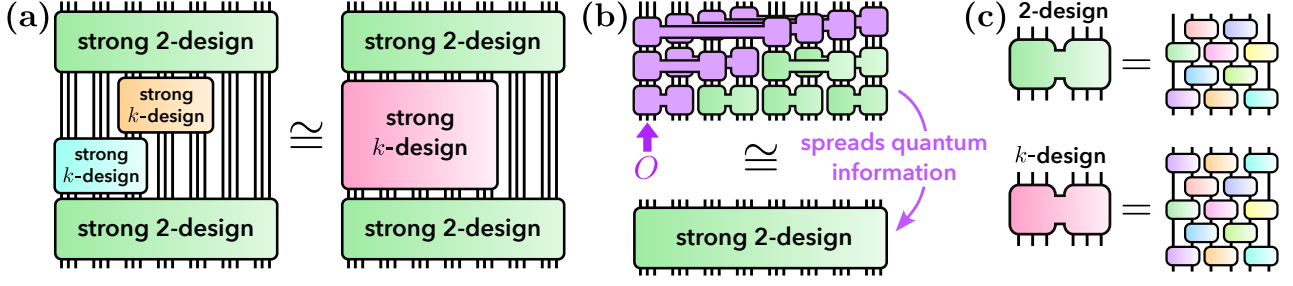


Figure 3: Illustration of key ideas from the proof of Theorem 1 and Theorem 2. (a) To analyze our glued construction, we prove that two strong unitary k -designs “glue” together whenever they are sandwiched by larger unitary 2-designs. This does not hold in the absence of the larger 2-designs. (b) To show that the blocked fast scrambling circuit forms a strong 2-design, we prove that any unitary ensemble that uniformly spreads quantum information (purple) is a strong 2-design. The circuit spreads information over n qubits in $\log n$ layers. (c) To replace each 2ξ -qubit unitary with a local random circuit, we prove a technical lemma that translates spectral gaps [32, 34, 72] to strong unitary designs.

dynamics can achieve pseudorandomness in logarithmic time.

Theorem 2 (Fast formation of strong PRUs). *Under standard cryptographic assumptions, strong PRUs with polynomial-time security can be realized in the following circuit depths:*

1. $d = \mathcal{O}(\log n)$ using all-to-all structured circuits with $\tilde{\mathcal{O}}(n)$ ancilla qubits.
2. $d = \text{poly}(\log n)$ using all-to-all structured circuits with no ancilla qubits.

We describe our constructions and proof methods in Section 4 and provide a complete proof in Appendix B and Appendix E. The first result utilizes our LRFC ensemble [Fig. 2(a)] combined with our gluing theorem for strong random unitaries [Fig. 2(b)]. A circuit depth lower bound of $\Omega(\log n)$ can be easily proven by noting that if the depth of U is sublinear in $\log n$, then an experiment that measures $U^\dagger X_1 U |0^n\rangle$ in the all Z basis will result in a bitstring with almost all zeros, whereas a Haar-random unitary U will result in a bitstring with almost equal number of zeros and ones. Hence, the achieved $d = \mathcal{O}(\log n)$ scaling is optimal. The second result combines the LRFC ensemble, our gluing theorem, and a new strategy for compiling random classical functions in quantum circuits and gluing them together by reusing system qubits on other local patches as ancilla qubits. Both results rely only on the subexponential hardness of standard learning with errors (LWE) [48]. All of our results immediately extend to quantum experiments involving queries to the controlled versions of $U, U^\dagger, U^*, U^T$, following the general reduction in [49, 50].

4 Our constructions

Having summarized our main results, we now introduce our random unitary ensembles. We proceed in three parts. In Section 4.1, we introduce the Luby-Rackoff-Function-Clifford (LRFC) ensemble. We prove that the LRFC ensemble forms a strong unitary design in $\mathcal{O}(\log k \cdot \log n)$ depth and a strong PRU in $\text{poly}(\log n)$ depth. In Section 4.2, we introduce a gluing construction for strong random unitaries, which allows us to further optimize each circuit depth to $\mathcal{O}(\log n + \log k \log \log k)$ and $\mathcal{O}(\log n)$. In Section 4.4, we introduce a modified gluing construction inspired by toy-model fast scrambling circuits in black hole physics [20, 21]. We use this to prove that all-to-all-connected local random circuits can form strong unitary k -designs in depth $\mathcal{O}(k \cdot \text{poly} \log k \cdot \log n / \varepsilon + \log n \cdot \log n / \varepsilon)$.

4.1 The Luby-Rackoff-Function-Clifford (LRFC) ensemble

The Luby-Rackoff-Function-Clifford (LRFC) ensemble is inspired by the Permutation-Function-Clifford (PFC) ensemble introduced in [40]. The key difference is that it replaces the random permutation in the PFC ensemble with a pair of random shuffle gates, which use only random functions. This replacement leads to an exponential improvement in circuit depth, since known constructions of quantum-secure pseudorandom functions [74] are much more efficient than those of pseudorandom permutations [73]. The random shuffle gates are inspired by the Luby-Rackoff block cipher in classical cryptography [75]. Crucially, we show that the random shuffle gates mimic the action of a random permutation *within the LRFC circuit*.

We define the LRFC ensemble as follows. We consider the random unitary,

$$U = D \cdot S_R \cdot F \cdot S_L \cdot C. \quad (4.1)$$

The unitaries C and D are drawn from any strong unitary 2-design on n qubits. For example, they can each be a random Clifford unitary, which are exact unitary 2-designs. The unitary F is a random ternary phase gate, $F = \sum_{x \in \{0,1\}^n} \omega^{f(x)} |x\rangle\langle x|$, where $\omega \equiv e^{i\frac{2\pi}{3}}$ and $f : \{0,1\}^n \rightarrow \{0,1,2\}$ is a random function. Finally, the unitaries S_L and S_R are random shuffle gates, which shuffle the bitstring of the left (or right) $n/2$ qubits conditional on the value of the right (or left) $n/2$ qubits. That is, $S_L |x_L, x_R\rangle = |x_L + h_1(x_R), x_R\rangle$ where $x_L, x_R \in \{0,1\}^{n/2}$ are the left and right $n/2$ bits and $h_1 : \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2}$ is a random function. Similarly, $S_R |x_L, x_R\rangle = |x_L, x_R + h_2(x_L)\rangle$.

To implement the LRFC ensemble efficiently, we will replace each random function in the phase and shuffle gates with a less-random efficient approximation. To construct strong unitary k -designs, we will replace each random function with an exact $2k$ -wise independent function [76]. This replicates the first $2k$ moments of a random function, which guarantees that any quantum experiment making k queries will proceed identically to if the function was random. The factor of two accounts for the bra and ket of the quantum state. Exact $2k$ -wise independent functions can be implemented in quantum circuit depth $\mathcal{O}(k \cdot \log n)$ using $\tilde{\mathcal{O}}(n)$ ancilla qubits, or depth $\mathcal{O}(\log k \cdot \log n)$ using $\tilde{\mathcal{O}}(nk)$ ancilla qubits [39]. To construct strong PRUs, we will replace each random function with a quantum-secure pseudorandom function (PRF) [74]. This is indistinguishable from a random function in any bounded time quantum experiment. Strong PRFs with security against any subexponential-time quantum adversary can be implemented in quantum circuit depth $\text{poly}(\log n)$ [36, 74].

Our main result is that the LRFC circuit forms a strong unitary k -design (when each random function is replaced with a $2k$ -wise independent function) and a strong PRU (when each random function is replaced with a quantum-secure pseudorandom function).

Theorem 3 (The LRFC ensemble is a strong unitary design). *Let f, h_1, h_2 be $2k$ -wise independent functions. Then the LRFC ensemble is a strong ε -approximate unitary k -design with $\varepsilon = \mathcal{O}(k^2/2^{n/6})$.*

Theorem 4 (The LRFC ensemble is a strong PRU). *Let f, h_1, h_2 be subexponentially⁴ quantum-secure pseudorandom functions. Then the LRFC ensemble is a strong PRU with subexponential security.*

The LRFC ensemble can be compiled in $\mathcal{O}(k \cdot \log n)$ circuit depth using $\tilde{\mathcal{O}}(n)$ ancilla qubits, or $\mathcal{O}(\log k \cdot \log n)$ circuit depth using $\tilde{\mathcal{O}}(nk)$ ancilla qubits, when each function is $2k$ -wise independent [39]. It can be compiled in $\text{poly}(\log n)$ circuit depth when each function is pseudorandom [36].

⁴A cryptographic primitive is defined to be sub-exponentially secure if, for a security parameter n , it is secure against attacks running in time $2^{O(n^\epsilon)}$, for some constant $\epsilon > 0$.

4.2 Gluing strong random unitaries

We can further improve upon the circuit depths of the LRFC ensemble by establishing a fundamental property of strong random unitaries. Namely, we prove that two strong random unitaries on overlapping subsystems “glue” together, whenever they are surrounded by larger unitary 2-designs [Fig. 3(a)]. Intuitively, the larger 2-designs scramble the input to the strong random unitaries, which guarantees that the overlap of the input state with counter-examples to the strong gluing construction is exceedingly small. This allows us to reduce the circuit depth of strong unitary k -designs and strong PRUs to match the circuit depth of unitary 2-designs, i.e. $\mathcal{O}(\log n)$ [68].

We consider the random unitary ensemble depicted in Fig. 2(b). Inspired by [36], we partition the n qubits into n/ξ patches of ξ qubits each, arranged in a 1D line. We then form a two-layer circuit composed of small strong random unitaries, where the small unitaries act on two neighboring patches each and are arranged in a brickwork fashion between the two layers. Finally, we “scramble” the two-layer circuit by appending it with an n -qubit strong unitary 2-design on either side.

Our main result is that the scrambled two-layer ensemble forms a strong unitary k -design (when each small random unitary is drawn from a strong unitary k -design) and a strong PRU (when each small random unitary is drawn from a strong PRU).

Theorem 5 (The scrambled two-layer ensemble is a strong unitary design). *Let each small random unitary be a strong $\frac{\varepsilon}{n}$ -approximate unitary k -design on 2ξ qubits. Then the scrambled two-layer ensemble is a strong ε -approximate unitary k -design when $\xi \geq \frac{16}{3} \log_2(nk^2/\varepsilon) + \mathcal{O}(1)$.*

Theorem 6 (The scrambled two-layer ensemble is a strong PRU). *Let each small random unitary be a strong PRU with poly n -time security on 2ξ qubits. Then the scrambled two-layer ensemble is a strong PRU with poly n -time security when $\xi = \omega(\log n)$.*

The theorems immediately yield strong unitary designs and strong PRUs in the circuit depths in Theorems 1 and 2. This follows by adding the circuit depth $\mathcal{O}(\log n)$ of an exact unitary 2-design [68] to the circuit depths of the LRFC ensemble on 2ξ qubits⁵.

As mentioned above, we analyze the scrambled two-layer ensemble by proving that one can glue small strong random unitaries together one brick at a time [36]. Without the larger unitary 2-designs, this gluing does not hold. Applying the following lemma n/ξ times yields Theorems 5 and 6.

Lemma 1 (Gluing strong random unitaries). *Let a, b, c be three subsystems of size at least ξ . Consider the unitary ensemble $U_1 = D_{abc}U_{bc}U_{ab}C_{abc}$, where C_{abc}, D_{abc} are strong ε_2 -approximate unitary 2-designs and U_{ab}, U_{bc} are strong ε_{ab} - and ε_{bc} -approximate unitary k -designs on their respective subsystems. Then U_1 forms a strong ε -approximate unitary k -design with measurable error $\varepsilon = \varepsilon_{ab} + \varepsilon_{bc} + \mathcal{O}(k^2/2^{(3/16)\xi}) + \mathcal{O}(k^{5/8}\varepsilon_2^{1/8})$.*

The strong gluing lemma also allows us to straightforwardly extend Theorems 5 and 6 to allow approximate strong unitary 2-designs instead of exact unitary 2-designs. This extension will be helpful for our construction of ancilla-free designs and PRUs.

We prove Lemma 1 in Appendix D.1 using the path-recording framework from [42]. We find that the path-recording framework enables the most effective analyses of strong random unitaries. This contrasts with standard approximate unitary designs and PRUs, where other succinct approaches based on the permutation group are possible [36, 39].

⁵For strong unitary k -designs, we set $\xi = \mathcal{O}(\log nk/\varepsilon)$ (Theorem 5) which yields a circuit $\mathcal{O}(\log k \log \log nk/\varepsilon)$ for the 2ξ -qubit LRFC unitary k -design. We then add this to the 2-design circuit depth and note that $\mathcal{O}(\log n + \log k \log \log nk/\varepsilon) = \mathcal{O}(\log n + \log k \log \log k/\varepsilon)$. For strong PRUs, we set $\xi = \omega(\log n)$ (Theorem 6), which yields circuit depth $\text{poly}(\log \log n)$ for the 2ξ -qubit LRFC PRU. This is sub-leading to the 2-design circuit depth $\mathcal{O}(\log n)$.

4.3 Ancilla-free pseudorandom unitaries

In this section, we give the first constructions of ancilla-free PRUs and strong PRUs. Our main cryptographic building block will be pseudorandom functions [77] computable in the complexity class “logspace-uniform TC^1 ”. A function is computable in logspace-uniform TC^1 if (1) it is computable by a family of $\mathcal{O}(\log n)$ -depth circuits with large fan-in threshold gates and (2) this family of circuits is output by a logspace Turing machine on the input 1^n . Crucially, it is known that such PRFs exist under the LWE assumption [78], and that this construction is post-quantum secure [74].

To construct ancilla-free PRUs, we prove (under standard cryptographic assumptions) the existence of an intermediate object: an “ancilla-independent” strong PRU. We say that an $(n + a)$ -qubit circuit implements an n -qubit unitary U in an ancilla-independent way if the circuit act as $U \otimes \mathbb{I}_{2^a}$. Note that the standard notion of a PRU only requires that the ancilla is undisturbed when it is initialized to the all 0 state; in comparison, an ancilla-independent implementation requires that the ancilla is undisturbed no matter how it is instantiated.

Theorem 7. *Assuming that there exist polynomially secure (respectively, sub-exponentially secure) post-quantum PRFs computable in logspace-uniform TC^1 , there exist polynomially secure (respectively, sub-exponentially secure) ancilla-independent strong PRUs.*

We show this by instantiating the LRFC ensemble with ancilla-independent implementations of the underlying pseudorandom functions. Towards this goal, our main technical result on ancilla-free computation is as follows.

Theorem 8. *Let $f : \{0, 1\}^n \rightarrow \mathbb{Z}_q^m$ be any logspace-uniform TC^1 -computable function, where $q = O(1)$. Then, there is a $\text{poly}(n, m)$ -size reversible circuit implementing the permutation*

$$(x, y, a) \mapsto (x, y + f(x) \bmod q, a), \quad (4.2)$$

where a denotes an arbitrary setting of the ancilla register.

To prove Theorem 8, we leverage and build upon recent work on catalytic quantum computation [79]. Based on this work, it is known that logspace-uniform TC^1 functions can be implemented in a *somewhat* ancilla-independent way. Namely, they require $\text{poly}(n)$ ancilla qubits but only $O(\log n)$ clean ancilla qubits: if the clean ancillae are all initialized to $|0\rangle$, the circuit properly computes the function and acts as identity on the remaining ancillae. In Section E, we show how to remove the need for these last $\mathcal{O}(\log n)$ clean ancillae by exploiting a number of reversible circuit identities.

From ancilla-independent PRUs to ancilla-free PRUs. Finally, to compile ancilla-independent strong PRUs into ancilla-free strong PRUs, we instantiate the scrambled two-layer ensemble with ancilla-independent strong PRUs on n^ϵ qubits each, where ϵ is a constant greater than zero. Crucially, the strong PRU blocks can *reuse* registers that serve as the ancilla registers of other PRU blocks, due to their ancilla-independence. This gives ancilla-free strong PRUs on n qubits of $\text{poly}(n)$ depth. To compress the depth down to $\text{poly}(\log n)$, we instantiate the two-layer ensemble again, with

- $\omega(\log^2 n)$ -depth ancilla-free instantiations of the unitary 2-designs; see Lemma 2 of the following section and set $\varepsilon^{-1} = \omega(\text{poly } n)$, and
- ancilla-free PRUs on $\text{poly}(\log n)$ qubits each, which have depth $\text{poly}(\log n)$. Note that for these to be secure against all $\text{poly}(n)$ -time adversaries, we need to assume that the underlying cryptography is sub-exponentially secure.

This yields $\text{poly}(\log n)$ -depth strong ancilla-free PRUs.

Theorem 9. *Assuming post-quantum PRFs computable in TC^1 , there exist ancilla-free strong PRUs. Moreover, assuming sub-exponentially secure post-quantum PRFs computable in TC^1 , there exist ancilla-free strong PRUs computable in depth $\text{poly}(\log n)$ with all-to-all circuits.*

Since logspace-uniform TC^1 -computable PRFs are known under the LWE assumption [78], we obtain instantiations of our results under LWE.

Corollary 1. *Assuming the post-quantum hardness of LWE there exist ancilla-free PRUs. Assuming the sub-exponential post-quantum hardness of LWE, there exist ancilla-free strong PRUs computable in depth $\text{poly}(\log n)$ with all-to-all circuits.*

4.4 Strong unitary designs from local random circuits

We now present our final construction of strong random unitaries, in all-to-all-interacting local random circuits with a specific architecture. This demonstrates that the fast formation of strong random unitaries is possible even in highly unstructured ensembles, complementing our highly structured implementations thus far. This generality is not trivial; for example, standard unitary designs can be implemented in circuit depth $\mathcal{O}(\log \log n)$ in highly structured unitary ensembles, but require depth $\Omega(\log n)$ in local random circuits on any architecture [36, 39, 80].

Our random circuit construction builds upon the scrambled two-layer ensemble introduced in the previous section [Fig. 2(c)]. We modify the ensemble in two ways to enable a random circuit realization. First, we replace both of the n -qubit unitary 2-designs with blocked fast scrambling circuits, composed of small unitary 2-designs acting on 2ξ qubits each. The small unitary 2-designs are arranged such that the i -th patch of qubits is coupled to the $(i + 2^{d-1})$ -patch of qubits at the d -th circuit layer. This guarantees that the light-cone of every qubit doubles at every circuit layer, so that every light-cone encompasses all n qubits after $\log_2(n/\xi)$ layers. Second, we replace all of the small random unitaries in the ensemble with 1D local random circuits [32]. We specify the depths of these circuits below. The circuit is highly unstructured, in the sense that each two-qubit gate is drawn independently at random from the Haar measure on $U(4)$.

To prove that the first modification is valid, we show that the blocked fast scrambling circuit is a strong unitary 2-design.

Lemma 2 (The blocked fast scrambling circuit is a strong unitary 2-design). *Let each small random unitary be a strong $\frac{\varepsilon}{n}$ -approximate unitary 2-design with depth d . Then the blocked fast scrambling circuit forms a strong ε -approximate unitary 2-design with depth $d \log_2(n/\xi)$ for any $\xi \geq \log_2(5n/\varepsilon)$.*

We then prove that each small strong approximate unitary design can be replaced with a 1D local random circuit.

Lemma 3 (1D random circuits are strong unitary k -designs). *1D random circuits on n qubits form strong ε -approximate unitary k -designs in depth $d = \Omega(\log(k)^7(nk + \log(1/\varepsilon)))$ for any $\varepsilon \geq 2k^2/2^n$.*

This requires circuit depth $\mathcal{O}(\text{poly} \log k(\xi k + \log n/\varepsilon))$ for the two layers of small unitary k -designs, and depth $\mathcal{O}(\xi + \log n/\varepsilon)$ per layer for the $\log_2(n/\xi)$ layers of small unitary 2-designs. Setting $\xi = \mathcal{O}(\log nk/\varepsilon)$ as in Theorem 5 yields a total circuit depth of $\mathcal{O}(k \cdot \text{poly} \log k \cdot \log n/\varepsilon + \log n \cdot \log nk/\varepsilon)$.

The proofs of Lemma 2 and Lemma 3 are contained in Appendix D.2 and A.4, respectively. We prove Lemma 2 by establishing a formal connection between operator spreading and strong unitary 2-designs. Operator spreading refers to the growth in support of initially local operators under a quantum circuit or time dynamics; this signifies the scrambling of local information into non-local correlations [25, 26, 52]. In random circuits, this growth is probabilistic and is characterized by a probability distribution over the set of Pauli strings [55]. We show that an ensemble forms a strong

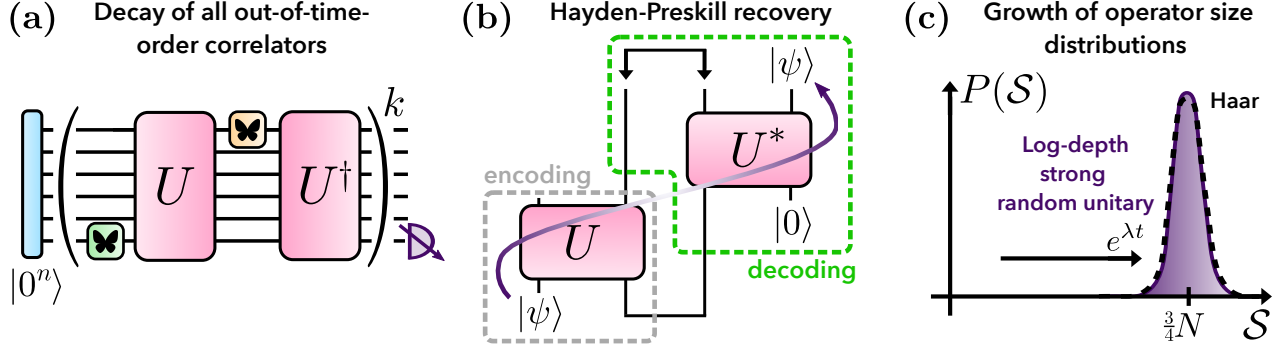


Figure 4: By allowing queries to $U^\dagger$ and U^* , strong random unitaries capture hallmark features of quantum information scrambling. **(a)** In a strong unitary k -design, every k -point time-ordered and out-of-time-order correlation function decays to near zero with high probability. **(b)** Strong random unitaries are good encoders of quantum information, as in the Hayden-Preskill thought experiment [21]. This follows because the decoding protocol uses the conjugate random unitary [45]. **(c)** In a strong unitary 4-design or strong pseudorandom unitary, the operator size distribution approaches its Haar-random value to within small total variational distance.

unitary 2-design if and only if its operator spreading distributions are close to those of a Haar-random unitary. To establish that the blocked fast scrambling circuit satisfies this condition, we prove that with high probability every operator is randomly supported within its light-cone at every layer.

The statement of Lemma 3 for strong unitary designs closely parallels an analogous statement for standard unitary designs [34]. These statements are derived by translating lower bounds on the spectral gap of random circuits to upper bounds on their design depth [32]. This translation involves several steps: One first uses the spectral gap to bound the so-called additive error of a unitary design, and then translates the additive error to a bound on the relative error. For standard unitary designs, this translation can either be proven using the Schur-Weyl duality [32] or from elementary properties of the permutation operators [36]. In Appendix A.1, we provide an analogous additive-to-relative-error translation result for strong unitary designs. Our analysis yields numerous insights into the structure of the mixed Haar twirl, which may be useful in other contexts. For example, we formalize the following statement: Within any quantum experiment, a Haar-random unitary U and its inverse $U^\dagger$ either cancel one another, or behave identically to two independent random unitaries U and V .

5 Fast scrambling

We now elaborate on the connections between our results and fast quantum information scrambling. Quantum information scrambling is a broad field focused on understanding the spreading of quantum information in dynamical many-body quantum systems. As discussed in detail in our introduction, the *fast scrambling* conjecture [20] posits that (i) all-to-all-connected quantum systems can scramble information in time growing only logarithmically in the system size n , and (ii) this is the fastest that any quantum system can scramble information.

Our construction of strong unitary k -designs and strong pseudorandom unitaries in $\mathcal{O}(\log n)$ circuit depth provides the strongest confirmation to date of the fast scrambling conjecture. These results prove that every observable feature of unitary quantum dynamics can mimic Haar-random behavior in logarithmic depth. This significantly expands upon existing works, which, as aforementioned, focus on either a small number of specific signatures or solely unitary 2-design properties [26, 62–71]. Meanwhile, our lower bound, which is simple to derive, confirms that a logarithmic depth is optimal

for any unitary to appear Haar-random in experiments that involve the inverse or conjugate.

We illustrate the connection between strong unitary designs and strong PRUs and quantum information scrambling in more detail through several examples (Fig. 4). We consider four hallmark diagnostics of quantum information scrambling: (a) the decay of all local time-ordered and out-of-time-order correlation functions [25], (b) the Hayden-Preskill thought experiment [21], (c) the saturation of operator size distributions to their Haar-random profile [26], and (d) the growth of the entanglement and operator entanglement entropies. The implications of our results for each behavior follow straightforwardly from our definitions of strong unitary k -designs and strong PRUs. We discuss this example-by-example below.

Decay of all out-of-time-order correlation functions. Perhaps the simplest diagnostic of scrambling is the decay of all local correlation functions to zero [53]. This includes both conventional *time-ordered* correlations functions (TOCs), as well as *out-of-time-order* correlations functions (OTOCs) [25]. The former can be measured with forward time-evolution under U . Crucially however, the latter can only be efficiently measured by alternating forward and backward time-evolution under U and $U^\dagger$ [Fig. 4(a)]. In Appendix G, we provide a short proof that all local k -point correlation functions are near zero with high probability in any strong unitary $2k$ -design. A similar statement holds for strong PRUs. This complements existing observations that OTOCs can decay in logarithmic time in the Sachdev-Ye-Kitaev model [62, 63] and all-to-all-connected random circuits [24, 56]. Our results capture both standard four-point OTOCs as well as higher-point OTOCs, which have risen in interest in recent work [10, 81–84].

Hayden-Preskill thought experiment. A key inspiration for early studies of quantum information scrambling came from the black hole information paradox [85]. In this context, Hayden and Preskill proposed that, if one models the dynamics of a black hole by a random unitary, then one could use the Hawking radiation collected from a black hole to recover a quantum state that fell into the black hole at an earlier time [21]. An explicit decoding protocol was later provided by Yoshida and Kitaev [45]. Crucially, the decoding protocol utilizes the conjugate random unitary U^* [Fig. 4(b)]. Thus, any strong unitary 2-design or strong pseudorandom unitary will encode information precisely as well as a Haar-random unitary in the Hayden-Preskill thought experiment⁶. Intriguingly, this result does not seem to extend to all applications of Haar-random unitaries as quantum codes; in particular, it applies only when the decoding can be performed *efficiently* using query access to U , $U^\dagger$, U^* , U^T .

Growth of operator size distributions. An even more fine-grained diagnostic of quantum information scrambling is the *operator size distribution* [26]. The size distribution characterizes the support of a time-evolved operator when expanded in the Pauli basis, $O(t) \equiv UOU^\dagger = \sum_P c_P(t)P$. Specifically, $P(\mathcal{S}) \equiv \sum_{|P|=\mathcal{S}} |c_P(t)|^2$, where the sum is over all Pauli operators of weight (i.e. *size*) $\mathcal{S}$. Operator size distributions are central to applications of information scrambling in quantum gravity [22–24, 26], quantum sensing [86], and understanding the impact of noise on quantum systems [47, 56, 60]. In Appendix G, we prove that the operator size distribution of any strong ε -approximate unitary 4-design is $n^2\varepsilon$ -close to its Haar-random value in total variational distance. Setting $\varepsilon = 1/\omega(\text{poly } n)$ yields operator size distributions that are super-polynomially close to their Haar values in circuit depth $\mathcal{O}(\log n)$.

⁶We note that the original work by Hayden and Preskill [21] utilized an early definition of approximate unitary 2-designs [31] that in fact bears some resemblance with our strong definition. This definition fell out of use in later works which focused on unitary k -designs for general k .

Entanglement and operator entanglement entropy. Finally, we consider the entanglement and operator entanglement entropies. In principle, neither of these quantities can be efficiently measured in any quantum experiment. Therefore their values in a Haar-random state need not be replicated by approximate strong unitary designs or strong PRUs. Nonetheless, in Appendix G, we show that an especially precise form of strong unitary designs, characterized by a small *relative error*, can efficiently capture the entanglement and operator entanglement entropies. In Appendix C, we show that such designs can be formed in $\mathcal{O}(\log n)$ circuit depth. From this, we find that the Renyi-2 entanglement entropy of any subsystem of any time-evolved state $|\psi(t)\rangle \equiv U|\psi\rangle$ reaches its Haar-random value in $\mathcal{O}(\log n)$ depth. In addition, the Renyi-2 operator entanglement entropy of any subsystem of any time-evolved operator $O(t) \equiv UOU^\dagger$ reaches its Haar-random value in $\mathcal{O}(\log n)$ depth. Formally, these bounds are achieved by reformulating each entropy as the expectation value of a positive-valued operator after U and U^* are applied to a fictitious larger system.

6 Discussions

Our results provide the strongest constructions of approximate unitary designs and PRUs to date. Moreover, the circuit depths of our constructions achieve the optimal $\Theta(\log n)$ scaling, as predicted by the fast scrambling conjecture. These results establish a rigorous operational foundation for quantum information scrambling and represent the most comprehensive confirmation of fast scrambling to date, capturing all efficiently observable quantum experiments. Our work leaves open several interesting questions.

We have motivated strong unitary designs and strong PRUs from applications to quantum information scrambling and black hole physics. What other applications of strong random unitaries might exist? For example, can strong unitary designs help us understand the classical hardness of recent quantum advantage proposals involving time-reversal dynamics [10, 61]? Or perhaps the sensitivity of such experiments to experimental noise [56]? More broadly, can strong random unitaries assist in device benchmarking and other quantum learning tasks?

Our constructions provide the first examples of PRUs secure against queries to all of U , $U^\dagger$, U^* , and U^T . Can the existence of these strong PRUs and the ability to generate them in logarithmic depth enable new quantum cryptographic applications [46]? Our ancilla-free constructions address a fundamental limitation of previous PRU constructions, which relied on auxiliary systems that are unrealistic in physical settings. This advance opens a deeper question: can we build upon ancilla-free strong random unitaries to demonstrate that dynamics naturally arising in condensed matter, quantum chaos, and high-energy physics form strong random unitaries?

More broadly, giving ancilla-free constructions of *any* quantum cryptographic object—such as commitments, encryption, uncloneable cryptography, etc.—can constitute a stronger form of evidence (compared to a pure existential result) that natural physical phenomena may possess these cryptographic properties. This motivates understanding whether, and under what hardness assumptions, other quantum cryptographic primitives have efficient ancilla-free instantiations.

Finally, our new techniques for analyzing strong random unitaries raise several questions. Can the circuit depth of our local random circuit construction of strong unitary designs be further improved, from $\mathcal{O}(\log^2 n)$ to $\mathcal{O}(\log n)$? In particular, our treatment of the blocked fast scrambling circuit is extremely coarse and likely leaves room for an improved analysis. Along similar lines, can one further remove the structure from our random circuit designs, and prove the fast formation of strong unitary designs in the standard model of all-to-all random circuits [64–66]? More broadly, can our refined techniques for analyzing the mixed-unitary twirl [87–89], and quantum experiments involving inverse and conjugate unitaries, yield any new progress or insights elsewhere in quantum information theory?

Acknowledgments:

We are grateful to Laura Cui, Jonas Haferkamp, and Nicholas Hunter-Jones for valuable discussions. 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, with which T.S., F.B., and H.H. are affiliated, is an NSF Physics Frontiers Center (NSF Grant PHY-2317110). This work was done while F.M. was a postdoctoral fellow at the Simons Institute for the Theory of Computing, supported by DOE QSA grant FP00010905, NSF QLCI Grant 2016245 and DOE grant DE-SC0024124.

Appendices

Our Appendices are organized as follows. In Appendix A, we provide the full details of our results on strong unitary designs. In Appendix B, we provide the full details of our results on strong pseudorandom unitaries. In Appendix C, we prove that the LRFC ensemble forms a strong unitary design and strong PRU. In Appendix D, we prove our gluing results for strong unitary designs and strong PRUs. In Appendix F, we provide additional details on the mixed Haar twirl, which are used to prove a translation lemma for the approximation errors of strong unitary designs in Appendix A. In Appendix G, we provide full details on our applications of strong random unitaries to scrambling.

Contents

A Strong unitary designs	17
A.1 Preliminaries and definitions	17
A.2 The mixed Haar twirl and strong unitary designs	23
A.3 Proof of Lemma 2: Strong unitary 2-designs from blocked fast scrambling random circuits	28
A.4 Proof of Lemma 3: Strong unitary k -designs from 1D random circuits	31
A.5 Proof of Theorem 1	32
A.6 Lower bounds on the depth of strong unitary designs	32
B Strong pseudorandom unitaries	34
B.1 Definitions	34
B.2 Preliminaries	35
B.3 The purified permutation-function oracle	38
B.4 The path-recording oracle V and its conjugate $\bar{V}$	40
B.5 Partial path-recording oracle W and its conjugate $\bar{W}$	41
B.6 $V, \bar{V}$ approximates Haar-random unitary U under $U, U^\dagger, U^*, U^T$	44
C The Luby-Rackoff-Function-Clifford (LRFC) ensemble	46
C.1 Definition of the ensemble	46
C.2 Purified Luby-Rackoff-Function oracle	47
C.3 Projecting onto the local distinct subspace	48
C.4 LRFC is indistinguishable from a Haar-random unitary	55
C.5 Proof of Theorem 3: LRFC is a strong unitary design	56
C.6 Proof of Theorem 4: LRFC is a strong PRU	56

D	Gluing strong random unitaries	56
D.1	Proof of Lemma 1: Gluing strong random unitaries	56
D.2	Proof of Theorems 5 and 6	66
D.3	Proof of Theorems 1 and 2	67
E	Ancilla-free pseudorandom unitaries	67
E.1	Ancilla-preserving reversible computation of functions	68
E.2	Constructing ancilla-independent PRUs	71
E.3	Constructing ancilla-free PRUs	72
F	Analysis of the mixed Haar twirl	72
F.1	Reformulating the mixed Haar twirl	73
F.2	Additional results on the mixed Haar twirl	83
G	Fast scrambling	91
G.1	Out-of-time-order correlation functions	91
G.2	Operator size distributions	92
G.3	Entanglement and operator entanglement entropy.	93

A Strong unitary designs

In this Appendix, we provide the full details of our definition and constructions of strong unitary designs. Beyond the first preliminaries and definitions section, we have structured each subsection so that they can be read relatively independently of one another.

A.1 Preliminaries and definitions

In this section, we introduce and define strong unitary k -designs for various notions of approximation error. Our definitions are closely modeled on the analogous definitions for (standard) unitary k -designs. With this in mind, we first review the standard definitions of unitary designs. We then briefly discuss the limitations of these definitions in regards to fast scrambling and quantum experiments involving time-reversal. We then introduce our strong definitions to capture such behaviors.

A.1.1 Averaging over Haar-random unitaries

To provide the definitions of unitary designs, let us first introduce the average (i.e. *twirl*) over a Haar-random unitary. This will form our point of comparison in the study of unitary designs. We consider two varieties of the twirl in our work: the Haar twirl and the mixed Haar twirl.

The Haar twirl. The Haar twirl has the following definition.

Definition 1 (The Haar twirl). *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:*

$$\Phi_H^{(k)}(X) = \int dU U^{\otimes k} X (U^\dagger)^{\otimes k}. \quad (\text{A.1})$$

An explicit formula for the Haar twirl can be derived from a simple argument in representation theory [90–92]. This yields the following expression.

Lemma 4 (Explicit expression for the Haar twirl). *For any $k \leq 2^n$. 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*

$$\Phi_H^{(k)}(X) = \sum_{\pi, \tilde{\pi} \in S_k} W_{g_{\pi, \tilde{\pi}}} \cdot \text{tr}(X \pi^{-1}) \cdot \tilde{\pi}, \quad (\text{A.2})$$

where $\pi, \tilde{\pi} \in S_k$ permute the k copies of the n -qubit Hilbert space, and the Weingarten matrix elements $W_{g_{\pi, \tilde{\pi}}}$ depend on k and the Hilbert space dimension 2^n .

The mixed Haar twirl. To incorporate quantum experiments that can query the inverse and conjugate of a random unitary, we will also make use of the mixed Haar twirl in our work. Here, the k copies of the unitary U are replaced by p copies of U and q copies of its conjugate U^* .

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

$$\Phi_H^{(p, q)}(X) = \int dU (U^{\otimes p} \otimes U^{*, \otimes q}) X (U^{\dagger, \otimes p} \otimes U^{T, \otimes q}). \quad (\text{A.3})$$

The mixed Haar twirl can be obtained from the standard Haar twirl by taking the partial transpose of the last q registers before and after $(U^*)^{\otimes q}$ is applied. Thus, the expression for the mixed Haar twirl is fully determined by the expression for the standard Haar twirl.

Lemma 5 (Explicit expression for the mixed Haar twirl). *For any $p+q \leq 2^n$. For any linear operator X acting on nk qubits, the (p, q) -th moment with respect to the unitary group can be written*

$$\Phi_H^{(p, q)}(X) = \sum_{\pi, \tilde{\pi} \in S_k} W_{g_{\pi, \tilde{\pi}}} \cdot \text{tr}(X (\pi^{-1})^\Gamma) \cdot \tilde{\pi}^\Gamma, \quad (\text{A.4})$$

where Γ is the partial transpose on the final q registers.

Proof. The expression follows from the equality $\Phi_H^{(p, q)}(X) = \Phi_H^{(k)}(X^\Gamma)^\Gamma$. The partial transpose Γ is then transferred from X to π^{-1} inside the trace using $\text{tr}(A^\Gamma B) = \text{tr}(AB^\Gamma)$. $\square$

A.1.2 Approximate unitary designs

Let us now turn to unitary designs. A unitary ensemble is an exact unitary k -design if it exactly replicates the first k moments of a Haar-random unitary.

Definition 3 (Exact unitary k -design). *An ensemble of unitaries $\mathcal{E}$ is an exact unitary k -design if it exactly reproduces the first k moments of the Haar measure*

$$\Phi_{\mathcal{E}}^{(k)} = \Phi_H^{(k)} \quad (\text{A.5})$$

where we have used the abbreviated notation

$$\Phi_{\mathcal{E}}^{(k)}(X) = \mathbb{E}_{U \sim \mathcal{E}} U^{\otimes k} X (U^\dagger)^{\otimes k} \quad (\text{A.6})$$

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

An exact design is the strongest notion of unitary design. It guarantees that any experiment that queries the unitary U (or $U^\dagger$ or U^T or U^* or controlled versions of any of these quantities) up to k times exactly reproduces the output of the same experiment querying a Haar-random unitary⁷.

In practice, exact constructions of unitary designs are extremely scarce beyond very low moments $k \leq 3$. This motivates the notion of an *approximate* design. Three forms of approximation error for unitary designs are common.

Additive error. The simplest form of approximation error is the additive or diamond-norm error.

Definition 4 (Unitary k -design with additive error). *Let $\varepsilon > 0$. An ensemble of unitaries $\mathcal{E}$ is an approximate unitary k -design with additive error ε if*

$$\left\| \Phi_{\mathcal{E}}^{(k)} - \Phi_H^{(k)} \right\|_{\diamond} \leq \varepsilon, \quad (\text{A.7})$$

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

Physically, the additive error is equivalent to security under parallel queries to the unitary U . Namely, 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 [39]. This follows immediately from the definition of the diamond norm.

Measurable error. The additive error has a significant drawback, in that it can only capture experiments in which U is applied k times in parallel. To address this, Ref. [39] introduced a stronger notion of approximation error, which guarantees that an ensemble is indistinguishable from Haar-random in *any* quantum experiment that queries U up to k times. This is termed the *measurable error* owing to its physical motivation.

Definition 5 (Unitary k -design with measurable error). *Let $\varepsilon > 0$. An ensemble of unitaries $\mathcal{E}$ is an approximate unitary k -design with 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,*

$$\sup_{W_1 \cdots W_{k+1}} \|\rho_{\mathcal{E}} - \rho_H\|_1 \leq \varepsilon, \quad (\text{A.8})$$

where we have used the notation

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

to denote the expected output state of a general quantum experiment that queries U k times. Each W_i is an arbitrary unitary on $n + m$ qubits, where the number m of ancilla qubits may be arbitrarily large.

In the definition, we can assume without loss of generality that each U is applied in sequence on the same subsystem A of n qubits. If the unitaries are in fact applied in parallel, this is equivalent to performing the first unitary U , then using W_1 to swap A with n ancilla qubits, then performing the second unitary U , then using W_2 to swap back A and the n ancilla qubits, and so on.

The measurable error is in some sense the most natural notion of approximation error for unitary designs. It captures precisely the features of a random unitary that can be measured in physical experiments that query the unitary.

⁷For experiments involving controlled queries, one should also assume that the unitary ensemble $\mathcal{E}$ is invariant under a random global phase $e^{i\phi}$. This guarantees that all un-matched moments, such as $\mathbb{E}_{U \sim \mathcal{E}} [U^{\otimes k}(\cdot) U^{\otimes k'}]^\dagger$ for $k \neq k'$, vanish. Equality of the matched moments (Definition 3) then guarantees that all controlled queries to a Haar-random unitary are exactly reproduced by controlled queries to a unitary sampled from $\mathcal{E}$.

Relative error. The strongest notion of approximation error for unitary designs is the relative error. Unlike the additive or measurable errors, the relative error is sensitive to properties that cannot be efficiently measured in any quantum experiment. It has the following definition.

Definition 6 (Unitary k -design with relative error). *Let $\varepsilon > 0$. Then an ensemble of unitaries $\mathcal{E}$ is an approximate unitary k -design up to relative error ε if*

$$(1 - \varepsilon)\Phi_H^{(k)} \preceq \Phi_{\mathcal{E}}^{(k)} \preceq (1 + \varepsilon)\Phi_H^{(k)}, \quad (\text{A.9})$$

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

Physically, an ensemble $\mathcal{E}$ is an approximate unitary k -design up to relative error ε if and only if for any quantum experiment with k queries to U (or U^T), the expectation value of any positive-valued operator χ is equal to its Haar value to within multiplicative precision, $(1 - \varepsilon)\text{tr}(\chi\rho_H) \leq \text{tr}(\chi\rho_{\mathcal{E}}) \leq (1 + \varepsilon)\text{tr}(\chi\rho_H)$. This holds even if the expectation value is exponentially small and cannot be efficiently measured.

Translating between unitary design approximation errors. We can translate between different notions of approximation error for unitary designs as follows.

Lemma 6 (Translating between different approximation errors [32, 36, 39]). *The additive error ε_a is upper bounded by the measurable error ε_m , which is in turn upper bounded by twice the relative error ε_r ,*

$$\varepsilon_a \leq \varepsilon_m \leq 2\varepsilon_r. \quad (\text{A.10})$$

Conversely, the relative error is bounded by the additive error times an exponentially large pre-factor,

$$\varepsilon_r \leq 2^{nk} \binom{2^n + k - 1}{k} \varepsilon_a \leq \left(\frac{4^{nk}}{k!}\right) \left(1 + \frac{k^2}{2^n}\right) \varepsilon_a, \quad (\text{A.11})$$

where the second inequality holds for $k^2 \leq 2^n$.

A.1.3 Strong approximate unitary designs

We can now introduce our strong notions of approximation error for unitary designs. To do so, let us first highlight the weakness of standard definitions towards capturing experiments that query the inverse or conjugate of a random unitary. We then introduce our definitions to resolve this.

Weakness of standard definitions of approximate unitary designs. We can illustrate the weakness of standard definitions of approximate unitary designs with two examples. The examples involve experiments that perform one query to U and one query to either the inverse or the conjugate. We show that both experiments can easily distinguish any low-depth unitary from Haar-random. Since low-depth circuits can form relative error unitary designs, this implies that such designs are not sufficient for bounding properties of such experiments. At a formal level, the translation from the relative error to the trace-norm error in the output of an experiment querying the inverse or conjugate incurs an exponential factor of 2^n , which ruins the error bound when the number of qubits n is large.

Our first and simplest example involves the inverse unitary [93, 94]. Consider a quantum experiment that prepares the zero state on all qubits, scrambles the system via U , then applies a Pauli operator X_1 on the first qubit, then attempts to un-scramble the system via $U^\dagger$. If U is Haar-random, the Pauli perturbation completely disrupts the time-reversal, resulting in an effectively Haar-random state after $U^\dagger$ is applied. On the other hand, if U is low-depth, all qubits outside of the light-cone of

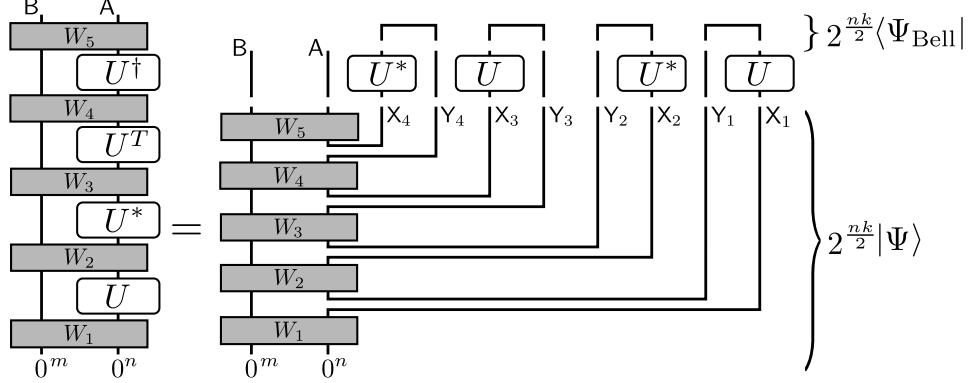


Figure 5: Reformulation of any quantum experiment that makes any k queries to U , U^* , U^T , or $U^\dagger$ as an alternative experiment that makes a single query to $U^{\otimes p} \otimes U^{*, \otimes q}$ and performs k post-selections on n -qubit Bell states. Here, p counts the number of applications of U and U^T and q counts the number of applications of U^* and $U^\dagger$. The subsystem labels match the notation used in our proofs based on the path-recording framework (Appendix D.1 and C).

the first qubit return to the zero state under $U^\dagger$. Hence, one can measure e.g. the fidelity for the last qubit to return to the zero state to easily distinguish any low-depth unitary from Haar-random.

Our second example is similar but replaces the inverse unitary with the conjugate. Consider an experiment that prepares the EPR state between two copies of n qubits, applies a Pauli operator X_1 on the first qubit of the left side, then applies U and U^* in parallel to the left and right side. This yields the state $(U \otimes U^*)(X_1 \otimes \mathbb{1}) |\Psi_{\text{EPR}}\rangle = (UX_1 U^\dagger \otimes \mathbb{1}) |\Psi_{\text{EPR}}\rangle$, where we use that $(\mathbb{1} \otimes O) |\Psi_{\text{EPR}}\rangle = (O^T \otimes \mathbb{1}) |\Psi_{\text{EPR}}\rangle$ for any operator O . When U is Haar-random, the operator $UX_1 U^\dagger$ is a seemingly random operator on all n qubits. This implies that the fidelity for any pair of qubits between the left and right side to be in the EPR state is close to its maximally mixed value, $1/4$. On the other hand, when U is low depth, the operator $UX_1 U^\dagger$ has support only on a small light-cone around the first qubit. Thus, the fidelity of e.g. the last pair of qubits to remain in the EPR state is equal to 1. Hence, one can again easily distinguish any low-depth unitary from Haar-random.

Strong measurable error. We can now introduce our definitions of strong unitary designs. We introduce each definition in order of its prominence in our work.

We begin with the strong analog of the measurable error. We say that a unitary ensemble is a strong unitary design with measurable error if it is indistinguishable from a Haar-random unitary in any quantum experiment with any combination k queries to U or $U^\dagger$ or U^T or U^* .

Definition 7 (Strong unitary k -design with measurable error). *Let $\varepsilon > 0$. An ensemble of unitaries $\mathcal{E}$ is a strong approximate unitary k -design with measurable error ε if for any quantum experiment with any combination of k queries to U or $U^\dagger$ or U^T or U^* , the output states when U is sampled from $\mathcal{E}$ versus the Haar ensemble are ε -close in trace distance,*

$$\sup_{W_1 \dots W_{k+1}, U_1 \dots U_k} \|\rho_{\mathcal{E}} - \rho_H\|_1 \leq \varepsilon, \quad (\text{A.12})$$

where we have used the notation

$$\rho_{\mathcal{E}} = \mathbb{E}_{U \sim \mathcal{E}} \left[W_{k+1} [U_k \otimes \mathbb{1}_m] \dots W_2 [U_1 \otimes \mathbb{1}_m] W_1 |0^{n+m}\rangle \langle 0^{n+m}| W_1^\dagger [U_1^\dagger \otimes \mathbb{1}_m] W_2^\dagger \dots [U_k^\dagger \otimes \mathbb{1}_m] W_{k+1}^\dagger \right]$$

to denote the expected output state of a general quantum experiment, where W_i are arbitrary unitaries for each $i = 1, \dots, k+1$ and $U_i \in \{U, U^\dagger, U^T, U^*\}$ for each $i = 1, \dots, k$.

Due to its natural definition, we will adopt the strong measurable error as our default error metric for strong unitary designs. Hence, in later sections, we will often refer to an *approximate unitary k -design with measurable error ε* as simply an ε -approximate unitary k -design.

Strong relative error. We can also define analogs of the relative error and additive error for strong unitary designs. These share similar drawbacks to the definitions of the relative and additive error for standard unitary designs (as discussed in the previous section). Nonetheless, they will be convenient for select technical purposes in our analysis. For convenience, we state the definitions in terms of the number of queries p to U or U^T and the number of queries q to U^* or $U^\dagger$, instead of the total number of queries $k = p + q$.

Definition 8 (Unitary (p, q) -design with relative error). *Let $\varepsilon > 0$. Then an ensemble of unitaries $\mathcal{E}$ is an approximate unitary (p, q) -design with relative error ε if*

$$(1 - \varepsilon)\Phi_H^{(p,q)} \preceq \Phi_{\mathcal{E}}^{(p,q)} \preceq (1 + \varepsilon)\Phi_H^{(p,q)}. \quad (\text{A.13})$$

The relative error guarantees that the expectation value of any positive-valued operator χ in the output state of any quantum experiment that performs any combination of p queries to U or $U^\dagger$ and q queries to U^T or U^* , is equal to its Haar value to within multiplicative precision. This follows from the fact that any such experiment can be reformulated as an experiment that performs p and q parallel queries to U and U^* and post-selects on the EPR state (Fig. 5).

Strong additive error. Finally, we define the additive error for strong unitary designs as follows.

Definition 9 (Unitary (p, q) -design with additive error). *Let $\varepsilon > 0$. An ensemble of unitaries $\mathcal{E}$ is an approximate unitary (p, q) -design with additive error ε if*

$$\left\| \Phi_{\mathcal{E}}^{(p,q)} - \Phi_H^{(p,q)} \right\|_{\diamond} \leq \varepsilon. \quad (\text{A.14})$$

Physically, the additive error is equivalent to security under p parallel queries to U and q parallel queries to U^* . In principle, one could extend this definition to include parallel queries to $U^\dagger$ and U^T as well. However, the only use of the additive error in our work is as a stepping stone to prove small relative and measurable errors, and the current definition will be sufficient for these purposes.

Translating between strong unitary design approximation errors. As in the standard case, it is possible to translate between different notions of approximation error for strong unitary designs. We formalize this in the following lemma. The first statement of the lemma follows immediately from the definitions of the approximation errors. The second statement is a significant result of our work. We provide the proof of the second statement in Section A.2.

Lemma 7 (Translating between different strong approximation errors). *Let $k = p + q$. The strong additive error $\varepsilon_a^{(p,q)}$ is upper bounded by the strong measurable error $\varepsilon_m^{(k)}$, which is in turn upper bounded by twice the strong relative error $\varepsilon_r^{(p,q)}$,*

$$\varepsilon_a^{(p,q)} \leq \varepsilon_m^{(k)} \leq 2\varepsilon_r^{(p,q)}. \quad (\text{A.15})$$

Conversely, the strong relative error is bounded by the strong additive error as follows,

$$\varepsilon_r^{(p,q)} \leq \left(\frac{4^{n(p+q)}}{p!q!} \right) 2\varepsilon_a^{(p,q)} + \frac{2(p+q)^2}{2^n}, \quad (\text{A.16})$$

for any $2k^2 = 2(p+q)^2 \leq 2^n$.

In Section A.4, we apply the second statement of the lemma to translate existing results on the spectral gap of one-dimensional random circuits into the statement that such circuits form strong unitary designs with small relative error.

A.2 The mixed Haar twirl and strong unitary designs

In this section, we build a basic framework for understanding the structure of the mixed Haar twirl. We first use this framework to derive a simpler approximate formula for the mixed Haar twirl. We then use this approximate formula to prove the second statement of Lemma 7, which allows one to perform tight translations between the additive and relative errors of strong unitary designs.

A.2.1 The approximate mixed Haar twirl

Let us begin by re-printing the formula for the mixed Haar twirl from Lemma 5,

$$\Phi_H^{(p,q)}(X) = \sum_{\sigma, \tau \in S_k^\Gamma} \widetilde{W}_{g_{\sigma, \tau}} \cdot \text{tr}(X \sigma^\dagger) \cdot \tau, \quad (\text{A.17})$$

where $\sigma \equiv \pi^\Gamma$ and $\tau \equiv \tilde{\pi}^\Gamma$ are summed over the *partially transposed permutations*, S_k^Γ . Here, we define $\widetilde{W}_{g_{\sigma, \tau}} \equiv W_{g_{\pi, \tilde{\pi}}}$. While this formula is simple to write down, it provides fairly little intuition about the properties and behavior of the mixed Haar twirl. We begin this section by reformulating this expression in a more intuitive manner. We will then derive our *approximate* expression for the mixed Haar twirl from this reformulation. For brevity, we defer the proofs of several facts stated in our reformulation of the mixed Haar twirl to the later Appendix F. The proofs are straightforward but require many detailed steps.

Unlike the permutation operators, which appear in the standard Haar twirl, the partially transposed permutations are not necessarily unitary. Indeed, a key role in the mixed Haar twirl is played by a subset of partially transposed permutations that are *projectors*. Consider any permutation π that is equal to a tensor product of (i) identity elements, and (ii) swap operations between a copy on the left side and a copy on the right side. Here, the “left side” corresponds to the p copies that U acts on, and the “right side” to the q copies that U^* acts on. When π is partially transposed, it results in a permutation $\sigma = \pi^\Gamma$ that is a tensor product of (i) identity elements, and (ii) EPR projectors between a copy on the left side and a copy on the right side. This follows because the partial transpose of a swap operator is proportional to an EPR projector, $\mathcal{S}_{ij}^\Gamma = 2^n P_{\text{EPR}, ij}$ for copies i, j . If we label the set of pairs between the left and right side as $\alpha_\sigma = \{(i_1, j_1), (i_2, j_2), \dots, (i_{|\alpha_\sigma|}, j_{|\alpha_\sigma|})\}$, then $P_{\alpha_\sigma} \equiv \sigma / 2^{n|\alpha_\sigma|}$ projects onto EPR states on every pair in α_σ and acts trivially on the remaining copies.

In Appendix F, we show that these projectors break up the Hilbert space $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ into a tensor sum of distinct components,

$$\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q} \cong \bigoplus_{\ell=0}^{\min(p,q)} \left(\left[\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)} \right]_{\text{nE}} \otimes \mathcal{A}_\ell \right). \quad (\text{A.18})$$

Here, $\left[\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)} \right]_{\text{nE}}$ denotes the subspace of $\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)}$ that is orthogonal to every EPR projector between a copy i on the left side and j on the right side. Meanwhile, $\mathcal{A}_\ell$ is an auxiliary Hilbert space of dimension $|\mathcal{A}_\ell| = \binom{p}{\ell} \binom{q}{\ell} \ell!$. This equals the number of distinct sets of ℓ pairs between the left and right side. Intuitively, the ℓ -th subspace in the tensor sum contains all states in $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ that have exactly ℓ EPR pairs between the left and right sides. There are $\binom{p}{\ell} \binom{q}{\ell} \ell!$ ways to place the ℓ EPR pairs, which are indexed by the subsystem $\mathcal{A}_\ell$. Once placed, the remaining $p - \ell$ and $q - \ell$ copies are free to be in any quantum state that has zero EPR pairs between the left and right. We

provide a detailed derivation of Eq. (A.18) in Appendix F using only basic properties of the partially transposed permutations.

A crucial property of the EPR state is that it is invariant under the action of $U \otimes U^*$ for any U . This follows because $(U \otimes \mathbb{1})P_{\text{EPR}} = (\mathbb{1} \otimes U^T)P_{\text{EPR}}$ and $U^*U^T = \mathbb{1}$. Hence, when a mixed unitary $(U)^{\otimes p} \otimes (U^*)^{\otimes q}$ is applied to a subspace with exactly ℓ EPR pairs, its action on each of the ℓ EPR pairs becomes trivial. This leaves $p - \ell$ copies of U and $q - \ell$ copies of U^* remaining. To formalize this, for each value of ℓ we define a partial isometry $\tilde{I}_\ell$ (see Appendix F for details) that maps each ℓ -EPR subspace $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ to the ℓ -th Hilbert space on the right side of Eq. (A.18). The partial isometries provide an orthogonal decomposition of the full Hilbert space, $\mathbb{1} = \sum_\ell \tilde{I}_\ell^\dagger \tilde{I}_\ell$, where each $\tilde{I}_\ell^\dagger \tilde{I}_\ell$ projects onto the subspace of exactly ℓ EPR pairs. We then show that one can re-write the mixed Haar twirl as,

$$\Phi_H^{(p,q)}(X) = \mathbb{E}_{U \sim H} \sum_\ell \tilde{I}_\ell^\dagger \left((U)^{\otimes(p-\ell)} \otimes (U^*)^{\otimes(q-\ell)} \otimes \mathbb{1} \right) \tilde{I}_\ell X \tilde{I}_\ell^\dagger \left((U^\dagger)^{\otimes(p-\ell)} \otimes (U^T)^{\otimes(q-\ell)} \otimes \mathbb{1} \right) \tilde{I}_\ell,$$

where the action of the mixed unitary twirl is “pulled” inside each partial isometry to act on the Hilbert space $[\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)}]_{\text{nE}}$. One can then compute each twirl explicitly, which yields

$$\Phi_H^{(p,q)}(X) = \sum_\ell \tilde{I}_\ell^\dagger \left[\sum_{\pi_L \pi_R} \sum_{\tilde{\pi}_L \tilde{\pi}_R} \text{tr} \left(\tilde{I}_\ell X \tilde{I}_\ell^\dagger (\pi_L \otimes \pi_R)^{-1} \right) \cdot \text{Wg}_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_R}^{(p+q-2\ell)} \cdot (\tilde{\pi}_L \otimes \tilde{\pi}_R) \right] \tilde{I}_\ell. \quad (\text{A.19})$$

Here, we apply the formula in Lemma 5 for the mixed Haar twirl for each ℓ . The only partially transposed permutations that contribute correspond to tensor products $\sigma \equiv \pi_L \otimes \pi_R$ and $\tau \equiv \tilde{\pi}_L \otimes \tilde{\pi}_R$. Every partially transposed permutation besides these contains at least one EPR projector and hence vanishes inside $\tilde{I}_\ell^\dagger(\cdot)\tilde{I}_\ell$. The trace is partial over $[\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)}]_{\text{nE}}$ and does not act on $\mathcal{A}_\ell$. We refer to Appendix F for full details.

This completes our exact reformulation of the mixed Haar twirl. To provide a more intuitive picture of its behavior, we will now derive our simpler approximate expression. Before doing so, let us first recall the approximate formula for the standard Haar twirl from Ref. [36]:

Lemma 1 of Ref. [36] (Approximation for Haar twirl). *For any $k^2 \leq D$, the Haar twirl is approximated by,*

$$\Phi_a^{(k)}(X) \equiv \frac{1}{2^{nk}} \sum_\pi \text{tr}(X \pi^{-1}) \cdot \pi, \quad (\text{A.20})$$

up to relative error, $(1 - \varepsilon)\Phi_a^{(k)} \preceq \Phi_H^{(k)} \preceq (1 + \varepsilon)\Phi_a^{(k)}$, for $\varepsilon = k^2/2D/(1 - k^2/2D)$.

The approximate formula is accurate up to exponentially small error and enables much easier applications due to its simplicity. In effect, it replaces the Weingarten matrix $\text{Wg}_{\pi, \tilde{\pi}}$ in the exact Haar twirl with the identity matrix $(1/2^{nk})\delta_{\pi, \tilde{\pi}}$.

We can now provide a similar simplification for the mixed Haar twirl.

Lemma 8 (Approximation for the mixed Haar twirl). *For any $k^2 \leq D$, the mixed Haar twirl is approximated by,*

$$\Phi_H^{(p,q)}(X) = \sum_\ell \tilde{I}_\ell^\dagger \left[\frac{1}{2^{n(p+q-2\ell)}} \sum_{\pi_L \pi_R} \text{tr} \left(\tilde{I}_\ell X \tilde{I}_\ell^\dagger (\pi_L \otimes \pi_R)^{-1} \right) \cdot (\pi_L \otimes \pi_R) \right] \tilde{I}_\ell. \quad (\text{A.21})$$

up to relative error, $(1 - \varepsilon)\Phi_a^{(p,q)} \preceq \Phi_H^{(p,q)} \preceq (1 + \varepsilon)\Phi_a^{(p,q)}$, for $\varepsilon = (p+q)^2/D$. The approximate mixed Haar twirl can be equivalently written as,

$$\Phi_a^{(p,q)} = \sum_\ell \left(\mathcal{I}_\ell^\dagger \circ [\Phi_a^{(p-\ell)} \otimes \Phi_a^{(q-\ell)} \otimes \mathbb{1}_{\mathcal{A}_\ell}] \circ \mathcal{I}_\ell \right) \quad (\text{A.22})$$

where $\Phi_a^{(p-\ell)}$ and $\Phi_a^{(q-\ell)}$ are the approximate standard Haar twirls [Eq. (A.20)] and $\mathcal{I}_\ell(\cdot) \equiv \tilde{I}_\ell(\cdot)\tilde{I}_\ell^\dagger$ denotes conjugation by the partial isometry.

Similar to the standard Haar twirl, our approximation in effect replaces the Weingarten matrix in Eq. (A.19) by the product of identity matrices, $(1/D^{p-\ell})\delta_{\pi_L, \tilde{\pi}_L}$ and $(1/D^{q-\ell})\delta_{\pi_R, \tilde{\pi}_R}$. We provide a proof of the lemma in Appendix A.2.3,

In addition to its technical convenience, the approximate mixed Haar twirl provides an intuitive picture for the behavior of random unitaries in experiments involving time-reversal. Consider a quantum experiment querying U and $U^\dagger$ (or U^* or U^T) many times. First, within the experiment, some subset of the applications of U might cancel with applications of $U^\dagger$ (or U^* , etc.). The number of cancellations corresponds to the ℓ in our earlier discussion, and the pairing of the cancellations corresponds to the register $\mathcal{A}_\ell$. In principle, a quantum experiment could be a superposition of many different pairings, hence $\mathcal{A}_\ell$ is a quantum register. Then, among the un-cancelled applications, U and $U^\dagger$ behave indistinguishably from two *independent* random unitaries U and V . This is the statement of Lemma 8: After pulling U and U^* inside the partial isometry, their twirl is equal to the tensor product of two standard Haar twirls $\Phi_a^{(p-\ell)}$ and $\Phi_a^{(q-\ell)}$ up to small relative error. So the behavior of time-reversal experiments is in some sense very simple: U and $U^\dagger$ either cancel or they act completely independently. The function of the original Weingarten matrix elements and the ensuing partial isometries is solely to keep track of all the different ways that U and $U^\dagger$ might cancel.

A.2.2 Bounding the relative error of strong unitary designs

We now provide a handful of useful techniques for bounding the relative error of strong unitary designs. Our strategy is as follows. We first establish a technical lemma (Lemma 9) that allows one to bound the relative error between any mixed unitary ensemble and the approximate mixed Haar twirl. We then use this lemma to bound the relative error between the exact mixed Haar twirl and the approximate mixed Haar twirl, which proves Lemma 8. We then combine Lemma 8 with Lemma 9 to prove Lemma 7, which allows one to translate additive to relative errors for strong unitary designs.

Our first technical lemma is as follows. It is inspired by Lemma 7 of Ref. [36] for the standard approximate Haar twirl.

Lemma 9 (Relative error to the approximate mixed Haar twirl). *Consider a unitary ensemble $\mathcal{E}$ and its mixed twirl $\Phi_{\mathcal{E}}^{(p,q)}$. The mixed twirl is approximated by $\Phi_a^{(p,q)}$ up to relative error,*

$$\varepsilon = \frac{4^{n(p+q)}}{p!q!} \left\| [\delta\Phi \otimes \mathbb{1}] ([\Pi^{nE} \otimes \mathbb{1}] P_{EPR} [\Pi^{nE} \otimes \mathbb{1}]) \right\|_\infty, \quad (\text{A.23})$$

where $\delta\Phi \equiv \Phi_{\mathcal{E}}^{(p,q)} - \Phi_a^{(p,q)}$ and P_{EPR} is the projector onto the EPR state on $(\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q})^{\otimes 2}$.

Further, let $\Pi^{nE} \equiv \tilde{I}_{\ell=0}^\dagger \tilde{I}_{\ell=0}$ project to the subspace of $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ that is orthogonal to all EPR projectors between a copy on the left side and a copy on the right side. On the no-EPR subspace Π^{nE} , the mixed twirl is approximated by $\Phi_a^{(p)} \otimes \Phi_a^{(q)}$ up to relative error,

$$\varepsilon = \frac{4^{n(p+q)}}{p!q!} \left\| [\delta\tilde{\Phi} \otimes \mathbb{1}] (\tilde{P}_{EPR}) \right\|_\infty, \quad (\text{A.24})$$

where $\delta\tilde{\Phi}(\cdot) \equiv \Phi_{\mathcal{E}}^{(p,q)}(\Pi^{nE}(\cdot)\Pi^{nE}) - \Phi_a^{(p,q)}(\Pi^{nE}(\cdot)\Pi^{nE})$ is the difference between channels restricted to the no-EPR subspace, and $\tilde{P}_{EPR} \equiv [\Pi^{nE} \otimes \mathbb{1}] P_{EPR} [\Pi^{nE} \otimes \mathbb{1}]$ is the EPR state on the no-EPR subspace.

We prove Lemma 9 below, and apply it to prove Lemma 5 and Lemma 7 in the following sections.

Proof. We will prove a slightly more general version of the lemma that encapsulates both Eq. (A.23) and Eq. (A.24). Consider any projectors Π_1 and Π_2 such that $\Pi_1 \otimes \Pi_2$ commutes with $[\Phi_a^{(p,q)} \otimes \mathbb{1}](P_{\text{EPR}})$. We will set $\Pi_1 = \Pi_2 = \mathbb{1}$ for Eq. (A.23), and $\Pi_1 = \Pi^{\text{nE}}$ and $\Pi_2 = \mathbb{1}$ for Eq. (A.24).

We follow a similar general strategy to the proof of Lemma 2 in Ref. [36]. Let

$$\rho \equiv [(\Pi_1 \circ \Phi_{\mathcal{E}}^{(p,q)} \circ \Pi_2) \otimes \mathbb{1}](P_{\text{EPR}}) = [\Pi_1 \otimes \Pi_2] \cdot [\Phi_{\mathcal{E}}^{(p,q)} \otimes \mathbb{1}](P_{\text{EPR}}) \cdot [\Pi_1 \otimes \Pi_2], \quad (\text{A.25})$$

where we define the channel $\Pi_\alpha(X) \equiv \Pi_\alpha X \Pi_\alpha$ whose action will be clear from context. Let ρ_a denote the same expression with Φ replaced by $\Phi_a^{(p,q)}$. Note that $\Phi_a^{(p,q)}(\Pi^{\text{nE}}(\cdot)\Pi^{\text{nE}}) = [\Phi_a^{(p)} \otimes \Phi_a^{(q)}](\Pi^{\text{nE}}(\cdot)\Pi^{\text{nE}})$ for the proof of Eq. (A.24). We have

$$\begin{aligned} \rho_a &\equiv [(\Pi_1 \circ \Phi \circ \Pi_2) \otimes \mathbb{1}](P_{\text{EPR}}) \\ &= [\Pi_1 \otimes \Pi_2] \cdot \sum_{\ell} \frac{D_{\ell}}{D} \left([\tilde{I}_{\ell}^{\dagger} \otimes \tilde{I}_{\ell}^{\dagger}] \cdot [(\Phi_a^{(p-\ell)} \otimes \Phi_a^{(q-\ell)}) \otimes \mathbb{1}](P_{\text{EPR}}^{\ell}) \cdot [\tilde{I}_{\ell} \otimes \tilde{I}_{\ell}] \right) \cdot [\Pi_1 \otimes \Pi_2] \\ &= [\Pi_1 \otimes \Pi_2] \cdot \sum_{\ell} \frac{D_{\ell}}{D^{2p+2q-2\ell}} \left([\tilde{I}_{\ell}^{\dagger} \otimes \tilde{I}_{\ell}^{\dagger}] \cdot \sum_{\pi} [\pi \otimes \pi] \cdot [\tilde{I}_{\ell} \otimes \tilde{I}_{\ell}] \right) \cdot [\Pi_1 \otimes \Pi_2] \\ &= \sum_{\ell} \frac{D_{\ell}(p-\ell)!(q-\ell)!}{D^{3p+3q-4\ell}} \left([\Pi_1 \otimes \Pi_2] \cdot [\tilde{I}_{\ell}^{\dagger} \otimes \tilde{I}_{\ell}^{\dagger}] \cdot \frac{1}{(p-\ell)!(q-\ell)!} \sum_{\pi} [\pi \otimes \pi] \cdot [\tilde{I}_{\ell} \otimes \tilde{I}_{\ell}] \cdot [\Pi_1 \otimes \Pi_2] \right) \end{aligned} \quad (\text{A.26})$$

where $D_{\ell} \equiv \text{tr}(\tilde{I}_{\ell}^{\dagger} \tilde{I}_{\ell}) \leq D^{p+q-2\ell} \binom{p}{\ell} \binom{q}{\ell} \ell!$ is the rank of the ℓ -EPR subspace, $D = 2^n$, and we abbreviate $\pi \equiv \pi_L \otimes \pi_R$, where $\pi_L \in S_{p-\ell}$ and $\pi_R \in S_{q-\ell}$. We use that the partial isometries $\tilde{I}_{\ell}$ are real (Appendix F), so that $[\tilde{I}_{\ell} \otimes \mathbb{1}]P_{\text{EPR}} = [\mathbb{1} \otimes \tilde{I}_{\ell}^{\dagger}]P_{\text{EPR}}$. We proceed in four steps.

(1) The term in parentheses in the final line of Eq. (A.26) is a projector, i.e. it squares to itself. This follows because the sum over permutations inside the partial isometry is a projector (onto the tensor product of the symmetric subspace [95] of the left and right copy), $\Pi_1 \otimes \Pi_2$ is a projector (by definition), and these two projectors commute with one another (by assumption). Hence, their product is also a projector. Thus, ρ_a is equal to a sum of projectors with coefficients,

$$\frac{D_{\ell}(p-\ell)!(q-\ell)!}{D^{3p+3q-4\ell}} \leq \frac{1}{\ell!} \frac{p!q!}{D^{2p+2q-2\ell}}. \quad (\text{A.27})$$

applying our upper bound on D_{ℓ} . The minimum non-zero eigenvalue of ρ_a is given by the $\ell = 0$ coefficient, and is equal to $p!q!/D^{2(p+q)}$.

(2) The state ρ has support entirely within the support of ρ_a . This follows because, first, the support of ρ_a is equal to the support of $\sum_{\ell} [\Pi_1 \otimes \Pi_2] Q_{\ell}$ (note that $[\Pi_1 \otimes \Pi_2] Q_{\ell} [\Pi_1 \otimes \Pi_2] = [\Pi_1 \otimes \Pi_2] Q_{\ell}$ since the two projectors commute), where Q_{ℓ} is defined as the term in between the two copies of $\Pi_1 \otimes \Pi_2$ in Eq. (A.26). Second, the latter operator stabilizes ρ ,

$$\sum_{\ell} [\Pi_1 \otimes \Pi_2] Q_{\ell} \cdot \rho = [\Pi_1 \otimes \Pi_2] \cdot \rho = \rho, \quad (\text{A.28})$$

where the first step follows because Q_{ℓ} commutes with $\Pi_1 \otimes \Pi_2$ and with $(U)^{\otimes p} \otimes (U^*)^{\otimes q}$ for any $U \sim \mathcal{E}$, and $\sum_{\ell} Q_{\ell} P_{\text{EPR}} = P_{\text{EPR}}$. The latter statement follows because $\pi \otimes \pi$ stabilizes the EPR state $[\tilde{I}_{\ell} \otimes \tilde{I}_{\ell}] P_{\text{EPR}} [\tilde{I}_{\ell}^{\dagger} \otimes \tilde{I}_{\ell}^{\dagger}]$ for any π . Hence, the sum over π can be eliminated and the remaining sum over ℓ yields $\sum_{\ell} [\tilde{I}_{\ell}^{\dagger} \tilde{I}_{\ell} \otimes \tilde{I}_{\ell}^{\dagger} \tilde{I}_{\ell}] P_{\text{EPR}} = \sum_{\ell} [\tilde{I}_{\ell}^{\dagger} \tilde{I}_{\ell} \tilde{I}_{\ell}^{\dagger} \tilde{I}_{\ell} \otimes \mathbb{1}] P_{\text{EPR}} = \sum_{\ell} [\tilde{I}_{\ell}^{\dagger} \tilde{I}_{\ell} \otimes \mathbb{1}] P_{\text{EPR}} = P_{\text{EPR}}$.

(3) Steps (1) and (2) immediately imply that the twirl has relative error ε [Eq. (A.23) or Eq. (A.24)] on the EPR state.

(4) The relative error on the EPR state upper bounds the relative error on any state. This follows because we can express $\Phi(\chi) = D^{2(p+q)} \text{tr}_2((\mathbb{1} \otimes \chi^T)[\Phi \otimes \mathbb{1}](P_{\text{EPR}}))$ for any Φ , where the trace is over the second copy of $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$.

This completes the proof. $\square$

A.2.3 Proof of Lemma 8: The approximate mixed Haar twirl

From Eq. (A.19), we have the following expression for the mixed Haar twirl,

$$\Phi_H^{(p,q)}(\rho) = \sum_{\ell} \tilde{I}_{\ell}^{\dagger} \left[\sum_{\pi_L, \pi_R} \sum_{\tilde{\pi}_L, \tilde{\pi}_R} \text{tr} \left(\tilde{I}_{\ell} \rho \tilde{I}_{\ell}^{\dagger} (\pi_L \otimes \pi_R)^{-1} \right) \cdot \text{Wg}_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_L}^{(p+q-2\ell)} \cdot (\tilde{\pi}_L \otimes \tilde{\pi}_R) \right] \tilde{I}_{\ell}, \quad (\text{A.29})$$

We can compare this with our desired approximation,

$$\Phi_a^{(p,q)}(\rho) = \sum_{\ell} \tilde{I}_{\ell}^{\dagger} \left[\frac{1}{2^{n(p+q-2\ell)}} \sum_{\pi_L \otimes \pi_R} \text{tr} \left(\tilde{I}_{\ell} \rho \tilde{I}_{\ell}^{\dagger} (\pi_L \otimes \pi_R)^{-1} \right) \cdot (\pi_L \otimes \pi_R) \right] \tilde{I}_{\ell}. \quad (\text{A.30})$$

Since both the mixed Haar twirl and our desired approximation are a tensor sum over ℓ , the two are close in relative error if and only if they are close in relative error within each partial isometry $\tilde{I}_{\ell}$. Within each partial isometry, the channels act solely on the no-EPR subspace of $\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)}$ by definition. Hence, to prove the proposition, it suffices to show that $\Phi_a^{(p-\ell)} \otimes \Phi_a^{(q-\ell)}$ and $\Phi_H^{(p-\ell, q-\ell)}$ are close in relative error on the no-EPR subspace.

Observing Lemma 9, we can bound this relative error in terms of the spectral norm

$$\begin{aligned} & \|[\delta\Phi \otimes \mathbb{1}]((\Pi^{\text{nE}} \otimes \mathbb{1})P_{\text{EPR}}(\Pi^{\text{nE}} \otimes \mathbb{1}))\| \\ &= \frac{1}{4^{n(p+q-2\ell)}} \sum_{\pi_L, \pi_R} \sum_{\tilde{\pi}_L, \tilde{\pi}_R} \left(2^{n(p+q-2\ell)} \text{Wg}_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_L}^{(p+q-2\ell)} - \delta_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_L} \right) \cdot (\pi_L \otimes \pi_R) \otimes (\tilde{\pi}_L \otimes \tilde{\pi}_R). \end{aligned} \quad (\text{A.31})$$

Applying the triangle inequality, we find

$$\begin{aligned} & 4^{n(p+q-2\ell)} \|[\delta\Phi^{(p-\ell, q-\ell)} \otimes \mathbb{1}]((\Pi^{\text{nE}} \otimes \mathbb{1})P_{\text{EPR}}(\Pi^{\text{nE}} \otimes \mathbb{1}))\|_{\infty} \\ & \leq \sum_{\pi_L, \pi_R} \sum_{\tilde{\pi}_L, \tilde{\pi}_R} \left| 2^{n(p+q-2\ell)} \text{Wg}_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_L}^{(p+q-2\ell)} - \delta_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_L} \right| \\ & \equiv \sum_{\pi_L, \pi_R} \sum_{\tilde{\pi}_L, \tilde{\pi}_R} A_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_L}, \end{aligned} \quad (\text{A.32})$$

where we define the $(p-\ell)!(q-\ell)! \times (p-\ell)!(q-\ell)!$ matrix $\hat{A}$ elementwise via the absolute values in the preceding expression.

Since $\hat{A}$ has all positive entries, its maximal eigenvalue is achieved by a vector with all positive entries. Moreover, it is invariant under multiplication by any permutation, $\pi_L \otimes \pi_R \rightarrow (\pi_L \otimes \pi_R)(\tilde{\pi}_L \otimes \tilde{\pi}_R)$, $\tilde{\pi}_L \otimes \tilde{\pi}_R \rightarrow (\tilde{\pi}_L \otimes \tilde{\pi}_R)(\tilde{\pi}_L \otimes \tilde{\pi}_R)$. Thus, without loss of generality, we can take its maximal eigenvector to be both positive and permutation invariant. This implies that the maximal eigenvalue is achieved by the constant vector. The sum in Eq. (A.32) is thus equal to the maximal eigenvalue multiplied by the matrix dimension, $(p-\ell)!(q-\ell)!$.

To determine the maximum eigenvalue of $\hat{A}$, we note that $\hat{A}$ is a sub-matrix of the $(p+q-2\ell)! \times (p+q-2\ell)!$ matrix with entries, $|\delta W|_{\sigma,\tau} \equiv |2^{(p+q-2\ell)} \text{Wg}_{\sigma,\tau} - \delta_{\sigma,\tau}|$, where $\sigma, \tau \in S_{p+q-2\ell}$. The spectral norm of a sub-matrix is upper bounded by the spectral norm of the matrix, and hence $\|\hat{A}\|_\infty \leq \|\delta \hat{W}\|_\infty$. From Ref. [96], the latter spectral norm is upper bounded by $(p+q-2\ell)^2/2^n \leq (p+q)^2/2^n$. Applying Lemma 9 completes our proof. $\square$

A.2.4 Proof of Lemma 7: Translating between different strong approximation errors

As aforementioned, the first statement of the lemma follows trivially from definitions. The combination of Lemma 8 and Lemma 9 immediately proves the second statement. We have $\|[(\Phi_{\mathcal{E}}^{(p,q)} - \Phi_H^{(p,q)}) \otimes \mathbb{1}](P_{\text{EPR}})\|_\infty \leq \varepsilon_a$ from the definition of the additive error. We also have $\frac{4^{n(p+q)}}{p!q!} \|[(\Phi_H^{(p,q)} - \Phi_a^{(p)} \otimes \Phi_a^{(q)}) \otimes \mathbb{1}](P_{\text{EPR}})\|_\infty \leq (p+q)^2/2^n$ from Lemma 8. Together, these imply that $\frac{4^{n(p+q)}}{p!q!} \|[(\Phi_{\mathcal{E}}^{(p,q)} - \Phi_a^{(p)} \otimes \Phi_a^{(q)}) \otimes \mathbb{1}](P_{\text{EPR}})\|_\infty \leq \frac{4^{n(p+q)}}{p!q!} \varepsilon_a + (p+q)^2/2^n \equiv \varepsilon'$. From Lemma 8 and Lemma 9, this proves that

$$\Phi_{\mathcal{E}}^{(p,q)} \preceq (1 + \varepsilon') \Phi_a^{(p,q)} \preceq \frac{1 + \varepsilon'}{1 - \frac{(p+q)^2}{2^n}} \Phi_H^{(p,q)} \preceq \left(1 + \left(\frac{4^{n(p+q)}}{p!q!}\right) \varepsilon_a + \frac{(p+q)^2}{2^n}\right) \left(1 + \frac{2(p+q)^2}{2^n}\right) \Phi_H^{(p,q)},$$

and similar in the reverse direction. Here, we assumed $2(p+q)^2 \leq 2^n$ in the third inequality. This completes the proof. $\square$

A.3 Proof of Lemma 2: Strong unitary 2-designs from blocked fast scrambling random circuits

In this section, we prove Lemma 2 showing that the blocked fast scrambling circuit is a strong unitary 2-design. The circuit has depth $\mathcal{O}(\log n \cdot \log n/\varepsilon)$ when each small random unitary is instantiated with a 1D random circuit of depth $\mathcal{O}(\log n/\varepsilon)$. This forms a key building block in our random circuit construction of strong unitary k -designs, as described in the main text.

Our proof of Lemma 2 proceeds in two steps. First, we introduce and prove a simple proposition that quantifies when any unitary ensemble forms a strong approximate unitary 2-design. Our proposition leverages a well-known mapping from 2-designs to classical Markov processes on the set of Pauli operators [55, 97]. We show that the measurable error of a strong approximate 2-design is upper bounded by the total variational distance between the Markov process associated to the circuit ensemble, and that associated to the Haar ensemble. Second, we prove that this total variational distance is small for the blocked fast scrambling circuit, which completes the proof.

Let us first review the mapping from unitary 2-designs to Markov processes, and formally state our proposition. Consider the action of the unitary $U \otimes U^*$ on $\mathcal{H} \otimes \mathcal{H}$, where U is drawn from any ensemble $\mathcal{E}$ that is invariant under random single-qubit rotations at the input and output. To understand the action of the unitary, we consider the complete basis of states,

$$|P\rangle \equiv (P \otimes \mathbb{1}) |\Psi_{\text{EPR}}\rangle, \quad (\text{A.33})$$

where $|\Psi_{\text{EPR}}\rangle$ is the EPR state and P runs over all 4^n Pauli operators. The invariance of $\mathcal{E}$ under random single-qubit rotations guarantees that the twirl over $\mathcal{E}$ can be written in the following form,

$$\mathbb{E}_{U \sim \mathcal{E}} \left[(U \otimes U^*) \rho (U^\dagger \otimes U^T) \right] = \langle \mathbb{1} | \rho | \mathbb{1} \rangle \cdot |\mathbb{1}\rangle\langle\mathbb{1}| + \sum_{P, Q \neq \mathbb{1}} p_{\mathcal{E}}(Q; P) \langle P | \rho | P \rangle \cdot |Q\rangle\langle Q|, \quad (\text{A.34})$$

where $p_{\mathcal{E}}(Q; P)$ is a normalized probability distribution over Pauli operators Q , for each Pauli operator P . For a Haar-random unitary, we have $p_H(Q; P) = 1/(4^n - 1)$.

Our proposition is as follows.

Proposition 2. Consider any unitary ensemble $\mathcal{E}$ is invariant under conjugation, transposition, and random single-qubit Pauli rotations at the input and output circuit layer. The ensemble forms a strong approximate unitary 2-design with measurable error,

$$\varepsilon = \max_P \text{TVD}(p_{\mathcal{E}}(Q; P), p_H(Q; P)), \quad (\text{A.35})$$

in any quantum experiment that queries one of U or U^T and one of U^* or $U^\dagger$.

The proposition does not cover experiments that query two of U or U^T and neither of U^* or $U^\dagger$ (and vice versa). We will address such experiments using standard unitary design features later on.

Proof of Proposition 2. Without loss of generality, we consider an experiment that first queries $U^\dagger$ and then queries U . The remaining seven classes of experiments follow by symmetric arguments⁸. The output state ρ of any such experiment can be written as (Fig. 5)

$$\rho_U = 4^n (\mathbb{1}_{BA} \otimes \langle \Psi_{\text{Bell}} |_{XY}) (\mathbb{1}_B \otimes U_A \otimes U_X^* \otimes \mathbb{1}_Y) |\Psi\rangle\langle\Psi|_{BAXY} (\mathbb{1}_B \otimes U_A^\dagger \otimes U_X^T \otimes \mathbb{1}_Y) (\mathbb{1}_{BA} \otimes |\Psi_{\text{Bell}}\rangle_{XY}),$$

where $|\Psi\rangle$ is a normalized quantum state. Taking the twirl over $\mathcal{E}$ yields,

$$\begin{aligned} \mathbb{E}_{U \sim \mathcal{E}} [\rho_U] &= 4^n \langle \mathbb{1} |_{XY} | \mathbb{1} \rangle \langle \mathbb{1} |_{AX} | \Psi \rangle \langle \Psi |_{BAXY} | \mathbb{1} \rangle \langle \mathbb{1} |_{AX} | \mathbb{1} \rangle_{XY} \\ &\quad + 4^n \sum_{P, Q \neq \mathbb{1}} p_{\mathcal{E}}(Q; P) \cdot \langle \mathbb{1} |_{XY} | Q \rangle \langle P |_{AX} | \Psi \rangle \langle \Psi |_{BAXY} | P \rangle \langle Q |_{AX} | \mathbb{1} \rangle_{XY} \\ &= S_{Y \rightarrow A} (\mathbb{1}_{A'} \otimes \langle \mathbb{1} |_{AX} \otimes \mathbb{1}_Y) |\Psi\rangle\langle\Psi|_{BAXY} (\mathbb{1}_{A'} \otimes | \mathbb{1} \rangle_{AX} \otimes \mathbb{1}_Y) S_{Y \rightarrow A}^\dagger \\ &\quad + \sum_{P, Q \neq \mathbb{1}} p_{\mathcal{E}}(Q; P) \cdot S_{Y \rightarrow A} (\mathbb{1}_{A'} \otimes \langle P |_{AX} \otimes Q_Y) |\Psi\rangle\langle\Psi|_{BAXY} (\mathbb{1}_{A'} \otimes | P \rangle_{AX} \otimes Q_Y) S_{Y \rightarrow A}^\dagger \end{aligned}$$

where $S_{Y \rightarrow A}$ swaps register Y to register A , and is obtained from the multiplying the Bell pairs, $\langle \mathbb{1} |_{XY} | Q \rangle_{AX} = (1/2^n) S_{Y \rightarrow A} Q_Y$.

Let us denote each state in the final line above as ρ_{PQ} which acts on AB . With this notation, the final line becomes

$$\mathbb{E}_{U \sim \mathcal{E}} [\rho_U] = \rho_{\mathbb{1}\mathbb{1}} + \sum_{P, Q \neq \mathbb{1}} p_{\mathcal{E}}(Q; P) \cdot \rho_{PQ}. \quad (\text{A.36})$$

We also let $\delta p(P, Q) = p_{\mathcal{E}}(P, Q) - p_H(P, Q)$. We can bound the additive error as follows,

$$\begin{aligned} \left\| \mathbb{E}_{U \sim \mathcal{E}} [\rho_U] - \mathbb{E}_{U \sim H} [\rho_U] \right\|_1 &= \left\| \sum_{P, Q \neq \mathbb{1}} \delta p(Q; P) \cdot \rho_{PQ} \right\|_1 \\ &\leq \sum_{P, Q \neq \mathbb{1}} |\delta p(Q; P)| \cdot \|\rho_{PQ}\|_1 \\ &\leq \sum_{P \neq \mathbb{1}} \|\rho_{P\mathbb{1}}\|_1 \cdot \sum_{Q \neq \mathbb{1}} |\delta p(Q; P)| \\ &= \sum_{P \neq \mathbb{1}} \|\rho_{P\mathbb{1}}\|_1 \cdot \text{TVD}(p_{\mathcal{E}}(Q; P), p_H(Q; P)) \\ &\leq \max_P \text{TVD}(p_{\mathcal{E}}(Q; P), p_H(Q; P)) \cdot \sum_{P \neq \mathbb{1}} \|\rho_{P\mathbb{1}}\|_1 \\ &\leq \max_P \text{TVD}(p_{\mathcal{E}}(Q; P), p_H(Q; P)). \end{aligned} \quad (\text{A.37})$$

⁸In particular, experiments that query U^* and then U follow the exact same proof exchanging X and Y . The remaining six classes of experiments follow from these two by exchanging replacements $U \leftrightarrow U^T$ or $U \leftrightarrow U^*$ or $U \leftrightarrow U^\dagger$. These replacements are allowed because the ensemble $\mathcal{E}$ is invariant under conjugation and transposition.

The first step uses the triangle inequality, the second step uses $\|\rho_{PQ}\|_1 = \|\rho_{P\mathbb{1}}\|_1$ since the 1-norm is invariant under Pauli rotations, the third step uses the definition of the total variational distance, the fourth step uses Holder's inequality, and the final step uses $\sum_{P \neq \mathbb{1}} \|\rho_{P\mathbb{1}}\|_1 \leq \sum_P \|\rho_{P\mathbb{1}}\|_1 = \sum_P \text{tr}(\rho_{P\mathbb{1}}) = \text{tr}(|\Psi\rangle\langle\Psi|) = 1$. This completes the proof. $\square$

We can now proceed to the proof of Lemma 2.

Proof of Lemma 2. There are sixteen classes of experiments that a strong unitary 2-design must capture, corresponding to whether the first query is to U , U^T , U^* , or $U^\dagger$ and similar for the second query. Let us first consider the eight classes of experiment that query two of U, U^T or two of $U^*, U^\dagger$. From the gluing Lemma 3 of Ref. [36], the blocked fast scrambling circuit with small Haar-random unitaries forms a standard approximate unitary 2-design with relative error $4m/2^\xi$. This implies that the ensemble has measurable error at most $8m/2^\xi$ in any of the eight experiments. Replacing each small random unitary with a relative error $\frac{\varepsilon}{n}$ -approximate unitary 2-design yields an additional measurable error $2m\varepsilon/n = 2\varepsilon/\xi$. Here, we only need to glue $2m$ unitaries together in order to realize a standard design via Lemma 3 of Ref. [36]; hence, we only pick up an additional error linear in m , instead of $m \log_2 m$. Thus, the blocked fast scrambling circuit has measurable error at most $8m/2^\xi + m\varepsilon/n$ in any of these eight experiments. Setting $\xi \geq \min(\log_2(3n/\varepsilon), 4)$ yields an error less than ε .

Let us now turn to the remaining eight experiments, which query one of U, U^T and one of $U^*, U^\dagger$. We will leverage Proposition 2 to bound the measurable error. To begin, we consider the blocked fast scrambling circuit in which each small unitary is Haar-random. Let P be any Pauli operator. When a Pauli operator is acted on by a small random unitary within its support, the resulting Pauli operator has support on both patches of the small random unitary with probability $1 - (2 \cdot 4^\xi - 1)/(4^{2\xi} - 1) \geq 1 - 2/4^\xi$, where the latter term counts the fraction of non-identity Pauli operators on 2ξ qubits that have support on only a single patch. Consider any single patch in the support of P , and all the small random unitaries within the light-cone of the patch. There are at most $1 + 2 + 4 + \dots + m = 2m - 1$ such unitaries. Therefore, the probability that *every* small random unitary in the light-cone spreads the Pauli operator to both patches in its support is at least $1 - (2m - 1)(2/4^\xi)$. The probability that the time-evolved operator $UPU^\dagger$ has support on every patch of ξ qubits is hence at least this value. We denote this probability as $1 - \delta_\mathcal{E}$, with $\delta_\mathcal{E} \leq 4m/4^\xi$.

Let us now turn to the action of an n -qubit Haar-random unitary. Under an n -qubit Haar-random unitary, the time-evolved operator $UPU^\dagger$ is drawn from the flat distribution on the set of $4^n - 1$ non-identity Pauli operators. Therefore, it has support on every patch of ξ qubits with probability $1 - \delta_H = (4^\xi - 1)^m / (4^n - 1) \geq (4^n - m4^{n-\xi}) / (4^n - 1) \geq 1 - m/4^\xi$.

The probability distributions $p_\mathcal{E}(P, Q)$ and $p_H(P, Q)$ are both flat among the Pauli operators Q that have support on every patch of ξ qubits, since both $\mathcal{E}$ and H are invariant under composition with small random unitaries on each patch. The TVD between the two distributions picks up contributions from two sources. The Q with full support contribute a factor of $|\delta_H - \delta_\mathcal{E}| \leq \delta_H + \delta_\mathcal{E}$, proportional to the difference in the flat value of $p_\mathcal{E}(P, Q)$ and $p_H(P, Q)$ on such Q . Meanwhile, the other Q contribute at most a factor of $\delta_H + \delta_\mathcal{E}$, since the two distributions have at most this support on such operators. Thus, the TVD between the two distributions is less than,

$$\text{TVD}(p_\mathcal{E}(Q; P), p_H(Q; P)) \leq 2(\delta_H + \delta_\mathcal{E}) \leq 2(4m/4^\xi + m/4^\xi), \quad (\text{A.38})$$

for any P . Applying Proposition 2 upper bounds the measurable error of the blocked fast scrambling circuit with small Haar-random unitaries. Replacing each small Haar-random unitary in the light-cone with an $\frac{\varepsilon}{n}$ -approximate strong unitary 2-design yields a measurable error less than

$$8m/4^\xi + 2m/4^\xi + \left(\frac{2m}{n}\right)\varepsilon. \quad (\text{A.39})$$

Setting $\xi \geq \min(\frac{1}{2} \log_2(5n/\varepsilon), 4)$ yields an error less than

$$(8/5)(m/n)\varepsilon + (2/5)(m/n)\varepsilon + 2(m/n)\varepsilon \leq \varepsilon, \quad (\text{A.40})$$

which completes our proof. $\square$

A.4 Proof of Lemma 3: Strong unitary k -designs from 1D random circuits

In this section, we provide our proof that one-dimensional local random circuits form strong unitary k -designs with small relative error in linear depth (Theorem 3 of the main text). Our proof follows the same approach used to show that 1D random circuits form standard unitary designs [32]. This is enabled by our new Lemma 7 which allows one to translate from spectral gaps [32, 34, 72] to relative error strong unitary designs.

Let us first review a few of the key definitions used in the spectral gap literature [32, 34, 98]. The central object studied in these works is the so-called moment operator,

$$M_{\mathcal{E}} = \mathbb{E}_{U \sim \mathcal{E}} [U^{\otimes k} \otimes (U^*)^{\otimes k}], \quad (\text{A.41})$$

of a random unitary ensemble $\mathcal{E}$. To quantify the closeness of the moment operator to the Haar-random moment operator, we let $\delta M = M_{\mathcal{E}} - M_H$ and define the *essential norm*,

$$g(\mathcal{E}) = \|\delta M\|_{\infty}. \quad (\text{A.42})$$

Ref. [34] proves that the ensemble of 1D local random brickwork circuits of depth d has essential norm $g(\mathcal{E}) \leq \exp(-\Omega(d \log^7 k))$.

The relationship between the essential norm and the approximation errors of standard unitary designs is well-known. One can bound $\|\delta\Phi(\rho)\|_{\infty} \leq g(\mathcal{E})$ for any ρ when $\delta\Phi = \Phi_{\mathcal{E}}^{(k)} - \Phi_H^{(k)}$ is defined with respect to the standard twirl [32]. This allows one to bound the relative error via Lemma 6. In what follows, we show that this approach proceeds identically for strong unitary designs after replacing Lemma 6 with our Lemma 7.

Proof of Lemma 3. Let $\delta\Phi = \Phi_{\mathcal{E}}^{(p,q)} - \Phi_H^{(p,q)}$ and $p + q = k$. The relationship between the essential norm and the spectral norm when $\delta\Phi$ is applied to a state follows from a straightforward series of equalities,

$$\|\delta\Phi(\rho)\|_{\infty} \leq \|\delta\Phi(\rho)\|_2 = \sqrt{\text{tr}(\delta\Phi(\rho)^2)} = \sqrt{\langle \rho | \delta M^2 | \rho \rangle} \leq \|\delta M\|_{\infty} \sqrt{\langle \rho | \rho \rangle} = \|\delta M\|_{\infty} = g(\mathcal{E}), \quad (\text{A.43})$$

where $|\rho\rangle$ denotes the vectorization of ρ . Hence, an upper bound on the essential norm immediately translates to an identical upper bound on the spectral norm of $\delta\Phi(\rho)$ for any state ρ . The two inequalities are saturated when ρ is pure and equal to the extremal eigenvector of δM .

In previous works, the equalities above are applied when $\delta\Phi$ is defined with respect to the standard twirl [32]. In this case, the k copies of U in δM act on the left (“ket”) side of the vectorization of ρ , and the k copies of U^* act on the right (“bra”) side. However, an identical bound holds for the mixed twirl as well. In this case, we have p copies of U and q copies of U^* that act on the left side of the vectorization of ρ , and q copies of U and p copies of U^* that act on the right side. Since there k copies of both U and U^* in total, the remaining steps proceed identically regardless of the value of p, q .

From Ref. [34] and Eq. (A.43), we have $\|\delta\Phi(\rho)\|_{\infty} \leq \exp(-\Omega(\log(k)^7 d))$ for any state ρ . Taking $\rho = P_{\text{EPR}}$ as in Lemma 9, we find from Lemma 9 that $\mathcal{E}$ is a strong unitary design with relative error

$$\varepsilon \leq \left(1 + \frac{k^2}{2^n}\right) \cdot \frac{4^{nk}}{p!q!} \cdot \exp(-\Omega(\log(k)^7 d)) + \frac{k^2}{2^n}, \quad (\text{A.44})$$

where again, $k = p + q$. The factors of $k^2/2^n$ arise when converting from the approximate mixed Haar twirl (used in Lemma 9) to the exact Haar twirl (in the definition of $\delta\Phi$ above). For any $\varepsilon \geq 2k^2/2^n$, we can set $d = \Omega(\log(k)^7(nk + \log(1/\varepsilon)))$ to ensure that $\mathcal{E}$ is a strong unitary design with relative error ε , as claimed. $\square$

A.5 Proof of Theorem 1

The combination of Theorem 3, Theorem 5, Lemma 2, and Lemma 3 immediately yield Theorem 1 on the circuit depth of strong unitary designs. We refer to Ref. [39] for a detailed derivation of the circuit depths and resources required to implement the LRFC ensemble with k -wise independent functions.

Proof of Theorem 1. The first two statements of Theorem 1 follow immediately from Theorem 3 and Theorem 5 as described in the main text. The third statement of Theorem 1 follows immediately from Theorem 5 (and its extension to the blocked fast scrambling circuit via Lemma 2) and Lemma 3. $\square$

A.6 Lower bounds on the depth of strong unitary designs

In this section, we prove our two lower bounds on the circuit depths of strong unitary designs. As discussed in the main text, our first lower bound applies to any circuit ensemble and any notion of approximation error (additive, measurable, or relative). It shows that strong unitary designs require depth $\Omega(n)$ in 1D circuits and $\Omega(\log n)$ in all-to-all connected circuits. Our second lower bound is specific to local random circuits and the *relative error* metric. It shows that local random circuits require depth $\Omega(n)$ to form relative error strong unitary designs in *any* circuit geometry. This contrasts with the measurable error, where we achieved local random circuit designs in depth $\mathcal{O}(\log^2 n)$ in Theorem 1.

A.6.1 Lower bound for any random unitary ensemble

Our first lower bound is Proposition 1 in the main text. The proof follows from a simple light-cone argument.

Proof. We consider the state, $U^\dagger Z_0 U |0^n\rangle$, where Z_0 is a local Pauli operator on the first qubit. We then measure the state in the computational basis, and count the average fraction of bits that are 1. This corresponds to the expectation value of the operator, $M = \sum_{\mathbf{s} \in \{0,1\}^n} (|\mathbf{s}|/n) \cdot |\mathbf{s}\rangle\langle\mathbf{s}|$, where $|\mathbf{s}|$ is the Hamming weight of a bitstring $\mathbf{s}$. When U is Haar-random, the expected number of bits flipped is just above $1/2$,

$$\mathbb{E}_{U \sim H}[\langle 0^n | U^\dagger Z_0 U \cdot M \cdot U^\dagger Z_0 U | 0^n \rangle] \geq \frac{1}{2}. \quad (\text{A.45})$$

Therefore, any strong ε -approximate unitary 2-design must have expectation value at least $1/2 - \varepsilon$.

Let us now turn to circuits with bounded depth. The operator $U^\dagger Z_0 U$ can have support on at most L qubits, where L is the size of the light-cone of U . For 1D circuits, we have $L \leq 2d$ for any U , and for all-to-all circuits, we have $L \leq 2^d$. This implies that the fraction of bits flipped in any individual unitary U is at most L/n , which yields

$$\mathbb{E}_{U \sim \mathcal{E}}[\langle 0^n | U^\dagger Z_0 U \cdot M \cdot U^\dagger Z_0 U | 0^n \rangle] \leq \frac{L}{n}. \quad (\text{A.46})$$

Hence, we require $d \geq n(1/2 - \varepsilon)$ in 1D, and $d \geq \log_2(n(1/2 - \varepsilon))$ in all-to-all circuits. We set $\varepsilon = \mathcal{O}(1)$ to obtain our stated bounds. $\square$

A.6.2 Lower bound for local random circuit ensembles

Our second lower bound is specific to circuit ensembles composed of independent random gates.

Proposition 3. (Depth lower bound for strong unitary designs from local random circuits) *Any quantum circuit ensemble composed of independent local Haar-random gates requires circuit depth*

- $d = \Omega(\min\{\log(1/\varepsilon), n\})$, to form a strong ε -approximate unitary 2-design,
- $d = \Omega(n)$, to form a strong ε -approximate unitary 2-design with relative error.

Both of the statements above hold on any circuit geometry. To prove the first statement, we show that any local operator retains a small, exponentially-decaying memory of its initial value under any local random circuit. To prove the latter statement, we show that this value must be exponentially small in n , $\mathcal{O}(4^{-n})$, in a strong unitary 2-design with relative error.

Proof. We consider an experiment which prepares the first qubit in the zero state and all other qubits in the maximally mixed state, applies U , and measures the probability for the first qubit to remain to the zero state. This yields an expectation value,

$$\text{tr}\left(Z_0 U (|0\rangle\langle 0| \otimes (\mathbb{1}/2)^{\otimes n-1}) U^\dagger\right) = \frac{1}{2^n} \text{tr}\left(Z_0 U Z_0 U^\dagger\right). \quad (\text{A.47})$$

In the second equality, we expand, $|0\rangle\langle 0| = (\mathbb{1} + Z_0)/2$, and note that the identity term vanishes after the trace. The expectation value will be zero, on average, whenever U is drawn from a unitary 1-design. To this end, our quantity of interest is the square of the expectation value. When U is Haar-random, we have

$$\mathbb{E}_{U \sim H} \left[\frac{1}{4^n} \text{tr}\left(Z_0 U Z_0 U^\dagger\right)^2 \right] = \frac{1}{4^n - 1}, \quad (\text{A.48})$$

because the time-evolved operator $U Z_0 U^\dagger$ has equal probability to be any of $4^n - 1$ non-identity Pauli operators.

Let us now consider when U is drawn from a circuit of independent local Haar-random gates. For convenience, let us re-write the squared expectation value as

$$\frac{1}{4^n} \text{tr}\left(Z_0 U Z_0 U^\dagger\right)^2 = \langle Z_0 | (U \otimes U^*) | Z_0 \rangle \langle Z_0 | (U^\dagger \otimes U^T) | Z_0 \rangle, \quad (\text{A.49})$$

where $|Z_0\rangle \equiv (Z_0 \otimes \mathbb{1}) |E\rangle$, and $|E\rangle$ is the EPR state. To proceed, we decompose the d layers of the circuit as, $U = U_d U_{d-1} \dots U_1$, and denote the gate acting on the first qubit in each layer as G_d . We assume the gates act on at most $r = \mathcal{O}(1)$ qubits. After a single layer, U_1 , of the circuit, we have

$$\begin{aligned} \mathbb{E}_{U_1} [(U_1 \otimes U_1^*) |Z_0\rangle\langle Z_0| (U_1^\dagger \otimes U_1^T)] &= \mathbb{E}_{G_1} [(G_1 \otimes G_1^*) |Z_0\rangle\langle Z_0| (G_1^\dagger \otimes G_1^T)] \\ &= \frac{1}{4^r - 1} \sum_{P \in \text{supp}(G_1), P \neq \mathbb{1}} |P\rangle\langle P|, \end{aligned} \quad (\text{A.50})$$

where the sum is over all non-identity Pauli operators in the support of G_1 . To proceed, we note that the state above is strictly greater than the initial state divided by $4^r - 1$,

$$\mathbb{E}_{U_1} [(U_1 \otimes U_1^*) |Z_0\rangle\langle Z_0| (U_1^\dagger \otimes U_1^T)] = \frac{1}{4^r - 1} \sum_{P \in \text{supp}(G_1), P \neq \mathbb{1}} |P\rangle\langle P| \geq \frac{1}{4^r - 1} |Z_0\rangle\langle Z_0|. \quad (\text{A.51})$$

Intuitively, this is because the Pauli operator Z_0 has probability $1/(4^r - 1)$ to return to itself under the r -qubit random gate G_1 .

We can now iterate. After the second circuit layer, we have

$$\begin{aligned} \mathbb{E}_{U_2, U_1} [(U_2 U_1 \otimes U_2^* U_1^*) |Z_0\rangle\langle Z_0| (U_1^\dagger U_2^\dagger \otimes U_1^T U_2^T)] &\geq \mathbb{E}_{U_2} [(U_2 \otimes U_2^*) |Z_0\rangle\langle Z_0| (U_2^\dagger \otimes U_2^T)] \\ &\geq \left(\frac{1}{4^r - 1}\right)^2 |Z_0\rangle\langle Z_0|, \end{aligned} \quad (\text{A.52})$$

where in the first inequality we apply Eq. (A.51) for the unitary U_1 , and in the second inequality we apply Eq. (A.51) for the unitary U_2 . Proceeding through all d circuit layers of U , we find

$$\mathbb{E}_{U \sim \mathcal{E}} [(U \otimes U^*) |Z_0\rangle\langle Z_0| (U^\dagger \otimes U^T)] \geq \left(\frac{1}{4^r - 1}\right)^d |Z_0\rangle\langle Z_0|. \quad (\text{A.53})$$

This yields a lower bound on our quantity of interest,

$$\mathbb{E}_{U \sim \mathcal{E}} \left[\frac{1}{4^n} \text{tr} \left(Z_0 U Z_0 U^\dagger \right)^2 \right] = \mathbb{E}_{U \sim \mathcal{E}} [\langle Z_0 | (U \otimes U^*) |Z_0\rangle\langle Z_0| (U^\dagger \otimes U^T) |Z_0\rangle] \geq \left(\frac{1}{4^r - 1}\right)^d. \quad (\text{A.54})$$

Hence, for the ensemble $\mathcal{E}$ to form a strong ε -approximate unitary 2-design, we must have $1/(4^r - 1)^d \leq 1/(4^n - 1) + \varepsilon$. This requires either $d = \Omega(\log(1/\varepsilon))$ or $d = \Omega(n)$. For the ensemble $\mathcal{E}$ to form a strong ε -approximate unitary 2-design with relative error, we must have $1/(4^r - 1)^d \leq (1 + \varepsilon)/(4^n - 1)$. This requires $d = \Omega(n)$. This completes the proof. $\square$

B Strong pseudorandom unitaries

In this section, we introduce strong pseudorandom unitaries (PRUs) and extend the proof of [99] to allow queries to the conjugate and transpose. This yields strong PRUs on n qubits in poly n circuit depth. We show how to reduce the circuit depth to $\mathcal{O}(\log n)$ using our new constructions in later sections.

B.1 Definitions

To define pseudorandom unitaries (PRU), we first define oracle adversaries that can query an n -qubit unitary oracle $\mathcal{O}$ in multiple ways. The oracle adversary is the quantum algorithm that aims to attack the pseudorandom unitary construction by distinguishing it from Haar-random unitaries. We consider the strongest possible adversary with access to all four fundamental operations: U , $U^\dagger$, U^T , and U^* .

Definition 10 (Oracle adversaries). *A t -query oracle adversary $\mathcal{A}$ is parameterized by a sequence of $(n + m)$ -qubit unitaries $(W_1, \dots, W_{t+1})$ acting on registers $(\mathbf{A}, \mathbf{B})$, where $\mathbf{A}$ is the n -qubit query register and $\mathbf{B}$ is an m -qubit ancilla, and a sequence of oracle queries $U_1, \dots, U_t$ where each $U_i \in \{U, U^\dagger, U^T, U^*\}$. The state after t queries is*

$$|\mathcal{A}_t^U\rangle_{\mathbf{AB}} := W_{t+1}[U_t \otimes \mathbb{1}_m] \cdots W_2[U_1 \otimes \mathbb{1}_m] W_1 |0^{n+m}\rangle_{\mathbf{AB}}. \quad (\text{B.1})$$

Definition 11 (Pseudorandom unitaries). *We say $\{\mathcal{U}_n\}_{n \in \mathbb{N}}$ is a secure PRU if, for all $n \in \mathbb{N}$, $\mathcal{U}_n = \{U_k\}_{k \in \mathcal{K}_n}$ is a set of n -qubit unitaries where $\mathcal{K}_n$ denotes the keyspace, satisfying:*

- **Efficient computation:** *There exists a poly(n)-time quantum algorithm that implements the n -qubit unitary U_k for all $k \in \mathcal{K}_n$.*

- **Indistinguishability from Haar:** For any oracle adversary $\mathcal{A}$ that runs in time $\text{poly}(n)$ and measures a two-outcome observable $D_{\mathcal{A}}$ with eigenvalues $\{0, 1\}$ after the queries, we have

$$|\mathbb{E}_{\mathcal{O} \leftarrow \mathcal{U}_n} \text{Tr}(D_{\mathcal{A}} \cdot |\mathcal{A}^{\mathcal{O}} \rangle \langle \mathcal{A}^{\mathcal{O}}|_{\text{AB}}) - \mathbb{E}_{\mathcal{O} \sim H} \text{Tr}(D_{\mathcal{A}} \cdot |\mathcal{A}^{\mathcal{O}} \rangle \langle \mathcal{A}^{\mathcal{O}}|_{\text{AB}})| \leq \text{negl}(n), \quad (\text{B.2})$$

where $\text{negl}(n)$ is any function that is $o(1/n^c)$ for all $c > 0$.

We distinguish between two security levels based on the adversary's query capabilities:

- A **standard PRU** achieves indistinguishability against adversaries that can only make forward queries, i.e., where each $U_i = U$ in Definition 10.
- A **strong PRU** achieves indistinguishability against adversaries with access to all four query types: U , $U^\dagger$, U^* , and U^T , as defined in Definition 10.

The strong PRU definition considered here is stronger than that of [42] due to the ability for the oracle adversary to query the transpose U^T and complex conjugation U^* . We next show how to enhance the proof in [42] to handle transpose and complex conjugation.

B.2 Preliminaries

This section establishes the notation, definitions, and basic results from [42] that underpin our analysis. For completeness, we present all necessary background material.

B.2.1 Notations

Basic notation. Let $N := 2^n$ where n denotes the number of qubits. We write $[N] := \{1, \dots, N\}$ and identify $[N]$ with $\{0, 1\}^n$ via the binary representation of $i-1$ for each $i \in [N]$. For any $1 \leq t \leq N$, let $[N]_{\text{dist}}^t$ denote the set of length- t sequences of distinct integers from $[N]$:

$$[N]_{\text{dist}}^t := \{(x_1, \dots, x_t) \in [N]^t : x_i \neq x_j \text{ for all } i \neq j\}. \quad (\text{B.3})$$

For $t = 0$, we set $[N]_{\text{dist}}^0 := \{()\}$. For any permutation $\pi \in S_t$, define the unitary S_π acting on $(\mathbb{C}^N)^{\otimes t}$:

$$S_\pi : |x_1, \dots, x_t\rangle \mapsto |x_{\pi^{-1}(1)}, \dots, x_{\pi^{-1}(t)}\rangle. \quad (\text{B.4})$$

We let $x = x_{<} \| x_{>} \in \{0, 1\}^n$, where $x_{<}, x_{>} \in \{0, 1\}^{n/2}$ and $\|$ denotes bitstring concatenation.

Quantum registers. We use capital sans-serif letters for quantum registers. For register $\mathbf{A}$, the associated Hilbert space is $\mathcal{H}_{\mathbf{A}}$. States on multiple registers $(\mathbf{A}, \mathbf{B})$ belong to $\mathcal{H}_{\mathbf{A}} \otimes \mathcal{H}_{\mathbf{B}}$. We sometimes include register labels as subscripts, e.g., $|\psi\rangle_{\text{AB}}$. When an operator U acts only on subsystem $\mathbf{A}$, we write $U_{\mathbf{A}}$ and extend it trivially to larger systems. To reduce notation, we often omit identity operators and write $U_{\mathbf{A}} |\psi\rangle_{\text{AB}}$ instead of $(U_{\mathbf{A}} \otimes \mathbb{1}_{\mathbf{B}}) |\psi\rangle_{\text{AB}}$.

Given a projector Π on register $\mathbf{A}$, we say state $|\psi\rangle \in \mathcal{H}_{\mathbf{A}}$ is in the image of Π if $\Pi |\psi\rangle = |\psi\rangle$. For $|\psi\rangle \in \mathcal{H}_{\mathbf{A}} \otimes \mathcal{H}_{\mathbf{B}}$, we say $|\psi\rangle$ is in the image of $\Pi_{\mathbf{A}}$ if $\Pi_{\mathbf{A}} |\psi\rangle_{\text{AB}} = |\psi\rangle_{\text{AB}}$. We denote partial traces as $\text{Tr}_{\mathbf{B}}(|\psi\rangle \langle \psi|)$ or $\text{Tr}_{-\mathbf{A}}(|\psi\rangle \langle \psi|)$ when tracing out all systems except $\mathbf{A}$.

Relations A relation $R = \{(x_1, y_1), \dots, (x_t, y_t)\}$ is a multiset of ordered pairs $(x_i, y_i) \in [N]^2$. The size $|R|$ equals the number of pairs counting multiplicities.

Definition 12 (Sets of relations). Let $\mathcal{R}$ denote the set of all relations and $\mathcal{R}_t$ the set of all size- t relations. Define

$$\text{Dom}(R) = \{x \in [N] : \exists y \text{ such that } (x, y) \in R\}, \quad (\text{B.5})$$

$$\text{Im}(R) = \{y \in [N] : \exists x \text{ such that } (x, y) \in R\}, \quad (\text{B.6})$$

$$\text{Dom}_{<}(R) = \{x_{<} \in [\sqrt{N}] : \exists x_{>}, y \text{ such that } (x_{<} \| x_{>}, y) \in R\}, \quad (\text{B.7})$$

$$\text{Dom}_{>}(R) = \{x_{>} \in [\sqrt{N}] : \exists x_{<}, y \text{ such that } (x_{<} \| x_{>}, y) \in R\}, \quad (\text{B.8})$$

$$\text{Im}_{<}(R) = \{y_{<} \in [\sqrt{N}] : \exists x, y_{>} \text{ such that } (x, y_{<} \| y_{>}) \in R\}, \quad (\text{B.9})$$

$$\text{Im}_{>}(R) = \{y_{>} \in [\sqrt{N}] : \exists x, y_{<} \text{ such that } (x, y_{<} \| y_{>}) \in R\}. \quad (\text{B.10})$$

Each relation R corresponds to a *relation state* in the symmetric subspace.

Definition 13 (Relation states). For relation $R = \{(x_1, y_1), \dots, (x_t, y_t)\}$, define

$$|R\rangle := \frac{\sum_{\pi \in S_t} |x_{\pi(1)}, y_{\pi(1)}, \dots, x_{\pi(t)}, y_{\pi(t)}\rangle}{\sqrt{t! \cdot \prod_{(x,y) \in [N]^2} \text{num}(R, (x, y))!}}, \quad (\text{B.11})$$

where $\text{num}(R, (x, y))$ denotes the multiplicity of pair (x, y) in R .

The relation states form an orthonormal basis for the symmetric subspace of $(\mathbb{C}^{N^2})^{\otimes t}$. When all pairs in R are distinct, the normalization simplifies to $1/\sqrt{t!}$.

Definition 14 (Restricted relation sets). We define the restricted relation sets as follows.

- $\mathcal{R}_t^{\text{inj}}$: injective relations where $(y_1, \dots, y_t) \in [N]_{\text{dist}}^t$
- $\mathcal{R}_t^{\text{bij}}$: bijective relations where $(x_1, \dots, x_t), (y_1, \dots, y_t) \in [N]_{\text{dist}}^t$

We also define $\mathcal{R}^{\text{inj}} = \bigcup_{t=0}^N \mathcal{R}_t^{\text{inj}}$ and $\mathcal{R}^{\text{bij}} = \bigcup_{t=0}^N \mathcal{R}_t^{\text{bij}}$.

Variable-length registers For each $t \geq 0$, let $R^{(t)}$ be a register with Hilbert space $\mathcal{H}_{R^{(t)}} = (\mathbb{C}^N \otimes \mathbb{C}^N)^{\otimes t}$. Define the variable-length register R with infinite-dimensional Hilbert space

$$\mathcal{H}_R := \bigoplus_{t=0}^{\infty} \mathcal{H}_{R^{(t)}} = \bigoplus_{t=0}^{\infty} (\mathbb{C}^N \otimes \mathbb{C}^N)^{\otimes t}. \quad (\text{B.12})$$

We decompose $R^{(t)} = (R_X^{(t)}, R_Y^{(t)})$ where $R_X^{(t)}$ contains $|x_1, \dots, x_t\rangle$ and $R_Y^{(t)}$ contains $|y_1, \dots, y_t\rangle$. States of different lengths are orthogonal by the direct sum structure.

Definition 15 (Projectors and extensions). Define the projector onto relation states of size t :

$$\Pi_t^{\mathcal{R}} := \sum_{R \in \mathcal{R}_t} |R\rangle\langle R| = \Pi_{\text{sym}}^{N^2, t}, \quad (\text{B.13})$$

where $\Pi_{\text{sym}}^{N^2, t}$ projects onto the symmetric subspace of $(\mathbb{C}^{N^2})^{\otimes t}$. The projector onto all relation states is

$$\Pi^{\mathcal{R}} := \sum_{t=0}^{\infty} \Pi_t^{\mathcal{R}} = \sum_{R \in \mathcal{R}} |R\rangle\langle R|. \quad (\text{B.14})$$

For any operator O on $\mathcal{H}_{R^{(t)}}$, we extend it to $\mathcal{H}_R$ by acting as the zero operator on $\mathcal{H}_{R^{(t')}}$ for $t' \neq t$.

Definition 16 (Variable-length tensor powers). *For any unitary $U \in \mathcal{U}(N^2)$, define*

$$U^{\otimes*} := \sum_{t=0}^{\infty} U^{\otimes t} \quad (\text{B.15})$$

acting on $\mathcal{H}_R$.

Pairs of variable-length registers For constructions involving two variable-length registers L and R , we introduce additional notation.

Definition 17 (Length projectors). *For integers $\ell, r \geq 0$, let $\Pi_{\ell,r}$ project onto $\mathcal{H}_{L^{(\ell)}} \otimes \mathcal{H}_{R^{(r)}}$. For integer $t \geq 0$, let $\Pi_{\leq t}$ project onto $\bigoplus_{\ell,r \geq 0: \ell+r \leq t} \mathcal{H}_{L^{(\ell)}} \otimes \mathcal{H}_{R^{(r)}}$.*

Definition 18 (Length-restricted operators). *For operator B acting on registers L and R , define*

$$B_{\ell,r} := B \cdot \Pi_{\ell,r}, \quad (\text{B.16})$$

$$B_{\leq t} := B \cdot \Pi_{\leq t}. \quad (\text{B.17})$$

We adopt the convention that $B_{\leq t}^\dagger = (B_{\leq t})^\dagger$.

Bounding distances between quantum states In our analysis of pseudorandom unitaries, we will make use of the following helpful inequalities for bounding distances between quantum states. For any pure states $|u\rangle, |v\rangle$ with $\langle u|u\rangle, \langle v|v\rangle \leq 1$,

$$\| |u\rangle\langle u| - |v\rangle\langle v| \|_1 \leq 2 \| |u\rangle - |v\rangle \|_2. \quad (\text{B.18})$$

We also have the gentle measurement lemma,

$$\| \Pi \rho \Pi - \rho \|_1 \leq 2 \sqrt{1 - \text{tr}(\Pi \rho)}. \quad (\text{B.19})$$

Finally, we will use the following variant on gentle measurement lemma from [42].

Lemma 10 (Sequential gentle measurement; Lemma 2.3 of [42]). *Let $|\psi\rangle$ be a normalized state, $P_1, \dots, P_t$ be projectors, and $U_1, \dots, U_t$ be unitaries.*

$$\| U_t \dots U_1 |\psi\rangle - P_t U_t \dots P_1 U_1 |\psi\rangle \|_2 \leq t \sqrt{1 - \| P_t U_t \dots P_1 U_1 |\psi\rangle \|_2^2}. \quad (\text{B.20})$$

Formulas for the 2-design twirl Finally, we will make use of the following formulas for the twirl over an exact 2-design $\mathfrak{D}$. Let α denote any subset of n qubits, and $\bar{\alpha}$ its complement. Also let $\Pi^{\text{eq}} = \sum_x |x\rangle\langle x| \otimes |x\rangle\langle x|$ denote the projector onto bitstrings that are equal between two copies, and $\Pi^{\text{neq}} = 1 - \Pi^{\text{eq}}$ its complement. We have

$$\mathbb{E}_{U \sim \mathfrak{D}} \left[(U \otimes U)^\dagger \cdot \Pi_\alpha^{\text{eq}} \Pi_{\bar{\alpha}}^{\text{neq}} \cdot (U \otimes U) \right] = \frac{N_\alpha N_{\bar{\alpha}} (N_{\bar{\alpha}} - 1)}{N^2} \cdot \mathbb{1} \preceq \frac{1}{N_\alpha} \cdot \mathbb{1}, \quad (\text{B.21})$$

and

$$\mathbb{E}_{U \sim \mathfrak{D}} \left[(U \otimes \bar{U})^\dagger \cdot \Pi_\alpha^{\text{eq}} \Pi_{\bar{\alpha}}^{\text{neq}} \cdot (U \otimes \bar{U}) \right] = \frac{N_\alpha N_{\bar{\alpha}} (N_{\bar{\alpha}} - 1)}{N^2} \cdot \mathbb{1} \preceq \frac{1}{N_\alpha} \cdot \mathbb{1}. \quad (\text{B.22})$$

From this, for any approximate unitary 2-design with additive error ε , we have

$$\left\| \mathbb{E}_{U \sim \mathfrak{D}} \left[(U \otimes U)^\dagger \cdot \Pi_\alpha^{\text{eq}} \Pi_{\bar{\alpha}}^{\text{neq}} \cdot (U \otimes U) \right] \right\|_\infty \leq \frac{1}{N_\alpha} + \varepsilon, \quad (\text{B.23})$$

and for any strong approximate unitary 2-design with additive error ε , we have

$$\left\| \mathbb{E}_{U \sim \mathfrak{D}} \left[(U \otimes \bar{U})^\dagger \cdot \Pi_\alpha^{\text{eq}} \Pi_{\bar{\alpha}}^{\text{neq}} \cdot (U \otimes \bar{U}) \right] \right\|_\infty \leq \frac{1}{N_\alpha} + \varepsilon. \quad (\text{B.24})$$

B.3 The purified permutation-function oracle

We now introduce the strong PFC ensemble [40]. In the remaining subsections of this section, we will present our extension of the proof of [42] to include the conjugate and transpose. We also extend the proof to allow for any strong approximate unitary 2-design instead of an exact unitary 2-design.

We analyze the view of an adversary that can make standard, inverse, complex-conjugated, and transposed queries to an oracle $P_\pi \cdot F_f$, for uniformly random $\pi \sim \text{Sym}_N$ and a random **ternary** function $f \sim \{0, 1, 2\}^N$. This will motivate an extension of the definition of the path recording oracle V proposed in [42] to include its conjugate $\bar{V}$.

Definition 19 (Purified permutation-function oracle). *The purified permutation-function oracle pfO is a unitary acting on registers $\mathbf{A}, \mathbf{P}, \mathbf{F}$, where*

- $\mathbf{P}$ is a register associated with the Hilbert space $\mathcal{H}_{\mathbf{P}}$, defined to be the span of the orthonormal states $|\pi\rangle$ for all $\pi \in \text{Sym}_N$.
- $\mathbf{F}$ is a register associated with the Hilbert space $\mathcal{H}_{\mathbf{F}}$, defined to be the span of the orthonormal states $|f\rangle$ for all $f \in \{0, 1, 2\}^N$.

The unitary pfO is defined to act as follows:

$$\text{pfO}_{\mathbf{APF}} |x\rangle_{\mathbf{A}} |\pi\rangle_{\mathbf{P}} |f\rangle_{\mathbf{F}} := \omega_3^{f(x)} |\pi(x)\rangle_{\mathbf{A}} |\pi\rangle_{\mathbf{P}} |f\rangle_{\mathbf{F}}, \quad (\text{B.25})$$

$$= \sum_{y \in [N]} |y\rangle_{\mathbf{A}} \delta_{\pi(x)=y} |\pi\rangle_{\mathbf{P}} \omega_3^{f(x)} |f\rangle, \quad (\text{B.26})$$

for all $x \in [N]$, $\pi \in \text{Sym}_N$, and $f \in \{0, 1, 2\}^N$. Here, $\omega_3 = \exp(2\pi i/3)$.

The action of $\text{pfO}^\dagger$ is

$$\text{pfO}^\dagger |y\rangle_{\mathbf{A}} |\pi\rangle_{\mathbf{P}} |f\rangle_{\mathbf{F}} = \sum_{x \in [N]} |x\rangle_{\mathbf{A}} \delta_{\pi(x)=y} |\pi\rangle_{\mathbf{P}} \omega_3^{-f(x)} |f\rangle. \quad (\text{B.27})$$

The action of pfO^* is

$$\text{pfO}^* |x\rangle_{\mathbf{A}} |\pi\rangle_{\mathbf{P}} |f\rangle_{\mathbf{F}} = \sum_{y \in [N]} |y\rangle_{\mathbf{A}} \delta_{\pi(x)=y} |\pi\rangle_{\mathbf{P}} \omega_3^{-f(x)} |f\rangle. \quad (\text{B.28})$$

The action of pfO^T is

$$\text{pfO}^T |y\rangle_{\mathbf{A}} |\pi\rangle_{\mathbf{P}} |f\rangle_{\mathbf{F}} = \sum_{x \in [N]} |x\rangle_{\mathbf{A}} \delta_{\pi(x)=y} |\pi\rangle_{\mathbf{P}} \omega_3^{-f(x)} |f\rangle. \quad (\text{B.29})$$

Consider $P_\pi := \sum_{x \in [N]} |\pi(x)\rangle\langle x|$ and $F_f := \sum_{x \in [N]} \omega_3^{f(x)} |x\rangle\langle x|$. We have the equivalence:

Fact 1 (Equivalence of purified and standard oracles). *For any oracle adversary, the following oracle instantiations are perfectly indistinguishable:*

- (Queries to a random $P_\pi \cdot F_f$) Sample a uniformly random $\pi \sim \text{Sym}_N$, $f \sim \{0, 1, 2\}^N$. On each query, apply $(P_\pi \cdot F_f)$, $(P_\pi \cdot F_f)^\dagger$, $(P_\pi \cdot F_f)^*$, $(P_\pi \cdot F_f)^T$ to register $\mathbf{A}$.
- (Queries to pfO) Initialize registers $\mathbf{P}, \mathbf{F}$ to $\frac{1}{\sqrt{N!}} \sum_{\pi \in \text{Sym}_N} |\pi\rangle_{\mathbf{P}} \otimes \frac{1}{\sqrt{2^N}} \sum_{f \in \{0, 1, 2\}^N} |f\rangle_{\mathbf{F}}$. At each query, apply pfO , $\text{pfO}^\dagger$, pfO^* or pfO^T to registers $\mathbf{A}, \mathbf{P}, \mathbf{F}$.

Definition 20 (pf-relation state). For relation $L = \{(x_1, y_1), \dots, (x_\ell, y_\ell)\} \in \mathcal{R}_\ell$ and relation $R = \{(x'_1, y'_1), \dots, (x'_r, y'_r)\} \in \mathcal{R}_r$, where ℓ and r are non-negative integers such that $\ell + r \leq N$, let

$$|\text{pf}_{L,R}\rangle := \frac{1}{\sqrt{3^N(N-\ell-r)!}} \sum_{\pi \in \text{Sym}_N} \delta_{\pi, L \cup R} |\pi\rangle \sum_{f \in \{0,1,2\}^N} \omega_3^{f(x_1)+\dots+f(x_\ell)-(f(x'_1)+\dots+f(x'_r))} |f\rangle, \quad (\text{B.30})$$

where $\delta_{\pi, L \cup R}$ is an indicator variable that equals 1 if $\pi(x) = y$ for all $(x, y) \in L \cup R$, and is 0 otherwise.

Definition 21. Let $\mathcal{R}^{2,\text{dist}}$ be the set of all ordered pairs of relations $(L, R) \in \mathcal{R}^2$ where $L \cup R = \{(x_1, y_1), \dots, (x_t, y_t)\}$ is a bijective relation, i.e., $x_1, \dots, x_t$ are distinct and $y_1, \dots, y_t$ are distinct.

Lemma 11 (Orthonormality of pf-relation states; From Claim 7 of [42]). $\{|\text{pf}_{L,R}\rangle\}_{(L,R) \in \mathcal{R}^{2,\text{dist}}}$ is an orthonormal set of vectors.

Definition 22. Define the partial isometry $\text{Compress}^{\text{PF}} : \mathcal{H}_P \otimes \mathcal{H}_F \rightarrow \mathcal{H}_L \otimes \mathcal{H}_R$ to be

$$\text{Compress}^{\text{PF}} := \sum_{(L,R) \in \mathcal{R}^{2,\text{dist}}} |L\rangle_L \otimes |R\rangle_R \cdot \langle \text{pf}_{L,R} |_{\text{PF}}. \quad (\text{B.31})$$

We can use the action of pfO^* , pfO^T to strengthen Claim 8 of [42] to obtain the following.

Lemma 12 (Action of pfO ; From Claim 8 of [42]). For any $(L, R) \in \mathcal{R}^{2,\text{dist}}$ and $x \in [N]$ such that $x \notin \text{Dom}(L \cup R)$, we have

$$\text{pfO} |x\rangle_A |\text{pf}_{L,R}\rangle_{\text{PF}} = \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{y \in [N]: \\ y \notin \text{Im}(L \cup R)}} |y\rangle_A |\text{pf}_{L \cup \{(x,y)\}, R}\rangle_{\text{PF}}. \quad (\text{B.32})$$

For any $(L, R) \in \mathcal{R}^{2,\text{dist}}$ and $y \in [N]$ such that $y \notin \text{Im}(L \cup R)$, we have

$$\text{pfO}^\dagger |y\rangle_A |\text{pf}_{L,R}\rangle_{\text{PF}} = \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{x \in [N]: \\ x \notin \text{Dom}(L \cup R)}} |x\rangle_A |\text{pf}_{L, R \cup \{(x,y)\}}\rangle_{\text{PF}}. \quad (\text{B.33})$$

For any $(L, R) \in \mathcal{R}^{2,\text{dist}}$ and $x \in [N]$ such that $x \notin \text{Dom}(L \cup R)$, we have

$$\text{pfO}^* |x\rangle_A |\text{pf}_{L,R}\rangle_{\text{PF}} = \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{y \in [N]: \\ y \notin \text{Im}(L \cup R)}} |y\rangle_A |\text{pf}_{L, R \cup \{(x,y)\}}\rangle_{\text{PF}}. \quad (\text{B.34})$$

For any $(L, R) \in \mathcal{R}^{2,\text{dist}}$ and $y \in [N]$ such that $y \notin \text{Im}(L \cup R)$, we have

$$\text{pfO}^T |y\rangle_A |\text{pf}_{L,R}\rangle_{\text{PF}} = \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{x \in [N]: \\ x \notin \text{Dom}(L \cup R)}} |x\rangle_A |\text{pf}_{L \cup \{(x,y)\}, R}\rangle_{\text{PF}}. \quad (\text{B.35})$$

From the above lemma, we can see that pfO^* , pfO^T closely mimics pfO , $\text{pfO}^\dagger$ with the only difference being the relations L and R are switched.

B.4 The path-recording oracle V and its conjugate $\bar{V}$

The path-recording oracle V proposed in [42] efficiently simulates a Haar-random unitary U under both queries to U (via query to V) and $U^\dagger$ (via query to $V^\dagger$). In this work, we extend the path-recording framework to enable queries to $U, U^\dagger, U^*$, and U^T by defining a new operator $\bar{V}$ that serves as the conjugate of V . While $\bar{V}$ is not the actual complex conjugate of V , we will show that $V, V^\dagger, \bar{V}, \bar{V}^\dagger$ efficiently simulates a Haar-random unitary U under queries to $U, U^\dagger, U^*, U^T$, respectively.

To define the path-recording oracle V , we need to define the left part V^L and right part V^R of V .

Definition 23 (Left and right parts of V). *Let V^L be the linear operator that acts as follows. For $x \in [N]$ and $(L, R) \in \mathcal{R}^{2, \leq N-1}$,*

$$V^L \cdot |x\rangle_A |L\rangle_L |R\rangle_R := \sum_{\substack{y \in [N]: \\ y \notin \text{Im}(L \cup R)}} \frac{1}{\sqrt{N - |\text{Im}(L \cup R)|}} |y\rangle_A |L \cup \{(x, y)\}\rangle_L |R\rangle_R. \quad (\text{B.36})$$

Define V^R to be the linear operator such that for all $y \in [N]$ and $(L, R) \in \mathcal{R}^{2, \leq N-1}$,

$$V^R \cdot |y\rangle_A |L\rangle_L |R\rangle_R := \sum_{\substack{x \in [N]: \\ x \notin \text{Dom}(L \cup R)}} \frac{1}{\sqrt{N - |\text{Dom}(L \cup R)|}} |x\rangle_A |L \cup \{(x, y)\}\rangle_L |R\rangle_R. \quad (\text{B.37})$$

By construction, V^L and V^R take states in $\mathbb{1}_A \otimes \Pi_{\leq i, \text{LR}}^{\mathcal{R}^2}$ to $\mathbb{1}_A \otimes \Pi_{\leq i+1, \text{LR}}^{\mathcal{R}^2}$.

Lemma 13 (Claim 14 [42]). *V^L and V^R are partial isometries.*

Definition 24 (Path-recording oracle V). *The path-recording oracle is the operator V defined as*

$$V := V^L \cdot (\mathbb{1} - V^R \cdot V^{R, \dagger}) + (\mathbb{1} - V^L \cdot V^{L, \dagger}) \cdot V^{R, \dagger}. \quad (\text{B.38})$$

By construction, V and $V^\dagger$ take states in $\mathbb{1}_A \otimes \Pi_{\leq i, \text{LR}}^{\mathcal{R}^2}$ to $\mathbb{1}_A \otimes \Pi_{\leq i+1, \text{LR}}^{\mathcal{R}^2}$ for any integer $i \geq 0$.

Lemma 14 (Claim 15 [42]). *V is a partial isometry.*

We now define the conjugate $\bar{V}$ of V . This operator is not the actual complex conjugation of the path-recording oracle V . $\bar{V}$ is a new object proposed to simulate the action of the complex conjugation U^* of a Haar-random unitary U . And the conjugate transpose $\bar{V}^\dagger$ of $\bar{V}$ is designed to simulate the action of the transpose U^T of a Haar-random unitary U .

Definition 25 (Conjugated left and right parts of V). *Let $\bar{V}^L$ be the linear operator that acts as follows. For $x \in [N]$ and $(L, R) \in \mathcal{R}^{2, \leq N-1}$,*

$$\bar{V}^L \cdot |x\rangle_A |L\rangle_L |R\rangle_R := \sum_{\substack{y \in [N]: \\ y \notin \text{Im}(L \cup R)}} \frac{1}{\sqrt{N - |\text{Im}(L \cup R)|}} |y\rangle_A |L \cup \{(x, y)\}\rangle_L |R\rangle_R. \quad (\text{B.39})$$

Define $\bar{V}^R$ to be the linear operator such that for all $y \in [N]$ and $(L, R) \in \mathcal{R}^{2, \leq N-1}$,

$$\bar{V}^R \cdot |y\rangle_A |L\rangle_L |R\rangle_R := \sum_{\substack{x \in [N]: \\ x \notin \text{Dom}(L \cup R)}} \frac{1}{\sqrt{N - |\text{Dom}(L \cup R)|}} |x\rangle_A |L \cup \{(x, y)\}\rangle_L |R\rangle_R. \quad (\text{B.40})$$

By construction, $\bar{V}^L$ and $\bar{V}^R$ take states in $\mathbb{1}_A \otimes \Pi_{\leq i, \text{LR}}^{\mathcal{R}^2}$ to $\mathbb{1}_A \otimes \Pi_{\leq i+1, \text{LR}}^{\mathcal{R}^2}$.

Definition 26 (Conjugated path-recording oracle $\bar{V}$). *The conjugated path-recording oracle is the operator $\bar{V}$ defined as*

$$\bar{V} := \bar{V}^L \cdot (\mathbb{1} - \bar{V}^R \cdot \bar{V}^{R,\dagger}) + (\mathbb{1} - \bar{V}^L \cdot \bar{V}^{L,\dagger}) \cdot \bar{V}^{R,\dagger}. \quad (\text{B.41})$$

By construction, $\bar{V}$ and $\bar{V}^\dagger$ take states in $\mathbb{1}_A \otimes \Pi_{\leq i, \text{LR}}^{\mathcal{R}^2}$ to $\mathbb{1}_A \otimes \Pi_{\leq i+1, \text{LR}}^{\mathcal{R}^2}$ for any integer $i \geq 0$.

Because the main change in $\bar{V}$ over V is in swapping L and R , using the same proof as Claim 14 and 15 of [42], we have the following lemma.

Lemma 15. $\bar{V}^L$, $\bar{V}^R$, and $\bar{V}$ are partial isometries.

We next present a central property of the path-recording oracle V and its conjugate $\bar{V}$.

Definition 27. For any n -qubit unitary C, D , define

$$Q[C, D] := (C \otimes D^T)_{\text{L}}^{\otimes*} \otimes (C^* \otimes D^\dagger)_{\text{R}}^{\otimes*}, \quad (\text{B.42})$$

where C^* is the complex conjugate of C .

Because $\bar{V}$ corresponds to swapping L and R in V , using the same proof, we can obtain the following two-sided unitary invariance property for V and $\bar{V}$.

Lemma 16 (Two-sided unitary invariance; Claim 16 of [42]). *For any integer $0 \leq t \leq N-1$ and any pair of n -qubit unitaries C, D ,*

$$\|D_{\text{A}} \cdot V_{\leq t} \cdot C_{\text{A}} \otimes Q[C, D]_{\text{LR}} - Q[C, D]_{\text{LR}} \cdot V_{\leq t}\|_{\infty} \leq 16\sqrt{\frac{2t(t+1)}{N}}, \quad (\text{B.43})$$

$$\left\| C_{\text{A}}^\dagger \cdot (V^\dagger)_{\leq t} \cdot D_{\text{A}}^\dagger \otimes Q[C, D]_{\text{LR}} - Q[C, D]_{\text{LR}} \cdot (V^\dagger)_{\leq t} \right\|_{\infty} \leq 16\sqrt{\frac{2t(t+1)}{N}}, \quad (\text{B.44})$$

$$\|D_{\text{A}}^* \cdot \bar{V}_{\leq t} \cdot C_{\text{A}}^* \otimes Q[C, D]_{\text{LR}} - Q[C, D]_{\text{LR}} \cdot \bar{V}_{\leq t}\|_{\infty} \leq 16\sqrt{\frac{2t(t+1)}{N}}, \quad (\text{B.45})$$

$$\left\| C_{\text{A}}^T \cdot (\bar{V}^\dagger)_{\leq t} \cdot D_{\text{A}}^T \otimes Q[C, D]_{\text{LR}} - Q[C, D]_{\text{LR}} \cdot (\bar{V}^\dagger)_{\leq t} \right\|_{\infty} \leq 16\sqrt{\frac{2t(t+1)}{N}}, \quad (\text{B.46})$$

B.5 Partial path-recording oracle W and its conjugate $\bar{W}$

A very useful object proposed in [42] is the partial path-recording oracle W , which is a restricted version of the path-recording oracle V . The operator W only acts nontrivially on a subspace and maps the orthogonal subspace to zero. The subspace is defined based on $\mathcal{R}^{2, \text{dist}}$.

Similar to V , the partial path-recording oracle W contains a left part W^L and a right part W^R .

Definition 28 (W^L and W^R). *Define W^L to be the linear map such that for any $(L, R) \in \mathcal{R}^{2, \text{dist}}$ and $x \in [N]$ such that $x \notin \text{Dom}(L \cup R)$,*

$$W^L \cdot |x\rangle_{\text{A}} |L\rangle_{\text{L}} |R\rangle_{\text{R}} := \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{y \in [N]: \\ y \notin \text{Im}(L \cup R)}} |y\rangle_{\text{A}} |L \cup \{(x, y)\}\rangle_{\text{L}} |R\rangle_{\text{R}}. \quad (\text{B.47})$$

Similarly, define W^R be the linear map such that for any $(L, R) \in \mathcal{R}^{2, \text{dist}}$ and $y \in [N]$ such that $y \notin \text{Im}(L \cup R)$,

$$W^R \cdot |y\rangle_{\text{A}} |L\rangle_{\text{L}} |R\rangle_{\text{R}} := \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{x \in [N]: \\ x \notin \text{Dom}(L \cup R)}} |x\rangle_{\text{A}} |L\rangle_{\text{L}} |R \cup \{(x, y)\}\rangle_{\text{R}}. \quad (\text{B.48})$$

Definition 29. *The partial path-recording oracle is the operator W defined as*

$$W := W^L + W^{R,\dagger}. \quad (\text{B.49})$$

We now extend the definition of W in [42] to define its conjugate $\overline{W}$. Note that $\overline{W}$ is not the exact complex conjugate of W . However, intuitively speaking, for an oracle adversary, $\overline{W}$ will behave like the complex conjugation of W similar to how $\overline{V}$ behave like the complex conjugation of V .

Definition 30 (Conjugates of W^L, W^R , and W). *Define $\overline{W}^L$ to be the linear map such that for any $(L, R) \in \mathcal{R}^{2,\text{dist}}$ and $x \in [N]$ such that $x \notin \text{Dom}(L \cup R)$,*

$$\overline{W}^L \cdot |x\rangle_A |L\rangle_L |R\rangle_R := \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{y \in [N]: \\ y \notin \text{Im}(L \cup R)}} |y\rangle_A |L\rangle_L |R \cup \{(x, y)\}\rangle_R. \quad (\text{B.50})$$

Similarly, define $\overline{W}^R$ be the linear map such that for any $(L, R) \in \mathcal{R}^{2,\text{dist}}$ and $y \in [N]$ such that $y \notin \text{Im}(L \cup R)$,

$$\overline{W}^R \cdot |y\rangle_A |L\rangle_L |R\rangle_R := \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{x \in [N]: \\ x \notin \text{Dom}(L \cup R)}} |x\rangle_A |L \cup \{(x, y)\}\rangle_L |R\rangle_R. \quad (\text{B.51})$$

The conjugate of the partial path-recording oracle W is the operator $\overline{W}$ defined as

$$\overline{W} := \overline{W}^L + \overline{W}^{R,\dagger}. \quad (\text{B.52})$$

We instantiate the following definitions of projectors.

Definition 31 (Bijective-relation projectors). *Define the projectors*

$$\Pi_{\text{LR}}^{\text{bij}} := \sum_{(L,R) \in \mathcal{R}^{2,\text{dist}}} |L\rangle\langle L|_L \otimes |R\rangle\langle R|_R, \quad \Pi_{\leq t, \text{LR}}^{\text{bij}} := \Pi_{\text{LR}}^{\text{bij}} \cdot \Pi_{\leq t, \text{LR}} = \Pi_{\leq t, \text{LR}} \cdot \Pi_{\text{LR}}^{\text{bij}}, \quad (\text{B.53})$$

where the projector $\Pi_{\leq t, \text{LR}}$ is the maximum-length projector defined in Definition 17.

Definition 32. *For a partial isometry G , let $\mathcal{D}(G)$ and $\mathcal{I}(G)$ denote its domain and image. Let $\Pi^{\mathcal{D}(G)} = G^\dagger \cdot G$ and $\Pi^{\mathcal{I}(G)} = G \cdot G^\dagger$ denote the orthogonal projectors onto $\mathcal{D}(G)$ and $\mathcal{I}(G)$.*

Because the conjugated versions of W^L, W^R , and W amounts to swapping the L and R register, the proofs in [42] can be combined with the action of pfO^* and pfO^T to establish the following lemmas.

Lemma 17 (W is a restriction of pfO up to isometry; From Claim 13 of [42]). *We have*

$$W = \text{Compress} \cdot \text{pfO} \cdot \text{Compress}^\dagger \cdot \Pi^{\mathcal{D}(W)}, \quad (\text{B.54})$$

$$W^\dagger = \text{Compress} \cdot \text{pfO}^\dagger \cdot \text{Compress}^\dagger \cdot \Pi^{\mathcal{I}(W)} \quad (\text{B.55})$$

$$\overline{W} = \text{Compress} \cdot \text{pfO}^* \cdot \text{Compress}^\dagger \cdot \Pi^{\mathcal{D}(\overline{W})}, \quad (\text{B.56})$$

$$\overline{W}^\dagger = \text{Compress} \cdot \text{pfO}^{\dagger *} \cdot \text{Compress}^\dagger \cdot \Pi^{\mathcal{I}(\overline{W})}. \quad (\text{B.57})$$

Lemma 18 (From Fact 5 of [42]). *For any integer $i \geq 0$, $W^L, W^R, \overline{W}^L, \overline{W}^R$ map states in the subspace associated to the projector $\mathbb{1}_A \otimes \Pi_{\leq i, \text{LR}}^{\text{bij}}$ into the subspace associated with the projector $\mathbb{1}_A \otimes \Pi_{\leq i+1, \text{LR}}^{\text{bij}}$.*

Lemma 19 (From Claim 9 and Claim 11 of [42]). $W^L, W^R, W, \overline{W}^L, \overline{W}^R, \overline{W}$ are partial isometries.

Lemma 20 (From Fact 8 of [42]). The domain and image of the partial isometry W are given by

$$\Pi^{\mathcal{D}(W)} = \Pi^{\mathcal{D}(W^L)} + \Pi^{\mathcal{I}(W^R)}, \quad (\text{B.58})$$

$$\Pi^{\mathcal{I}(W)} = \Pi^{\mathcal{D}(W^R)} + \Pi^{\mathcal{I}(W^L)}. \quad (\text{B.59})$$

The domain and image of the partial isometry $\overline{W}$ are given by

$$\Pi^{\mathcal{D}(\overline{W})} = \Pi^{\mathcal{D}(\overline{W}^L)} + \Pi^{\mathcal{I}(\overline{W}^R)}, \quad (\text{B.60})$$

$$\Pi^{\mathcal{I}(\overline{W})} = \Pi^{\mathcal{D}(\overline{W}^R)} + \Pi^{\mathcal{I}(\overline{W}^L)}. \quad (\text{B.61})$$

Lemma 21 (From Claim 10 and Claim 12 of [42]). For all integers $t \geq 0$, $\Pi_{\leq t}$ commutes with $\Pi^{\mathcal{D}(W^L)}$, $\Pi^{\mathcal{I}(W^L)}$, $\Pi^{\mathcal{D}(W^R)}$, $\Pi^{\mathcal{I}(W^R)}$, $\Pi^{\mathcal{D}(W)}$, $\Pi^{\mathcal{I}(W)}$, $\Pi^{\mathcal{D}(\overline{W}^L)}$, $\Pi^{\mathcal{I}(\overline{W}^L)}$, $\Pi^{\mathcal{D}(\overline{W}^R)}$, $\Pi^{\mathcal{I}(\overline{W}^R)}$, $\Pi^{\mathcal{D}(\overline{W})}$, and $\Pi^{\mathcal{I}(\overline{W})}$.

Lemma 22 (W is a restriction of V ; From Claim 17 of [42]). We have

$$W = V \cdot \Pi^{\mathcal{D}(W)}, \quad (\text{B.62})$$

$$W^\dagger = V^\dagger \cdot \Pi^{\mathcal{I}(W)}, \quad (\text{B.63})$$

$$\overline{W} = \overline{V} \cdot \Pi^{\mathcal{D}(\overline{W})}, \quad (\text{B.64})$$

$$\overline{W}^\dagger = \overline{V}^\dagger \cdot \Pi^{\mathcal{I}(\overline{W})}. \quad (\text{B.65})$$

Lemma 23 (From Corollary 8.3 of [42]). We have

$$W^\dagger \cdot V = \Pi^{\mathcal{D}(W)}, \quad (\text{B.66})$$

$$W \cdot V^\dagger = \Pi^{\mathcal{I}(W)}, \quad (\text{B.67})$$

$$\overline{W}^\dagger \cdot \overline{V} = \Pi^{\mathcal{D}(\overline{W})}, \quad (\text{B.68})$$

$$\overline{W} \cdot \overline{V}^\dagger = \Pi^{\mathcal{I}(\overline{W})}. \quad (\text{B.69})$$

Lemma 24 (Twirling by strong approximate unitary 2-design; From Lemma 9.2 of [42]). For any strong approximate unitary 2-design $\mathfrak{D}$ with additive error ε , and any integer $0 \leq t \leq N-1$, we have

$$\left\| \mathbb{E}_{C,D \sim \mathfrak{D}} (C_A \otimes Q[C, D]_{\text{LR}})^\dagger \cdot \left(\Pi_{\leq t, \text{LR}}^{\text{bij}} - \Pi_{\leq t, \text{ALR}}^{\mathcal{D}(W)} \right) \cdot (C_A \otimes Q[C, D]_{\text{LR}}) \right\|_\infty \leq 6t \sqrt{\frac{t}{N}} + 2t\varepsilon, \quad (\text{B.70})$$

$$\left\| \mathbb{E}_{C,D \sim \mathfrak{D}} (D_A^\dagger \otimes Q[C, D]_{\text{LR}})^\dagger \cdot \left(\Pi_{\leq t, \text{LR}}^{\text{bij}} - \Pi_{\leq t, \text{ALR}}^{\mathcal{I}(W)} \right) \cdot (D_A^\dagger \otimes Q[C, D]_{\text{LR}}) \right\|_\infty \leq 6t \sqrt{\frac{t}{N}} + 2t\varepsilon, \quad (\text{B.71})$$

$$\left\| \mathbb{E}_{C,D \sim \mathfrak{D}} (C_A^* \otimes Q[C, D]_{\text{LR}})^\dagger \cdot \left(\Pi_{\leq t, \text{LR}}^{\text{bij}} - \Pi_{\leq t, \text{ALR}}^{\mathcal{D}(\overline{W})} \right) \cdot (C_A^* \otimes Q[C, D]_{\text{LR}}) \right\|_\infty \leq 6t \sqrt{\frac{t}{N}} + 2t\varepsilon, \quad (\text{B.72})$$

$$\left\| \mathbb{E}_{C,D \sim \mathfrak{D}} (D_A^T \otimes Q[C, D]_{\text{LR}})^\dagger \cdot \left(\Pi_{\leq t, \text{LR}}^{\text{bij}} - \Pi_{\leq t, \text{ALR}}^{\mathcal{I}(\overline{W})} \right) \cdot (D_A^T \otimes Q[C, D]_{\text{LR}}) \right\|_\infty \leq 6t \sqrt{\frac{t}{N}} + 2t\varepsilon. \quad (\text{B.73})$$

Proof. The proof follows from the proof of Lemma 9.2 in [99] with one replacement. In Claims 29 and 30 and Eq. (11.82), [99] uses the following spectral norm bound for the twirl over an *exact* unitary 2-design $\mathfrak{D}'$,

$$\left\| \mathbb{E}_{U \sim \mathfrak{D}'} \left[(U \otimes U)^\dagger \cdot \Pi^{\text{eq}} \cdot (U \otimes U) \right] \right\|_\infty \leq \frac{2}{N+1}, \quad (\text{B.74})$$

$$\left\| \mathbb{E}_{U \sim \mathfrak{D}'} \left[(U \otimes U^*) \cdot (\Pi^{\text{eq}} - \Pi^{\text{EPR}}) \cdot (U \otimes U^*) \right] \right\|_{\infty} \leq \frac{1}{N+1}. \quad (\text{B.75})$$

Here, we replace these bounds with analogous bounds for the twirl over an *approximate* unitary 2-design $\mathfrak{D}$. For any (standard) approximate unitary 2-design with additive error ε , the first inequality becomes,

$$\left\| \mathbb{E}_{U \sim \mathfrak{D}} \left[(U \otimes U)^{\dagger} \cdot \Pi^{\text{eq}} \cdot (U \otimes U) \right] \right\|_{\infty} \leq \frac{2}{N+1} + \varepsilon. \quad (\text{B.76})$$

Meanwhile, for any strong approximate unitary 2-design with additive error ε , the second inequality becomes,

$$\left\| \mathbb{E}_{U \sim \mathfrak{D}'} \left[(U \otimes U^*) \cdot (\Pi^{\text{eq}} - \Pi^{\text{EPR}}) \cdot (U \otimes U^*) \right] \right\|_{\infty} \leq \frac{1}{N+1} + \varepsilon. \quad (\text{B.77})$$

To derive the first inequality, we abbreviate $\Phi_{\mathfrak{D}}(X) \equiv \mathbb{E}_{U \sim \mathfrak{D}} [(U \otimes U)X(U \otimes U)^{\dagger}]$ and $\delta\Phi_{\mathfrak{D}} \equiv \Phi_{\mathfrak{D}} - \Phi_{\mathfrak{D}'}$, and apply $\|\delta\Phi_{\mathfrak{D}}^{\dagger}(O)\|_{\infty} = \max_{\rho} \text{tr}(\delta\Phi_{\mathfrak{D}}^{\dagger}(O)\rho) = \max_{\rho} \text{tr}(O\delta\Phi_{\mathfrak{D}}(\rho)) \leq \max_{\rho} \|O\|_{\infty} \cdot \|\Phi_{\mathfrak{D}}(\rho)\|_1 \leq \|O\|_{\infty} \cdot \varepsilon$. An identical series of steps derives the second inequality. Propagating this replacement through the remainder of the proof yields Lemma 24. $\square$

Note that in the statement of Lemma 24, $\Pi_{\leq t, \text{LR}}^{\text{bij}}$ is shorthand for $\mathbb{1}_{\text{A}} \otimes \Pi_{\leq t, \text{LR}}^{\text{bij}}$, and thus the operators inside the spectral norm $\|\cdot\|_{\infty}$ act on $\text{A}, \text{L}, \text{R}$.

B.6 $V, \bar{V}$ approximates Haar-random unitary U under $U, U^{\dagger}, U^*, U^T$

Because all lemmas generalize to complex conjugation and transpose using the suitably defined $\bar{W}$ and $\bar{V}$, we can follow the same proof of [42] to show that the extended path recording oracle $V, \bar{V}$ approximates the following random unitary ensemble under $U, U^{\dagger}, U^*, U^T$.

Definition 33 (sPFC($\mathfrak{D}$) distribution). *For any distribution $\mathfrak{D}$ supported on $\mathcal{U}(N)$, define the distribution sPFC($\mathfrak{D}$) as follows:*

1. *Sample a uniformly random permutation $\pi \sim \text{Sym}_N$, a uniformly random $f \sim \{0, 1, 2\}^N$, and two independently sampled n -qubit unitaries $C, D \sim \mathfrak{D}$. Following the definitions in Section B.3,*

$$F_f := \sum_{x \in [N]} e^{2\pi \cdot f(x) \cdot i/3} |x\rangle\langle x| \quad \text{and} \quad P_{\pi} := \sum_{x \in [N]} |\pi(x)\rangle\langle x|. \quad (\text{B.78})$$

2. *Output the n -qubit unitary $\mathcal{O} := D \cdot P_{\pi} \cdot F_f \cdot C$.*

Definition 34 (Global state after queries to $V, \bar{V}$). *For a t -query oracle adversary $\mathcal{A}$ that can perform queries to $U, U^{\dagger}, U^*, U^T$, where $b_i \in \{0, 1\}$ and $c_i \in \{0, 1\}$ denote the four choices ($U \rightarrow b_i = 0, c_i = 0$; $U^{\dagger} \rightarrow b_i = 1, c_i = 0$; $U^* \rightarrow b_i = 0, c_i = 1$; $U^T \rightarrow b_i = 1, c_i = 1$), and any $0 \leq i \leq t$, let*

$$|\mathcal{A}_i^{V, \bar{V}}\rangle_{\text{ABLR}} := \prod_{i=1}^t \left(\left((1 - c_i)((1 - b_i) \cdot V_{\text{ALR}} + b_i \cdot V_{\text{ALR}}^{\dagger}) \right. \right. \quad (\text{B.79})$$

$$\left. + c_i((1 - b_i) \cdot \bar{V}_{\text{ALR}} + b_i \cdot \bar{V}_{\text{ALR}}^{\dagger}) \right) \cdot A_{i, \text{AB}} \Big) |0^{n+m}\rangle_{\text{AB}} \otimes |\emptyset\rangle_{\text{L}} |\emptyset\rangle_{\text{R}} \quad (\text{B.80})$$

denote the global state on registers $\text{A}, \text{B}, \text{L}, \text{R}$ after $\mathcal{A}$ makes i queries to V .

We will also consider the global purified state after queries to $W, \overline{W}$, where we twirl the input and the output states by two independent random unitaries sampled from any unitary 2-design. For this purpose, we define the purification of two random unitaries C, D .

Definition 35. For any distribution $\mathfrak{D}$ over n -qubit unitaries, define the state

$$|\text{init}(\mathfrak{D})\rangle_{\text{CD}} := \int_{C,D} \sqrt{d\mu_{\mathfrak{D}}(C)d\mu_{\mathfrak{D}}(D)} |C\rangle_C \otimes |D\rangle_D, \quad (\text{B.81})$$

where $\mu_{\mathfrak{D}}(C)$ is the probability measure for which C is sampled from $\mathfrak{D}$.

Definition 36 (Controlled C, D and Q). Define the following operators

$$\text{cC} := \int_C C_A \otimes |C\rangle\langle C|_C, \quad \text{cD} := \int_D D_A \otimes |D\rangle\langle D|_D, \quad (\text{B.82})$$

$$\text{cQ} := \int_{C,D} Q[C, D]_{\text{L,R}} \otimes |C\rangle\langle C|_C \otimes |D\rangle\langle D|_D. \quad (\text{B.83})$$

Definition 37 (Global state after queries to Twirled $W, \overline{W}$). For a t -query adversary $\mathcal{A}$ that can perform queries to $U, U^\dagger, U^*, U^T$, where $b_i \in \{0, 1\}$ and $c_i \in \{0, 1\}$ denote the four choices ($U \rightarrow b_i = 0, c_i = 0; U^\dagger \rightarrow b_i = 1, c_i = 0; U^* \rightarrow b_i = 0, c_i = 1; U^T \rightarrow b_i = 1, c_i = 1$), let

$$|\mathcal{A}_0^{W, \overline{W}, \mathfrak{D}}\rangle := |0^n\rangle_A |0^m\rangle_B |\emptyset\rangle_L |\emptyset\rangle_R |\text{init}(\mathfrak{D})\rangle_{\text{CD}}. \quad (\text{B.84})$$

For i from 1 to t , let

$$|\mathcal{A}_i^{W, \overline{W}, \mathfrak{D}}\rangle := \left((1 - c_i)((1 - b_i) \cdot (\text{cD} \cdot W \cdot \text{cC}) + b_i \cdot (\text{cD} \cdot W \cdot \text{cC})^\dagger) + \right. \quad (\text{B.85})$$

$$\left. c_i((1 - b_i) \cdot (\text{cD}^* \cdot \overline{W} \cdot \text{cC}^*) + b_i \cdot (\text{cD}^* \cdot \overline{W} \cdot \text{cC}^*)^\dagger) \right) \cdot A_i \cdot |\mathcal{A}_{i-1}^{W, \mathfrak{D}}\rangle. \quad (\text{B.86})$$

Lemma 25 (W is indistinguishable from V after twirling; From Lemma 9.3 of [42]). Let $\mathfrak{D}$ be any strong approximate unitary 2-design with additive error ε . For any t -query oracle adversary $\mathcal{A}$ that can query $\mathcal{O}, \mathcal{O}^\dagger, \mathcal{O}^*, \mathcal{O}^T$,

$$\text{TD}(\text{Tr}_{\text{AB}} |\mathcal{A}_t^{W, \overline{W}, \mathfrak{D}}\rangle\langle \mathcal{A}_t^{W, \overline{W}, \mathfrak{D}}|_{\text{ABLRCD}}, \text{Tr}_{\text{AB}} |\mathcal{A}_t^{V, \overline{V}}\rangle\langle \mathcal{A}_t^{V, \overline{V}}|_{\text{ABLR}}) \leq \frac{9t}{N^{1/8}} + 2t^{1/4}\varepsilon^{1/4}. \quad (\text{B.87})$$

Proof. The proof follows from the proof of Lemma 9.3 in [99] with one replacement. In the application of Lemma 9.2 in Eq. (9.45) of the proof of Claim 18, we apply Lemma 24 for the twirl over a strong ε -approximate unitary 2-design instead. This modifies the right hand side of the statement of Claim 18 to $1 - 35t^2/N^{1/4} - \sqrt{2t\varepsilon}$. Propagating this replacement through the rest of the proof of Lemma 9.3 and applying the inequality $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$ yields Lemma 25. $\square$

Lemma 26 ($\text{sPFC}(\mathfrak{D})$ is indistinguishable from V ; From Lemma 9.1 of [42]). Let $\mathfrak{D}$ be any strong approximate unitary 2-design with additive error ε . For any t -query oracle adversary $\mathcal{A}$ that can query $\mathcal{O}, \mathcal{O}^\dagger, \mathcal{O}^*, \mathcal{O}^T$,

$$\text{TD} \left(\mathbb{E}_{\mathcal{O} \sim \text{sPFC}(\mathfrak{D})} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle \mathcal{A}_t^{\mathcal{O}}|_{\text{AB}}, \text{Tr}_{\text{LR}} \left(|\mathcal{A}_t^{V, \overline{V}}\rangle\langle \mathcal{A}_t^{V, \overline{V}}|_{\text{ABLR}} \right) \right) \leq \frac{9t(t+1)}{N^{1/8}} + 4t^{5/4}\varepsilon^{1/4}. \quad (\text{B.88})$$

Proof. The proof follows from the proof of Lemma 9.1 in [99]. The right hand side of the statement of Lemma 9.4 is modified to $1 - 70t^2/N^{1/4} - 2\sqrt{2t\varepsilon}$ following the modification of Claim 18. From this, the right hand side of the statement of Lemma 9.5 is modified to $9t^2/N^{1/8} + t\sqrt{2\sqrt{2t\varepsilon}} \leq 9t^2/N^{1/8} + 2t^{5/4}\varepsilon^{1/4}$. Inserting this modification and that of Lemma 25 into the proof of Lemma 9.1 in [99] yields Lemma 26. $\square$

Theorem 10 (V is indistinguishable from a Haar-random unitary; From Theorem 8 of [42]). *For any t -query oracle adversary $\mathcal{A}$ that can query $\mathcal{O}, \mathcal{O}^\dagger, \mathcal{O}^*, \mathcal{O}^T$,*

$$\text{TD} \left(\mathbb{E}_{\mathcal{O} \sim \mu_{\text{Haar}}} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\text{AB}}, \text{Tr}_{\text{LR}} \left(|\mathcal{A}_t^{V,\bar{V}}\rangle\langle\mathcal{A}_t^{V,\bar{V}}|_{\text{ABLR}} \right) \right) \leq \frac{9t(t+1)}{N^{1/8}}. \quad (\text{B.89})$$

To simplify the notation, we will often denote $|\mathcal{A}_t^{V,\bar{V}}\rangle_{\text{ABLR}}$ as simply $|\mathcal{A}_t^V\rangle_{\text{ABLR}}$. Similarly, we will denote $|\mathcal{A}_t^{W,\bar{W},\mathfrak{D}}\rangle_{\text{ABLRCD}}$ as simply $|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\text{ABLRCD}}$ when appropriate.

C The Luby-Rackoff-Function-Clifford (LRFC) ensemble

In this section we present the central random unitary construction of this work, the Luby-Rackoff-Function-Clifford (LRFC) ensemble, which only uses random unitary 2-designs and random functions. The LRFC ensemble does not require the use of random permutations, which is useful for generating minimum depth strong random unitaries, due to the lack of known low-depth constructions of quantum-secure pseudorandom permutations. The best known construction of quantum-secure strong pseudorandom permutations is given in [73], which requires $\text{poly}(n)$ circuit depth for n -qubit systems.

In what follows, we first define the LRFC ensemble and then proceed step-by-step through our proof that it is indistinguishable from a Haar-random unitary.

C.1 Definition of the ensemble

We begin by formally defining the LRFC ensemble and its key ingredients.

Feistel network. Let n be the number of qubits and $N := 2^n$. Our construction utilizes a simple variant of the Feistel network, also known as the Luby-Rackoff construction [75]. For a function $h : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$, we define the *Left* and *Right* Luby-Rackoff function as follows:

$$\mathbf{L}_h(x_{<} \| x_{>}) := (x_{<} \oplus h(x_{>})) \| x_{>}, \quad (\text{C.1})$$

$$\mathbf{R}_h(x_{<} \| x_{>}) := x_{<} \| (x_{>} \oplus h(x_{<})), \quad (\text{C.2})$$

where $x = x_{<} \| x_{>} \in \{0, 1\}^n$, and $\|$ denotes bitstring concatenation.

Quantum oracles. We define the following n -qubit quantum oracles:

$$\mathcal{O}^f := \sum_{x \in \{0,1\}^n} e^{2\pi i f(x)/3} |x\rangle\langle x|, \quad (\text{C.3})$$

$$\mathcal{O}^{\mathbf{L}, h_1} := \sum_{x \in \{0,1\}^n} |\mathbf{L}_{h_1}(x)\rangle\langle x| = \sum_{x \in \{0,1\}^n} |(x_{<} \oplus h_1(x_{>})) \| x_{>}\rangle\langle x|, \quad (\text{C.4})$$

$$\mathcal{O}^{\mathbf{R}, h_2} := \sum_{x \in \{0,1\}^n} |\mathbf{R}_{h_2}(x)\rangle\langle x| = \sum_{x \in \{0,1\}^n} |x_{<} \| (x_{>} \oplus h_2(x_{<}))\rangle\langle x|. \quad (\text{C.5})$$

These are identical to the operators F, S_L, S_R defined in the main text.

Construction. Let C, D be two n -qubit random unitaries sampled independently from a unitary 2-design, such as a random Clifford circuit. A random unitary U sampled from the LRFC ensemble is given by:

$$U := D \cdot \mathcal{O}^{\mathbf{R}, h_2} \cdot \mathcal{O}^{\mathbf{L}, h_1} \cdot \mathcal{O}^f \cdot C. \quad (\text{C.6})$$

Putting everything together, we have the following definition for LRFC ensemble.

Definition 38 (LRFC ensemble). *Suppose h_1 and h_2 are drawn uniformly randomly from functions on $\{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$, f is drawn uniformly randomly from ternary functions on $\{0, 1\}^n$, and C, D are drawn uniformly from a unitary 2-design on n qubits. Then the Luby-Rackoff-Function-Clifford (LRFC) ensemble is given by the family of n -qubit unitaries:*

$$U := \sum_{x \in \{0, 1\}^n} e^{2\pi i f(x)/3} \cdot D \cdot |x_{<} \oplus h_1(x_{>})\|x_{>} \oplus h_2(x_{<} \oplus h_1(x_{>}))\rangle\langle x| \cdot C, \quad (\text{C.7})$$

where $\|$ denotes the concatenation of two $\frac{n}{2}$ -bit strings and $x = x_{<} \| x_{>}$.

C.2 Purified Luby-Rackoff-Function oracle

In this section, we analyze the view of an adversary that makes queries to an oracle implementing the Luby-Rackoff-Function construction with random functions h_1, h_2 , and a random ternary function f . We will do this by analyzing the *purified Luby-Rackoff-Function oracle*, which uses a purification of these random functions.

Definition 39 (Purified Luby-Rackoff-Function oracle). *The purified Luby-Rackoff-Function oracle lrfo is a unitary acting on registers A, H_1, H_2, F , where*

- H_1 is a register associated with the Hilbert space $\mathcal{H}_{H_1}$, defined to be the span of the orthonormal states $|h_1\rangle$ for all $h_1 : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$.
- H_2 is a register associated with the Hilbert space $\mathcal{H}_{H_2}$, defined to be the span of the orthonormal states $|h_2\rangle$ for all $h_2 : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$.
- F is a register associated with the Hilbert space $\mathcal{H}_F$, defined to be the span of the orthonormal states $|f\rangle$ for all $f : \{0, 1\}^n \rightarrow \{0, 1, 2\}$.

The unitary lrfo is defined to act as follows:

$$\text{lrfo}_{AH_1H_2F} |x\rangle_A |h_1\rangle_{H_1} |h_2\rangle_{H_2} |f\rangle_F \quad (\text{C.8})$$

$$:= \omega_3^{f(x)} |x_{<} \oplus h_1(x_{>})\|x_{>} \oplus h_2(x_{<} \oplus h_1(x_{>}))\rangle_A |h_1\rangle_{H_2} |h_2\rangle_{H_2} |f\rangle_F, \quad (\text{C.9})$$

for all $x = x_{<} \| x_{>} \in \{0, 1\}^n$ with $x_{<}, x_{>} \in \{0, 1\}^{n/2}$, and for all functions $h_1, h_2 : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$, $f : \{0, 1\}^n \rightarrow \{0, 1, 2\}$. Here, $\omega_3 = \exp(2\pi i/3)$.

The action of lrfo^* is

$$\text{lrfo}^* |x\rangle_A |h_1\rangle_{H_1} |h_2\rangle_{H_2} |f\rangle_F \quad (\text{C.10})$$

$$= \omega_3^{-f(x)} |x_{<} \oplus h_1(x_{>})\|(x_{>} \oplus h_2(x_{<} \oplus h_1(x_{>})))\rangle_A |h_1\rangle_{H_2} |h_2\rangle_{H_2} |f\rangle_F. \quad (\text{C.11})$$

The action of $\text{lrfo}^\dagger$ is

$$\text{lrfo}^\dagger |y\rangle_A |h_1\rangle_{H_1} |h_2\rangle_{H_2} |f\rangle_F \quad (\text{C.12})$$

$$= \omega_3^{-f(x)} |(y_{<} \oplus h_1(y_{>} \oplus h_2(y_{<})))\|y_{>} \oplus h_2(y_{<})\rangle_A |h_1\rangle_{H_2} |h_2\rangle_{H_2} |f\rangle_F. \quad (\text{C.13})$$

The action of lrfo^T is

$$\text{lrfo}^T |y\rangle_A |h_1\rangle_{H_1} |h_2\rangle_{H_2} |f\rangle_F \quad (\text{C.14})$$

$$= \omega_3^{f(x)} |(y_{<} \oplus h_1(y_{>} \oplus h_2(y_{<})))\|y_{>} \oplus h_2(y_{<})\rangle_A |h_1\rangle_{H_2} |h_2\rangle_{H_2} |f\rangle_F. \quad (\text{C.15})$$

Because lrfo is constructed by purifying the randomness in h_1, h_2, f , the output state of any oracle adversary that queries the purified oracle after tracing out H_1, H_2, F is equivalent to the output state of the adversary that queries the standard oracle $\mathcal{O}^{R, h_2} \cdot \mathcal{O}^{L, h_1} \cdot \mathcal{O}^f$, for uniformly random $h_1, h_2 \sim \{0, 1\}^{n/2 \cdot \sqrt{N}}$ and $f \sim \{0, 1, 2\}^N$.

Fact 2 (Equivalence of purified and standard oracles). *For any oracle adversary, the following oracle instantiations are perfectly indistinguishable:*

- (Queries to a random $\mathcal{O}^{R, h_2} \cdot \mathcal{O}^{L, h_1} \cdot \mathcal{O}^f$) Sample a uniformly random $h_1, h_2 \sim \{0, 1\}^{n/2 \cdot \sqrt{N}}$, $f \sim \{0, 1, 2\}^N$. On each query, apply $U = \mathcal{O}^{R, h_2} \cdot \mathcal{O}^{L, h_1} \cdot \mathcal{O}^f, U^\dagger, U^*$ or U^T to register A .
- (Queries to lrfo) Initialize registers H_1, H_2, F to $\frac{1}{\sqrt{N} \sqrt{N}} \sum_{h_1, h_2: \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}} |h_1\rangle_{H_1} \otimes |h_2\rangle_{H_2} \otimes \frac{1}{\sqrt{3^N}} \sum_{f \in \{0, 1, 2\}^N} |f\rangle_F$. On each query, apply $\text{lrfo}, \text{lrfo}^\dagger, \text{lrfo}^*$ or lrfo^T to registers A, H_1, H_2, F .

Next, we define the relation states for the LRF oracle.

Definition 40 (lrf-relation state). *For the relations $L = \{(x_1, y_1), \dots, (x_\ell, y_\ell)\} \in \mathcal{L}_\ell$ and $R = \{(x'_1, y'_1), \dots, (x'_r, y'_r)\} \in \mathcal{R}_r$, where ℓ and r are non-negative integers such that $\ell + r \leq 2^{n/2}$, let*

$$|\text{lrf}_{L,R}\rangle_{H_1 H_2 F} := \frac{1}{\sqrt{\sqrt{N} \sqrt{N}^{\ell+r}}} \sum_{h_1: \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}} \delta_{h_1, L \cup R} |h_1\rangle_{H_1} \quad (\text{C.16})$$

$$\otimes \frac{1}{\sqrt{\sqrt{N} \sqrt{N}^{\ell+r}}} \sum_{h_2: \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}} \delta'_{h_2, L \cup R} |h_2\rangle_{H_2} \quad (\text{C.17})$$

$$\otimes \frac{1}{\sqrt{3^N}} \sum_{f: \{0, 1\}^n \rightarrow \{0, 1, 2\}} \omega_3^{\sum_{(x, y) \in L} f(x) - \sum_{(x', y') \in R} f(x')} |f\rangle_F. \quad (\text{C.18})$$

Here, $\delta_{h_1, L \cup R}$ is an indicator variable that equals 1 if $y_{<} = (x_{<} \oplus h_1(x_{>}))$ for all $(x, y) \in L \cup R$, and 0 otherwise; $\delta'_{h_2, L \cup R}$ equals 1 if $(y_{>} \oplus h_2(y_{<})) = x_{>}$ for all $(x, y) \in L \cup R$, and 0 otherwise.

C.3 Projecting onto the local distinct subspace

Our analysis of the LRFC ensemble centers upon a projection onto the *local distinct subspace* on the registers L and R . In this section, we first define this subspace and then show that we can project onto this subspace (and close variants of it) throughout any quantum experiment that queries a Haar-random unitary or the LRFC ensemble. These latter steps form the core technical results behind our proof that the LRFC ensemble is indistinguishable from a Haar-random unitary.

We define the local distinct subspace as follows.

Definition 41. Let $\mathcal{R}^{2, \text{lcdist}}$ be the set of all ordered pairs of relations $(L, R) \in \mathcal{R}^2$ where $L \cup R = \{(x_1, y_1), \dots, (x_t, y_t)\}$ satisfies $x_{1, >}, \dots, x_{t, >}$ are all distinct and $y_{1, <}, \dots, y_{t, <}$ are all distinct.

The states $|\text{lrf}_{L,R}\rangle$ possess several nice properties when L and R are locally distinct. For example, by expanding the definition of $|\text{lrf}_{L,R}\rangle$, we obtain the following facts.

Fact 3 (Orthonormality). $\{|\text{lrf}_{L,R}\rangle\}_{(L,R) \in \mathcal{R}^{2, \text{lcdist}}}$ forms an orthonormal set of vectors.

Fact 4 (Action of lrfo). For any $(L, R) \in \mathcal{R}^{2, \text{lcdist}}$ and $x \in [N]$ such that $x_{>} \notin \text{Dom}_{>}(L \cup R)$,

$$\text{lrfo} |x\rangle_A |\text{lrf}_{L,R}\rangle_{H_1 H_2 F} = \frac{1}{\sqrt{N}} \sum_{y \in [N]} |y\rangle_A |\text{lrf}_{L \cup \{(x, y)\}, R}\rangle_{H_1 H_2 F}, \quad (\text{C.19})$$

$$\text{lrfo}^* |x\rangle_A |\text{lr}_{L,R}\rangle_{H_1 H_2 F} = \frac{1}{\sqrt{N}} \sum_{y \in [N]} |y\rangle_A |\text{lr}_{L, R \cup \{(x,y)\}}\rangle_{H_1 H_2 F}. \quad (\text{C.20})$$

Similarly, for any $(L, R) \in \mathcal{R}^{2, \text{ldist}}$ and $y \in [N]$ such that $y_< \notin \text{Im}_<(L \cup R)$,

$$\text{lrfo}^\dagger |y\rangle_A |\text{lr}_{L,R}\rangle_{H_1 H_2 F} = \frac{1}{\sqrt{N}} \sum_{x \in [N]} |x\rangle_A |\text{lr}_{L, R \cup \{(x,y)\}}\rangle_{H_1 H_2 F}, \quad (\text{C.21})$$

$$\text{lrfo}^T |y\rangle_A |\text{lr}_{L,R}\rangle_{H_1 H_2 F} = \frac{1}{\sqrt{N}} \sum_{x \in [N]} |x\rangle_A |\text{lr}_{L \cup \{(x,y)\}, R}\rangle_{H_1 H_2 F}. \quad (\text{C.22})$$

We can also define a partial isometry between the states $|\text{lr}_{L,R}\rangle$, and the states $|L\rangle \otimes |R\rangle$, when L and R are locally distinct.

Definition 42. Define the partial isometry $\text{Compress}_{\text{LRF}} : \mathcal{H}_{H_1} \otimes \mathcal{H}_{H_2} \otimes \mathcal{H}_F \rightarrow \mathcal{H}_L \otimes \mathcal{H}_R$ to be

$$\text{Compress}_{\text{LRF}} := \sum_{(L,R) \in \mathcal{R}^{2, \text{ldist}}} |L\rangle_L \otimes |R\rangle_R \cdot \langle \text{lr}_{L,R} |_{H_1 H_2 F}. \quad (\text{C.23})$$

Note that Compress is a partial isometry by Fact 3.

For our later analysis, it will be convenient to define projectors that keep one in the locally distinct subspace. We do so as follows. First, we recall the definition of the projector onto *bijective* relation states,

$$\Pi_{\text{LR}}^{\text{bij}} |L\rangle_L |R\rangle_R = \begin{cases} |L\rangle_L |R\rangle_R, & \text{if } \text{Dom}(L \cup R) \in \text{distinct}, \\ & \text{and } \text{Im}(L \cup R) \in \text{distinct} \\ 0, & \text{else.} \end{cases} \quad (\text{C.24})$$

In a similar fashion, we define the not-in-domain projector on ALR as,

$$\Pi_{\text{ALR}}^{\notin \text{Dom}} |x\rangle_A |L\rangle_L |R\rangle_R = \begin{cases} |x\rangle_A |L\rangle_L |R\rangle_R, & \text{if } x \notin \text{Dom}(L \cup R), \\ 0, & \text{else,} \end{cases} \quad (\text{C.25})$$

and the not-in-image projector as,

$$\Pi_{\text{ALR}}^{\notin \text{Im}} |y\rangle_A |L\rangle_L |R\rangle_R = \begin{cases} |y\rangle_A |L\rangle_L |R\rangle_R, & \text{if } y \notin \text{Im}(L \cup R), \\ 0, & \text{else.} \end{cases} \quad (\text{C.26})$$

Turning to the local distinct projectors, we define the *locally bijective* relation states via the projector,

$$\Pi_{\text{LR}}^{\text{locbij}} |L\rangle_L |R\rangle_R = \begin{cases} |L\rangle_L |R\rangle_R, & \text{if } \text{Dom}_>(L \cup R) \in \text{distinct}, \\ & \text{and } \text{Im}_<(L \cup R) \in \text{distinct} \\ 0, & \text{else,} \end{cases} \quad (\text{C.27})$$

and the not-in-local-domain and not-in-local-image projectors as,

$$\Pi_{\text{ALR}}^{\notin \text{locDom}} |x\rangle_A |L\rangle_L |R\rangle_R = \begin{cases} |x\rangle_A |L\rangle_L |R\rangle_R, & \text{if } x_> \notin \text{Dom}_>(L \cup R), \\ 0, & \text{else,} \end{cases} \quad (\text{C.28})$$

$$\Pi_{\text{ALR}}^{\notin \text{locIm}} |y\rangle_A |L\rangle_L |R\rangle_R = \begin{cases} |y\rangle_A |L\rangle_L |R\rangle_R, & \text{if } y_< \notin \text{Im}_<(L \cup R), \\ 0, & \text{else.} \end{cases} \quad (\text{C.29})$$

We also let,

$$\Pi_{\text{ALR}}^{\notin \text{Dom} \rightarrow \notin \text{locDom}} = 1 - \Pi_{\text{ALR}}^{\notin \text{Dom}} + \Pi_{\text{ALR}}^{\notin \text{locDom}} \quad (\text{C.30})$$

$$\Pi_{\text{ALR}}^{\notin \text{Im} \rightarrow \notin \text{locIm}} = 1 - \Pi_{\text{ALR}}^{\notin \text{Im}} + \Pi_{\text{ALR}}^{\notin \text{locIm}}, \quad (\text{C.31})$$

denote projectors which do nothing if $x \in \text{Dom}(L \cup R)$, and project to the not-in-local-domain subspace if $x \notin \text{Dom}(L \cup R)$ (and similar for Im).

C.3.1 Twirled W is indistinguishable from twirled projected W

In this and the following two sections, we use the local distinct subspace projectors can be inserted, up to small error, throughout any quantum experiment that queries the LRFC ensemble or a Haar-random unitary. We begin in this section by analyzing the insertion of the local distinct subspace projectors for experiments that involve the path-recording oracles W and $\bar{W}$.

We define projected versions of the path-recording oracles W and $\bar{W}$ as follows,

$$W' \equiv \Pi^{\text{locbij}} \cdot W \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \cdot \Pi^{\text{locbij}} \quad (\text{C.32})$$

$$(W^\dagger)' \equiv \Pi^{\text{locbij}} \cdot W^\dagger \cdot \Pi^{\notin \text{Im} \rightarrow \notin \text{locIm}} \cdot \Pi^{\text{locbij}} \quad (\text{C.33})$$

$$\bar{W}' \equiv \Pi^{\text{locbij}} \cdot \bar{W} \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \cdot \Pi^{\text{locbij}} \quad (\text{C.34})$$

$$(\bar{W}^\dagger)' \equiv \Pi^{\text{locbij}} \cdot \bar{W}^\dagger \cdot \Pi^{\notin \text{Im} \rightarrow \notin \text{locIm}} \cdot \Pi^{\text{locbij}}. \quad (\text{C.35})$$

In the remainder of this section, we show that the projected oracles are indistinguishable from the original oracles whenever the oracles are surrounded by random unitary 2-designs.

Lemma 27 (Twirled W is indistinguishable from twirled W'). *Let $\mathfrak{D}$ be any strong approximate unitary 2-design with additive error ε . For any t -query oracle adversary $\mathcal{A}$, we have*

$$\text{TD} \left(|\mathcal{A}_t^{W, \mathfrak{D}} \rangle \langle \mathcal{A}_t^{W, \mathfrak{D}}|_{\text{ALRCD}}, |\mathcal{A}_t^{W', \mathfrak{D}} \rangle \langle \mathcal{A}_t^{W', \mathfrak{D}}|_{\text{ALRCD}} \right) \leq \frac{\sqrt{70}t(t-1)}{N^{1/8}} + \frac{2t(t+1)}{N^{1/4}} + 4t^{5/4}\varepsilon^{1/4}. \quad (\text{C.36})$$

Here and in the remainder of the manuscript, we abbreviate $|\mathcal{A}_t^{W, \bar{W}, \mathfrak{D}} \rangle$ as simply $|\mathcal{A}_t^{W, \mathfrak{D}} \rangle$. All of our analysis includes queries to the conjugate and transpose.

Proof. Let TD_t denote the trace distance in Eq. (C.36). We will prove the theorem by induction. The statement holds trivially at $t = 0$. To prove the inductive step, suppose that the Eq. (C.36) holds up to time $t - 1$ for any $t \geq 1$. Without loss of generality, we assume that the oracle W is applied at time t . The case when $W^\dagger$, $\bar{W}$, and $\bar{W}^\dagger$ are applied follow by symmetric arguments. The states at time t are obtained from the states at time $t - 1$ as follows,

$$|\mathcal{A}_t^{W, \mathfrak{D}} \rangle = \text{cD} \cdot W \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{W, \mathfrak{D}} \rangle \quad (\text{C.37})$$

$$|\mathcal{A}_t^{W', \mathfrak{D}} \rangle = \text{cD} \cdot \Pi^{\text{locbij}} \cdot W \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{W', \mathfrak{D}} \rangle \quad (\text{C.38})$$

In the second line, we use that $\Pi^{\text{locbij}} |\mathcal{A}_{t-1}^{W', \mathfrak{D}} \rangle = |\mathcal{A}_{t-1}^{W', \mathfrak{D}} \rangle$ to eliminate the final projector in W' . This follows because the projector Π^{locbij} has already been applied after the prior $(t-1)$ -th query. We have

$$\begin{aligned} \text{TD}_t &\leq \text{TD}_{t-1} + 2 \left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot \text{cC} \cdot A_t |\mathcal{A}_{t-1}^{W, \mathfrak{D}} \rangle \right\|_2 \\ &\quad + 2 \left\| (1 - \Pi^{\text{locbij}}) \cdot W \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{W', \mathfrak{D}} \rangle \right\|_2, \end{aligned} \quad (\text{C.39})$$

where the first term accounts for the error up to time $t - 1$, the second term for the error induced by the projector $\Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}$ [using Eq. (B.18)], and the third term for the error induced by the projector Π^{locbij} [again using Eq. (B.18)].

We bound the second term as follows. From Eq. (9.55) and Claim 18 of Ref. [42] (see also the modification of Claim 18 to strong approximate designs in the proof of Lemma 25), we have

$$\left\| |\mathcal{A}_{t-1}^{W, \mathfrak{D}}\rangle - \mathbf{cQ} \cdot |\mathcal{A}_{t-1}^V\rangle \right\|_2 \leq \frac{\sqrt{70}(t-1)}{N^{1/8}} + 2t^{1/4}\varepsilon^{1/4}. \quad (\text{C.40})$$

This yields,

$$\begin{aligned} & \left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot \mathbf{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{W, \mathfrak{D}}\rangle \right\|_2 \\ & \leq \left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot \mathbf{cC} \cdot A_t \cdot \mathbf{cQ} \cdot |\mathcal{A}_{t-1}^V\rangle \right\|_2 + \frac{\sqrt{70}(t-1)}{N^{1/8}} + 2t^{1/4}\varepsilon^{1/4}. \end{aligned} \quad (\text{C.41})$$

The latter state norm can be written out explicitly, as

$$\begin{aligned} & \left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot \mathbf{cC} \cdot A_t \cdot \mathbf{cQ} \cdot |\mathcal{A}_{t-1}^V\rangle \right\|_2 \\ & = \sqrt{\langle \mathcal{A}_{t-1}^V | \cdot A_t^\dagger \cdot \mathbf{cQ}^\dagger \cdot \mathbf{cC}^\dagger \cdot (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot \mathbf{cC} \cdot \mathbf{cQ} \cdot A_t \cdot |\mathcal{A}_{t-1}^V \rangle}. \end{aligned} \quad (\text{C.42})$$

where we used that A_t and $\mathbf{cQ}$ act on distinct registers to commute them past one another.

To proceed, we first apply the operator inequality,

$$1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \preceq \sum_{\ell} \sum_{i \in [\ell]} \Pi_{A > L_{X_{>,i}}^{(\ell)}}^{\text{eq}} \Pi_{A < L_{X_{<,i}}^{(\ell)}}^{\text{neq}} + \sum_r \sum_{j \in [r]} \Pi_{A > R_{X_{>,j}}^{(r)}}^{\text{eq}} \Pi_{A < R_{X_{<,j}}^{(r)}}^{\text{neq}}, \quad (\text{C.43})$$

where $\Pi_{A > L_{X_{>,i}}^{(\ell)}}^{\text{eq}}$ projects onto states with the same bitstring on $A_{>}$ as on $L_{X_{>,i}}^{(\ell)}$, and

$$\Pi_{A < L_{X_{<,i}}^{(\ell)}}^{\text{neq}} \equiv 1 - \Pi_{A < L_{X_{<,i}}^{(\ell)}}^{\text{eq}} \quad (\text{C.44})$$

does the reverse on $<$. For each individual term with $i \in [\ell]$, we have

$$\begin{aligned} & \langle \mathcal{A}_{t-1}^V | \cdot A_t^\dagger \cdot \mathbf{cQ}_{\text{CDLR}}^\dagger \cdot \mathbf{cC}_{\text{CA}}^\dagger \cdot \Pi_{A > L_{X_{>,i}}^{(\ell)}}^{\text{eq}} \Pi_{A < L_{X_{<,i}}^{(\ell)}}^{\text{neq}} \cdot \mathbf{cC}_{\text{CA}} \cdot \mathbf{cQ}_{\text{CDLR}} \cdot A_t \cdot |\mathcal{A}_t^V \rangle \\ & = \langle \mathcal{A}_{t-1}^V | \cdot A_t^\dagger \cdot \mathbf{cC}_{\text{CL}_{X_{<,i}}^{(\ell)}}^\dagger \cdot \mathbf{cC}_{\text{CA}}^\dagger \cdot \Pi_{A > L_{X_{>,i}}^{(\ell)}}^{\text{eq}} \Pi_{A < L_{X_{<,i}}^{(\ell)}}^{\text{neq}} \cdot \mathbf{cC}_{\text{CA}} \cdot \mathbf{cC}_{\text{CL}_{X_{<,i}}^{(\ell)}} \cdot A_t \cdot |\mathcal{A}_{t-1}^V \rangle, \end{aligned} \quad (\text{C.45})$$

where all but one of the Clifford unitaries in $\mathbf{cQ}$ cancel, since the middle term in the expectation value acts only on register $L_{X_{>,i}}$. For terms with $j \in [r]$, we have instead

$$\begin{aligned} & \langle \mathcal{A}_{t-1}^V | \cdot A_t^\dagger \cdot \mathbf{cQ}_{\text{CDLR}}^\dagger \cdot \mathbf{cC}_{\text{CA}}^\dagger \cdot \Pi_{A > R_{X_{>,j}}^{(r)}}^{\text{eq}} \Pi_{A < R_{X_{<,j}}^{(r)}}^{\text{neq}} \cdot \mathbf{cC}_{\text{CA}} \cdot \mathbf{cQ}_{\text{CDLR}} \cdot A_t \cdot |\mathcal{A}_{t-1}^V \rangle \\ & = \langle \mathcal{A}_{t-1}^V | \cdot A_t^\dagger \cdot \mathbf{cC}_{\text{CR}_{X_{<,j}}^{(r)}}^\dagger \cdot \mathbf{cC}_{\text{CA}}^\dagger \cdot \Pi_{A > R_{X_{>,j}}^{(r)}}^{\text{eq}} \Pi_{A < R_{X_{<,j}}^{(r)}}^{\text{neq}} \cdot \mathbf{cC}_{\text{CA}} \cdot \mathbf{cC}_{\text{CR}_{X_{<,j}}^{(r)}} \cdot A_t \cdot |\mathcal{A}_{t-1}^V \rangle. \end{aligned} \quad (\text{C.46})$$

We can upper bound the latter expectation values by performing the twirl over C . From Eq. (B.23) and Eq. (B.24), this yields an upper bound of $1/N^{1/2} + \varepsilon$ on both Eq. (C.45) and Eq. (C.46). Therefore, in total, we have an upper bound

$$\left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot \mathbf{cC} \cdot A_t \cdot \mathbf{cQ} \cdot |\mathcal{A}_{t-1}^V\rangle \right\|_2 \leq \sqrt{(\ell + r)^2(1/N^{1/2} + \varepsilon)} \leq t/N^{1/4} + t\varepsilon^{1/2}. \quad (\text{C.47})$$

The third term in Eq. (C.39) is simpler to bound. The input state to W lies in the subspace $\Pi_{\leq t}^{\text{locbij}}$ by construction. Therefore, the output of W lies in the subspace $\Pi^{\mathcal{I}(W\Pi_{\leq t}^{\text{locbij}})}$. This latter subspace is spanned by two classes of states. The first class is,

$$|y\rangle_A |L\rangle_L |R\rangle_R, \quad (\text{C.48})$$

for any $\ell + r \leq t$, where $\text{Dom}_>(L \cup R)$ is distinct, $\text{Im}_<(L \cup R)$ is distinct, and $y_< \notin \text{Im}_<(L \cup R)$. These arise if the $W^{R,\dagger}$ branch of W is applied. The second class is,

$$\frac{1}{\sqrt{N - \ell - r}} \sum_{y \notin \text{Im}(L \cup R)} |y\rangle_A |L \cup (x, y)\rangle_L |R\rangle_R, \quad (\text{C.49})$$

for $\ell + r \leq t$, where $\text{Dom}_>(L \cup R)$ is distinct, $\text{Im}_<(L \cup R)$ is distinct, and $x_> \notin \text{Dom}_>(L \cup R)$. These arise if the W^L branch of W is applied. The states above are mutually orthogonal to one another as well as between different ℓ, r .

The first class of states is invariant under Π^{locbij} . Thus, the projector Π^{locbij} acts trivially and incurs no error. Meanwhile, on the second class of states, we have

$$\begin{aligned} \Pi^{\text{locbij}} \frac{1}{\sqrt{N - \ell - r}} \sum_{y \notin \text{Im}(L \cup R)} |y\rangle_A |L \cup (x, y)\rangle_L |R\rangle_R \\ = \frac{1}{\sqrt{N - \ell - r}} \sum_{y_< \notin \text{Im}_<(L \cup R)} |y\rangle_A |L \cup (x, y)\rangle_L |R\rangle_R. \end{aligned} \quad (\text{C.50})$$

The final state is orthogonal to the first class of states, as well as between different ℓ, r . The state has norm $(N^{1/2}(N^{1/2} - \ell - r))/(N - \ell - r) \geq 1 - t/N^{1/2}$. The above analysis establishes that $\Pi^{\text{locbij}} \Pi^{\mathcal{I}(W\Pi_{\leq t}^{\text{locbij}})}$ is block diagonal between the two classes of input and output states, as well as between different ℓ, r . Therefore, the desired error is given by the maximum error within each block. From the above, the maximum is achieved at $\ell + r = t$, which yields,

$$\left\| (1 - \Pi^{\text{locbij}}) \cdot W \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{\overline{W}, \mathcal{D}}\rangle \right\|_2 \leq \sqrt{t/N^{1/2}}. \quad (\text{C.51})$$

In total, we have shown that the error in Eq. (C.39) is upper bounded by,

$$\text{TD}_t \leq \text{TD}_{t-1} + \frac{2\sqrt{70}(t-1)}{N^{1/8}} + 4t^{1/4}\varepsilon^{1/4} + 2t/N^{1/4} + 2\sqrt{t/N^{1/2}} \leq \frac{\sqrt{70}t(t-1)}{N^{1/8}} + 4t^{5/4}\varepsilon^{1/4} + \frac{2t(t+1)}{N^{1/4}},$$

applying the inductive hypothesis. This completes our proof. $\square$

C.3.2 Projected W is indistinguishable from projected lrfO

We will now show that the path-recording oracle W and the LRF oracle lrfO are equal on the locally distinct subspace. To show this, let us adopt the general notation,

$$\tilde{\Pi} \equiv \text{Compress}_{\text{LRF}}^\dagger \cdot \Pi \cdot \text{Compress}_{\text{LRF}} \quad (\text{C.52})$$

for any projector Π on ALR. We will also let $\tilde{\Pi}^{\mathcal{I}(\text{lrfO}\Pi^{\notin \text{locDom}}\Pi^{\text{locbij}})}$ denote the projector onto the subspace spanned by states of the form Eq. (C.19), $\tilde{\Pi}^{\mathcal{I}(\text{lrfO}^* \Pi^{\notin \text{locDom}}\Pi^{\text{locbij}})}$ analogously for Eq. (C.20), $\tilde{\Pi}^{\mathcal{I}(\text{lrfO}^\dagger \Pi^{\notin \text{locIm}}\Pi^{\text{locbij}})}$ for Eq. (C.21), and $\tilde{\Pi}^{\mathcal{I}(\text{lrfO}^T \Pi^{\notin \text{locIm}}\Pi^{\text{locbij}})}$ for Eq. (C.22). As indicated in the notation, these project onto the image of the lrfO oracles when they are applied to locally distinct states.

Leveraging these projectors, we can define projected versions of the lrfo oracle as follows,

$$\text{lrfo}' \equiv \tilde{\Pi}^{\text{locbij}} \cdot \text{lrfo} \cdot \left(\tilde{\Pi}^{\notin \text{locDom}} + \tilde{\Pi}^{\mathcal{I}(\text{lrfo}^\dagger \Pi^{\notin \text{locIm}} \Pi^{\text{locbij}})} \cdot \tilde{\Pi}^{\mathcal{D}(W_R^\dagger)} \right) \cdot \tilde{\Pi}^{\text{locbij}} \quad (\text{C.53})$$

$$(\text{lrfo}^\dagger)' \equiv \tilde{\Pi}^{\text{locbij}} \cdot \text{lrfo}^\dagger \cdot \left(\tilde{\Pi}^{\notin \text{locIm}} + \tilde{\Pi}^{\mathcal{D}(\text{lrfo} \Pi^{\notin \text{locDom}} \Pi^{\text{locbij}})} \cdot \tilde{\Pi}^{\mathcal{D}(W_L^\dagger)} \right) \cdot \tilde{\Pi}^{\text{locbij}} \quad (\text{C.54})$$

$$(\text{lrfo}^*)' \equiv \tilde{\Pi}^{\text{locbij}} \cdot \text{lrfo}^* \cdot \left(\tilde{\Pi}^{\notin \text{locDom}} + \tilde{\Pi}^{\mathcal{I}(\text{lrfo}^T \Pi^{\notin \text{locIm}} \Pi^{\text{locbij}})} \cdot \tilde{\Pi}^{\mathcal{D}(\bar{W}_R^\dagger)} \right) \cdot \tilde{\Pi}^{\text{locbij}} \quad (\text{C.55})$$

$$(\text{lrfo}^T)' \equiv \tilde{\Pi}^{\text{locbij}} \cdot \text{lrfo}^T \cdot \left(\tilde{\Pi}^{\notin \text{locIm}} + \tilde{\Pi}^{\mathcal{D}(\text{lrfo}^* \Pi^{\notin \text{locDom}} \Pi^{\text{locbij}})} \cdot \tilde{\Pi}^{\mathcal{D}(\bar{W}_L^\dagger)} \right) \cdot \tilde{\Pi}^{\text{locbij}}. \quad (\text{C.56})$$

The first key result of this section is that W' and lrfo' are nearly equal up to the compress isometry.

Lemma 28 (W' and lrfo' are nearly equal up to isometry). *We have*

$$\left\| \Pi_{\leq t} \left(W' - \text{Compress}_{\text{LRF}} \cdot \text{lrfo}' \cdot \text{Compress}_{\text{LRF}}^\dagger \right) \Pi_{\leq t} \right\|_\infty \leq t/N, \quad (\text{C.57})$$

$$\left\| \Pi_{\leq t} \left((W^\dagger)' - \text{Compress}_{\text{LRF}} \cdot (\text{lrfo}^\dagger)' \cdot \text{Compress}_{\text{LRF}}^\dagger \right) \Pi_{\leq t} \right\|_\infty \leq t/N \quad (\text{C.58})$$

$$\left\| \Pi_{\leq t} \left(\bar{W}' - \text{Compress}_{\text{LRF}} \cdot (\text{lrfo}^*)' \cdot \text{Compress}_{\text{LRF}}^\dagger \right) \Pi_{\leq t} \right\|_\infty \leq t/N \quad (\text{C.59})$$

$$\left\| \Pi_{\leq t} \left((\bar{W}^\dagger)' - \text{Compress}_{\text{LRF}} \cdot (\text{lrfo}^T)' \cdot \text{Compress}_{\text{LRF}}^\dagger \right) \Pi_{\leq t} \right\|_\infty \leq t/N. \quad (\text{C.60})$$

Proof. We focus on the first equality without loss of generality. The remaining three equalities following by symmetric arguments. The W' and lrfo' oracles act on states in two domains, corresponding to the two terms in parentheses in Eq. (C.53). The first is the domain of $\tilde{\Pi}^{\notin \text{locDom}} \tilde{\Pi}^{\text{locbij}}$. For states in this domain, lrfo' acts as

$$\text{lrfo}' |x\rangle_A |\text{rf}_{L,R}\rangle_{\text{H}_1\text{H}_2\text{F}} = \frac{1}{\sqrt{N}} \sum_{y \in [N]} \delta_{y < \notin \text{Im}_{<}(L \cup R)} |y\rangle_A |\text{rf}_{L \cup \{(x,y)\}, R}\rangle_{\text{H}_1\text{H}_2\text{F}}, \quad (\text{C.61})$$

where $(L, R) \in \mathcal{R}^{2, \text{ldist}}$ and $x > \notin \text{Dom}_{>}(L \cup R)$. Meanwhile, on the un-compressed versions of the same states, W' acts as

$$W' |x\rangle_A |L\rangle_L |R\rangle_L = \frac{1}{\sqrt{N - \ell - r}} \sum_{y \notin \text{Im}(L \cup R)} \delta_{y < \notin \text{Im}_{<}(L \cup R)} |y\rangle_A |L \cup \{(x,y)\}\rangle_L |R\rangle_R, \quad (\text{C.62})$$

After compression by $\text{Compress}_{\text{LRF}}$, the actions of the two oracles are identical aside from a normalization ratio of $\sqrt{1 - (\ell + r)/N}$.

The second is the domain of $\tilde{\Pi}^{\mathcal{D}(W_R^\dagger)} \tilde{\Pi}^{\text{locbij}}$. This domain is spanned by states of the form,

$$\sum_{x \notin \text{Dom}(L \cup R)} \delta_{x > \notin \text{Dom}_{>}(L \cup R)} |x\rangle_A |\text{rf}_{L, R \cup \{(x,y)\}}\rangle_{\text{H}_1\text{H}_2\text{F}}, \quad (\text{C.63})$$

where $(L, R) \in \mathcal{R}^{2, \text{ldist}}$ and $y < \notin \text{Im}_{<}(L \cup R)$, and we leave the state un-normalized for brevity. For states in this domain, lrfo' acts as

$$\text{lrfo}' \sum_{x \notin \text{Dom}(L \cup R)} \delta_{x > \notin \text{Dom}_{>}(L \cup R)} |x\rangle_A |\text{rf}_{L, R \cup \{(x,y)\}}\rangle_{\text{H}_1\text{H}_2\text{F}} \quad (\text{C.64})$$

$$= N^{1/2} \frac{N - \ell - r}{N} \frac{N^{1/2} (N^{1/2} - \ell - r)}{N - \ell - r} |y\rangle_A |\text{rf}_{L,R}\rangle_{\text{H}_1\text{H}_2\text{F}}, \quad (\text{C.65})$$

where the second ratio arises from the action of $\tilde{\Pi}^{\mathcal{D}(W_R^\dagger)}$, the first ratio arises from the action of $\tilde{\Pi}^{\mathcal{I}(\text{lrfo}^\dagger \Pi^{\notin \text{loc} \text{lm}} \Pi^{\text{loc} \text{bij}})}$, and then factor of $N^{1/2}$ arises from applying Eq. (C.21). Meanwhile, on the un-compressed versions of the same states, W' acts as

$$W' \sum_{x \notin \text{Dom}(L \cup R)} \delta_{x > \text{Dom}_>(L \cup R)} |x\rangle_A |L\rangle_L |R \cup \{(x, y)\}\rangle_R \quad (\text{C.66})$$

$$= (N - \ell - r)^{1/2} \frac{N^{1/2}(N^{1/2} - \ell - r)}{N - \ell - r} |y\rangle_A |L\rangle_L |R\rangle_R, \quad (\text{C.67})$$

After compression by $\text{Compress}_{\text{LFR}}$, the actions of the two oracles are identical aside from a normalization ratio of $\sqrt{1 - (\ell + r)/N}$.

The W' and lrfo' oracles are block-diagonal between different values of ℓ, r . Hence, the spectral norm of the difference between the two operators (after compressing lrfo') is bounded by the maximum spectral norm of the difference for each ℓ, r . From the above analysis, the two oracles are related by a constant re-scaling $\sqrt{1 - (\ell + r)/N} \geq 1 - (\ell + r)/N$ within each ℓ, r . Hence, the spectral norm of their difference is at most $(\ell + r)/N$. Applying $\ell + r \leq t$ completes the proof. $\square$

Using Lemma 28, we can then show that W' is indistinguishable from lrfo' by any adversary.

Lemma 29 (W' is indistinguishable from lrfo'). *For any t -query oracle adversary $\mathcal{A}$, we have*

$$\left\| \text{Tr}_{\text{LRCD}} (|\mathcal{A}_t^{W', \mathfrak{D}}\rangle \langle \mathcal{A}_t^{W', \mathfrak{D}}|_{\text{ABLRCD}}) - \text{Tr}_{\text{H}_1 \text{H}_2 \text{FCD}} (|\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}\rangle \langle \mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}|_{\text{ABH}_1 \text{H}_2 \text{FCD}}) \right\|_1 \leq \frac{t(t+1)}{2N}. \quad (\text{C.68})$$

Proof. From Lemma 28, every application of W' in $|\mathcal{A}_t^{W', \mathfrak{D}}\rangle$ can be replaced by an application of $\text{Compress}_{\text{LFR}} \cdot \text{lrfo}' \cdot \text{Compress}_{\text{LFR}}^\dagger$ up to total trace norm error $\sum_{s=1}^t s/N = t(t+1)/2N$. Since the $\text{Compress}_{\text{LFR}}^\dagger$ operations act only the L and R registers, they commute with all other objects in $|\mathcal{A}_t^{W', \mathfrak{D}}\rangle$ (namely, cC and cD and A_s). This implies that all compress operations between adjacent applications of the lrfo oracle cancel one another, leaving only a first application of $\text{Compress}_{\text{LFR}}^\dagger$ before the first query to lrfo and a last application of $\text{Compress}_{\text{LFR}}$ following the t -th application. The first application acts trivially because L and R are empty in the initial state. The final application has no effect since L and R are traced out in the final state. Hence, all applications of $\text{Compress}_{\text{LFR}}$ and $\text{Compress}_{\text{LFR}}^\dagger$ vanish which yields the state $|\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}\rangle$. $\square$

C.3.3 Twirled projected lrfo is indistinguishable from twirled lrfo

Finally, we can leverage our results thus far to show that the projected oracle lrfo' is indistinguishable from the original oracle lrfo by any adversary.

Lemma 30 (Twirled lrfo' is indistinguishable from twirled lrfo). *Let $\mathfrak{D}$ be any strong approximate unitary 2-design with additive error ε . For any t -query oracle adversary $\mathcal{A}$, we have*

$$\left\| |\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}\rangle \langle \mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}| - |\mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}\rangle \langle \mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}| \right\|_1 = \mathcal{O}(t^2/N^{1/16}) + \mathcal{O}(t^{5/8}\varepsilon^{1/8}).$$

Proof. Let us rewrite the projected oracle as follows,

$$\text{lrfo}' \equiv \tilde{\Pi}^{\text{loc} \text{bij}} \cdot \text{lrfo} \cdot \left(\tilde{\Pi}^{\notin \text{loc} \text{Dom}} + \tilde{\Pi}^{\mathcal{I}(\text{lrfo}^\dagger \Pi^{\notin \text{loc} \text{lm}} \Pi^{\text{loc} \text{bij}})} \right) \cdot \left(\tilde{\Pi}^{\notin \text{loc} \text{Dom}} + \tilde{\Pi}^{\mathcal{D}(W_R^\dagger)} \right) \cdot \tilde{\Pi}^{\text{loc} \text{bij}},$$

and similar for $(\text{lrfo}^\dagger)'$, $(\text{lrfo}^*)'$, and $(\text{lrfo}^T)'$. This decomposition follows from the original definition because $\tilde{\Pi}^{\notin \text{loc} \text{Dom}}$ acts on an orthogonal subspace to $\tilde{\Pi}^{\mathcal{I}(\text{lrfo}^\dagger \Pi^{\notin \text{loc} \text{lm}} \Pi^{\text{loc} \text{bij}})}$ and $\tilde{\Pi}^{\mathcal{D}(W_R^\dagger)}$. This fact also

implies that each sum in parentheses above is a projector. Hence, lrfo' is equal to the product of lrfo and four projectors.

From Eq. (B.18) and the sequential gentle measurement lemma (Lemma 10), the trace distance of interest is upper bounded as,

$$\left\| |\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}\rangle\langle\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}| - |\mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}\rangle\langle\mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}| \right\|_1 \leq 2 \left\| |\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}\rangle - |\mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}\rangle \right\|_2 \leq 8t \sqrt{1 - \langle\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}|\mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}\rangle}.$$

To bound the normalization on the right hand side, we apply Lemma 29 and Lemma 27 and Lemma 25 and Theorem 10 to find

$$\left| \langle\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}|\mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}\rangle - \mathbb{E}_{U \sim H} \langle\mathcal{A}_t^{U, \mathfrak{D}}|\mathcal{A}_t^{U, \mathfrak{D}}\rangle \right| \leq \frac{t(t+1)}{2N} + \frac{\sqrt{70}t(t-1)}{N^{1/8}} + \frac{2t(t+1)}{N^{1/4}} + \frac{9t(t+2)}{N^{1/8}} + 8t^{5/4}\varepsilon^{1/4}.$$

We have $\langle\mathcal{A}_t^{U, \mathfrak{D}}|\mathcal{A}_t^{U, \mathfrak{D}}\rangle = 1$ since U is unitary. Hence, the trace distance is bounded above by $8t$ multiplied by the square root of the right hand side of the above equation. The right hand side is $\mathcal{O}(t^2/N^{1/8}) + \mathcal{O}(t^{5/4}\varepsilon^{1/4})$. Hence, the trace distance is $\mathcal{O}(t^2/N^{1/16}) + \mathcal{O}(t^{5/8}\varepsilon^{1/8})$ as claimed. $\square$

C.4 LRFC is indistinguishable from a Haar-random unitary

We now prove our main result, that the LRFC ensemble is indistinguishable from a Haar-random unitary. This follows relatively quickly from the results in the previous sections.

Theorem 11 (LRFC is indistinguishable from Haar-random). *Let $\mathfrak{D}$ be any strong approximate unitary 2-design with additive error ε . For any t -query oracle adversary $\mathcal{A}$, we have*

$$\left\| \mathbb{E}_{U \sim \text{LRFC}} (|\mathcal{A}_t^U\rangle\langle\mathcal{A}_t^U|) - \mathbb{E}_{U \sim H} (|\mathcal{A}_t^U\rangle\langle\mathcal{A}_t^U|) \right\|_1 = \mathcal{O}(t^2/N^{1/16}) + \mathcal{O}(t^{5/8}\varepsilon^{1/8}).$$

Proof. Our proof follows from the results in the preceding subsections in four steps. At each step, we bound the trace distance between two density matrices. The density matrices are,

$$\rho^{(0)} = \mathbb{E}_{U \sim H} (|\mathcal{A}_t^U\rangle\langle\mathcal{A}_t^U|_{\text{AB}}) \quad (\text{C.69})$$

$$\rho^{(1)} = \text{Tr}_{\text{LRCD}} (|\mathcal{A}_t^{W, \mathfrak{D}}\rangle\langle\mathcal{A}_t^{W, \mathfrak{D}}|_{\text{ABLRCD}}) \quad (\text{C.70})$$

$$\rho^{(2)} = \text{Tr}_{\text{LRCD}} (|\mathcal{A}_t^{W', \mathfrak{D}}\rangle\langle\mathcal{A}_t^{W', \mathfrak{D}}|_{\text{ABLRCD}}) \quad (\text{C.71})$$

$$\rho^{(3)} = \text{Tr}_{\text{H}_1\text{H}_2\text{FCD}} (|\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}\rangle\langle\mathcal{A}_t^{\text{lrfo}', \mathfrak{D}}|_{\text{ABH}_1\text{H}_2\text{FCD}}) \quad (\text{C.72})$$

$$\rho^{(4)} = \mathbb{E}_{U \sim \text{LRFC}} (|\mathcal{A}_t^U\rangle\langle\mathcal{A}_t^U|_{\text{AB}}) = \text{Tr}_{\text{H}_1\text{H}_2\text{FCD}} (|\mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}\rangle\langle\mathcal{A}_t^{\text{lrfo}, \mathfrak{D}}|_{\text{ABH}_1\text{H}_2\text{FCD}}) \quad (\text{C.73})$$

The first density matrix is the expected output state of an experiment that queries a Haar-random unitary U . The last density matrix is the expected output of an experiment that queries the a random LRFC unitary. The intermediary density matrices denote the output state of experiments in which the action of each unitary is replaced with a path-recording oracle from the previous sections.

In the previous sections, we have already bounded the trace distance between each pair of density matrices. These are:

1. $\|\rho^{(0)} - \rho^{(1)}\|_1 \leq 18t(t+1)/N^{1/8}$ (Lemma 25 and Theorem 10)
2. $\|\rho^{(1)} - \rho^{(2)}\|_1 \leq \sqrt{70}t(t-1)/N^{1/8} + 2t(t+1)/N^{1/4} + 4t^{5/4}\varepsilon^{1/4}$ (Lemma 27)
3. $\|\rho^{(2)} - \rho^{(3)}\|_1 \leq t(t+1)/2N$ (Lemma 29)
4. $\|\rho^{(3)} - \rho^{(4)}\|_1 = \mathcal{O}(t^2/N^{1/16}) + \mathcal{O}(t^{5/8}\varepsilon^{1/8})$ (Lemma 30)

By the triangle inequality, the total trace distance, $\|\rho^{(0)} - \rho^{(4)}\|_1$, is less than the sum of the four distances above. This yields $\|\rho^{(0)} - \rho^{(4)}\|_1 = \mathcal{O}(t^2/N^{1/16})$ as claimed. $\square$

C.5 Proof of Theorem 3: LRFC is a strong unitary design

We let $\mathfrak{D}$ be an exact unitary 2-design [68, 100] with additive error zero. By definition, the output of any quantum experiment that queries any combination of U , $U^\dagger$, U^* , U^T up to k times is identical whether f, h_1, h_2 are $2k$ -wise independent random functions versus truly random functions. From Theorem 11, the output of any quantum experiment that queries the truly random LRFC ensemble k times is close to the output of the same experiment that queries a Haar-random unitary, up to trace distance $\mathcal{O}(k^2/N^{1/6})$ where $N = 2^n$. Hence, the $2k$ -wise independent variant of the LRFC ensemble forms an ε -approximate strong unitary k -design with $\varepsilon = \mathcal{O}(t^2/N^{1/6})$. $\square$

C.6 Proof of Theorem 4: LRFC is a strong PRU

We let $\mathfrak{D}$ be an exact unitary 2-design [68, 100] with additive error zero. By definition, no subexponential-time quantum experiment can distinguish whether f, h_1, h_2 are PRFs (with security against any subexponential-time quantum adversary) versus truly random functions. From Theorem 11, the output of any quantum experiment that queries the truly random LRFC ensemble k times is close to the output of the same experiment that queries a Haar-random unitary, up to trace distance $\mathcal{O}(k^2/N^{1/6})$ where $N = 2^n$. This is negligibly small for any k subexponential in n . Hence, the pseudorandom variant of the LRFC ensemble forms a strong PRU with security against any subexponential-time quantum adversary. $\square$

D Gluing strong random unitaries

In this section, we provide a proof of the strong gluing lemma (Lemma 1). We then apply the strong gluing lemma to prove our Theorems 5 and 6 on the scrambled two-layer circuit ensemble.

D.1 Proof of Lemma 1: Gluing strong random unitaries

Our proof is long but straightforward, and uses the path-recording framework introduced in Ref. [42]. We refer the reader to Appendices B and C for a complete introduction to this framework and key notation. In what follows, we begin in Appendix D.1.1 by introducing several new objects within the path-recording framework that will be useful in the strong gluing proof. We then provide a summary of our proof in Appendix D.1.2. Each step in the proof summary is then proven individually in the following Appendices D.1.3, D.1.4, and D.1.5. At a high-level, our proof follows a roughly similar approach to our analysis of the LRFC ensemble in Appendix C.

D.1.1 Preliminaries

In this subsection, we provide a short overview of the new notation used in our proof.

Registers. Our proof will apply the path-recording framework to the unitaries U_{abc} and $U_{bc}U_{ab}$. To each Haar-random unitary, the path-recording framework associate two ancilla registers. We denote these registers as L_{abc} and R_{abc} , L_{bc} and R_{bc} , and L_{ab} and R_{ab} , for the three unitaries in consideration. We denote the system register as $A = a \cup b \cup c$. As in Ref. [42], we also allow an arbitrary-sized physical register B , as well as ancilla registers C and D which purify the twirl over $C, D \sim \mathfrak{D}$.

The registers L_{abc} , R_{abc} , L_{bc} , R_{bc} , L_{ab} , R_{ab} contain relation states. For L_{abc} and R_{abc} , a relation state takes the form,

$$|L\rangle_{L_{abc}} = |\{(x_a^i x_b^i x_c^i, y_a^i y_b^i y_c^i) : i \in [\ell]\}\rangle_{L_{abc}} \quad (\text{D.1})$$

$$|R\rangle_{R_{abc}} = \left| \{ (x_a^j x_b^j x_c^j, y_a^j y_b^j y_c^j) : j \in [r] \} \right\rangle_{R_{abc}}, \quad (D.2)$$

where x_α^i is bitstring on subsystem $\alpha \in \{a, b, c\}$ (and similar for y_α^i , x_α^j , and y_α^j). Here, ℓ and r denote the length of the relation state registers. For L_{bc} and R_{bc} and L_{ab} and R_{ab} , we write,

$$|L_{ab}\rangle_{L_{ab}} |L_{bc}\rangle_{L_{bc}} = |\{ (x_a^i x_b^i, y_a^i y_b^i) : i \in [\ell] \}\rangle_{L_{ab}} |\{ (z_b^i x_c^i, y_b^i y_c^i) : i \in [\ell'] \}\rangle_{L_{bc}} \quad (D.3)$$

$$|R_{ab}\rangle_{R_{ab}} |R_{bc}\rangle_{R_{bc}} = |\{ (x_a^j x_b^j, y_a^j y_b^j) : j \in [r] \}\rangle_{R_{ab}} |\{ (z_b^j x_c^j, y_b^j y_c^j) : j \in [r'] \}\rangle_{R_{bc}}, \quad (D.4)$$

where $z_b^i, z_b^i, z_b^j, z_b^j$ are bitstrings on subsystem b . We use a different character, z , for these bitstrings, because they will correspond to the bitstrings that appear “between” U_{bc} and U_{ab} in $U_{bc}U_{ab}$, and will play a special role in our proof.

Projectors on L_{abc} and R_{abc} . We will often wish to restrict attention to certain subsets of the relation states. As in Appendix C, we have the projector onto bijective relation states,

$$\Pi_{L_{abc}R_{abc}}^{\text{bij}} |L\rangle_{L_{abc}} |R\rangle_{R_{abc}} = \begin{cases} |L\rangle_{L_{abc}} |R\rangle_{R_{abc}}, & \text{if } \text{Dom}(L \cup R) \in \text{distinct}, \\ & \text{and } \text{Im}(L \cup R) \in \text{distinct} \\ 0, & \text{else.} \end{cases} \quad (D.5)$$

Here, $\text{Dom}(L \cup R) = \{x_a^i x_b^i x_c^i : i \in [\ell]\} \cup \{x_a^j x_b^j x_c^j : j \in [r]\}$, and $\text{Im}(L \cup R) = \{y_a^i y_b^i y_c^i : i \in [\ell]\} \cup \{y_a^j y_b^j y_c^j : j \in [r]\}$. Identical to before, we also define the not-in-domain projector on ALR as,

$$\Pi_{\text{AL}_{abc}R_{abc}}^{\notin \text{Dom}} |x_a x_b x_c\rangle_A |L\rangle_{L_{abc}} |R\rangle_{R_{abc}} = \begin{cases} |x_a x_b x_c\rangle_A |L\rangle_{L_{abc}} |R\rangle_{R_{abc}}, & \text{if } x_a x_b x_c \notin \text{Dom}(L \cup R), \\ 0, & \text{else,} \end{cases} \quad (D.6)$$

and the not-in-image projector as,

$$\Pi_{\text{AL}_{abc}R_{abc}}^{\notin \text{Im}} |y_a y_b y_c\rangle_A |L\rangle_{L_{abc}} |R\rangle_{R_{abc}} = \begin{cases} |y_a y_b y_c\rangle_A |L\rangle_{L_{abc}} |R\rangle_{R_{abc}}, & \text{if } y_a y_b y_c \notin \text{Im}(L \cup R), \\ 0, & \text{else.} \end{cases} \quad (D.7)$$

For the strong gluing proof, we will also introduce new local variants of the above projectors. These are extremely similar to those defined in Appendix C. For this reason, we use the same notation here as in Appendix C, even though the precise definitions are slightly different. We define the *locally bijective* relation states via the projector,

$$\Pi_{L_{abc}R_{abc}}^{\text{locbij}} |L\rangle_{L_{abc}} |R\rangle_{R_{abc}} = \begin{cases} |L\rangle_{L_{abc}} |R\rangle_{R_{abc}}, & \text{if } \text{Dom}(L \cup R)_\alpha \in \text{distinct}, \forall \alpha = a, b, c \\ & \text{and } \text{Im}(L \cup R)_\alpha \in \text{distinct}, \forall \alpha = a, b, c \\ 0, & \text{else,} \end{cases} \quad (D.8)$$

where $\text{Dom}(L \cup R)_\alpha = \{x_\alpha^i : i \in [\ell]\} \cup \{x_\alpha^j : j \in [r]\}$, and $\text{Im}(L \cup R) = \{y_\alpha^i : i \in [\ell]\} \cup \{y_\alpha^j : j \in [r]\}$. Similarly, we define the not-in-local-domain and not-in-local-image projectors as,

$$\Pi_{\text{AL}_{abc}R_{abc}}^{\notin \text{locDom}} |x_a x_b x_c\rangle_A |L\rangle_{L_{abc}} |R\rangle_{R_{abc}} = \begin{cases} |x_a x_b x_c\rangle_A |L\rangle_{L_{abc}} |R\rangle_{R_{abc}}, & \text{if } x_\alpha \notin \text{Dom}(L \cup R)_\alpha, \forall \alpha = a, b, c \\ 0, & \text{else,} \end{cases} \quad (D.9)$$

$$\Pi_{\text{AL}_{abc}R_{abc}}^{\notin \text{locIm}} |y_a y_b y_c\rangle_A |L\rangle_{L_{abc}} |R\rangle_{R_{abc}} = \begin{cases} |y_a y_b y_c\rangle_A |L\rangle_{L_{abc}} |R\rangle_{R_{abc}}, & \text{if } y_\alpha \notin \text{Im}(L \cup R)_\alpha, \forall \alpha = a, b, c \\ 0, & \text{else.} \end{cases} \quad (D.10)$$

We also let,

$$\Pi_{\mathcal{L}_{abc}\mathcal{R}_{abc}}^{\notin \text{Dom} \rightarrow \notin \text{locDom}} = 1 - \Pi_{\mathcal{L}_{abc}\mathcal{R}_{abc}}^{\text{Dom}} + \Pi_{\mathcal{L}_{abc}\mathcal{R}_{abc}}^{\text{locDom}} \quad (\text{D.11})$$

$$\Pi_{\mathcal{L}_{abc}\mathcal{R}_{abc}}^{\notin \text{Im} \rightarrow \notin \text{locIm}} = 1 - \Pi_{\mathcal{L}_{abc}\mathcal{R}_{abc}}^{\text{Im}} + \Pi_{\mathcal{L}_{abc}\mathcal{R}_{abc}}^{\text{locIm}}, \quad (\text{D.12})$$

denote projectors which do nothing if $x_a x_b x_c \in \text{Dom}(L \cup R)$, and project to the not-in-local-domain subspace if $x_a x_b x_c \notin \text{Dom}(L \cup R)$ (and similar for Im).

Projectors on $\mathcal{L}_{ab}$, $\mathcal{R}_{ab}$, $\mathcal{L}_{bc}$, $\mathcal{R}_{bc}$ and the Compress partial isometry. Let us now turn to the registers $\mathcal{L}_{bc}$, $\mathcal{R}_{bc}$, $\mathcal{L}_{ab}$, $\mathcal{R}_{ab}$. A key component of our proof is to construct a partial isometry between relation states on $\mathcal{L}_{abc} \otimes \mathcal{R}_{abc}$ and those on $\mathcal{L}_{ab} \otimes \mathcal{R}_{ab} \otimes \mathcal{L}_{bc} \otimes \mathcal{R}_{bc}$. Namely, for any state in $\Pi_{\mathcal{L}_{abc}\mathcal{R}_{abc}}^{\text{locbij}}$ on $\mathcal{L}_{abc} \otimes \mathcal{R}_{abc}$, we define an “un-compressed” state,

$$\begin{aligned} \text{Compress}^\dagger \cdot & |\{(x_a^i x_b^i x_c^i, y_a^i y_b^i y_c^i) : i \in [\ell]\}\rangle_{\mathcal{L}_{abc}} |\{(x_a^j x_b^j x_c^j, y_a^j y_b^j y_c^j) : j \in [r]\}\rangle_{\mathcal{R}_{abc}} \\ &= \frac{1}{\sqrt{N_b^{\ell+r}}} \sum_{z_\ell, z_r} |\{(x_a^i x_b^i, y_a^i z_b^i) : i \in [\ell]\}\rangle_{\mathcal{L}_{ab}} |\{(z_b^i x_c^i, y_b^i y_c^i) : i \in [\ell]\}\rangle_{\mathcal{L}_{bc}} \\ &\quad \otimes |\{(x_a^j x_b^j, y_a^j z_b^j) : j \in [r]\}\rangle_{\mathcal{R}_{ab}} |\{(z_b^j x_c^j, y_b^j y_c^j) : j \in [r]\}\rangle_{\mathcal{R}_{bc}}, \end{aligned} \quad (\text{D.13})$$

where we abbreviate $z_\ell \equiv \{z_b^i : i \in [\ell]\}$, $z_r \equiv \{z_b^j : j \in [r]\}$. The final state is a valid relation state because $\{y_a^i : i \in [\ell]\} \cup \{y_a^j : j \in [r]\}$ and $\{x_c^i : i \in [\ell]\} \cup \{x_c^j : j \in [r]\}$ are distinct by assumption. We define **Compress** as the adjoint of this operation.

The range of **Compress**[†] on $\mathcal{L}_{ab} \otimes \mathcal{R}_{ab} \otimes \mathcal{L}_{bc} \otimes \mathcal{R}_{bc}$ consists of the *paired* relation states,

$$\begin{aligned} & \frac{1}{\sqrt{N_b^{\ell+r}}} \sum_{z_\ell, z_r} |L_{ab}^{z_\ell}\rangle_{\mathcal{L}_{ab}} |L_{bc}^{z_\ell}\rangle_{\mathcal{L}_{bc}} |R_{ab}^{z_r}\rangle_{\mathcal{R}_{ab}} |R_{bc}^{z_r}\rangle_{\mathcal{R}_{bc}} \\ & \equiv \frac{1}{\sqrt{N_b^{\ell+r}}} \sum_{z_\ell, z_r} |\{(x_a^i x_b^i, y_a^i z_b^i) : i \in [\ell]\}\rangle_{\mathcal{L}_{ab}} |\{(z_b^i x_c^i, y_b^i y_c^i) : i \in [\ell]\}\rangle_{\mathcal{L}_{bc}} \\ & \quad \otimes |\{(x_a^j x_b^j, y_a^j z_b^j) : j \in [r]\}\rangle_{\mathcal{R}_{ab}} |\{(z_b^j x_c^j, y_b^j y_c^j) : j \in [r]\}\rangle_{\mathcal{R}_{bc}}, \end{aligned} \quad (\text{D.14})$$

for any locally bijective $L \equiv \{(x_a^i x_b^i x_c^i, y_a^i y_b^i y_c^i) : i \in [\ell]\}$ and $R \equiv \{(x_a^j x_b^j x_c^j, y_a^j y_b^j y_c^j) : j \in [r]\}$. We let $\Pi_{\mathcal{L}_{ab}\mathcal{L}_{bc}\mathcal{R}_{ab}\mathcal{R}_{bc}}^{\text{paired}}$ denote the projector onto the set of states above. We have

$$\text{Compress} \cdot \text{Compress}^\dagger = \Pi_{\mathcal{L}_{abc}\mathcal{R}_{abc}}^{\text{locbij}} \quad (\text{D.15})$$

$$\text{Compress}^\dagger \cdot \text{Compress} = \Pi_{\mathcal{L}_{ab}\mathcal{L}_{bc}\mathcal{R}_{ab}\mathcal{R}_{bc}}^{\text{paired}}, \quad (\text{D.16})$$

by construction.

D.1.2 Proof overview

Our proof proceeds in five steps. At each step, we bound the trace distance between two density matrices. The density matrices are,

$$\rho^{(0)} = \mathbb{E}_{U_{abc} \sim H} (|\mathcal{A}_t^{U_{abc}, \mathcal{D}}\rangle \langle \mathcal{A}_t^{U_{abc}, \mathcal{D}}|_{ABCD}) \quad (\text{D.17})$$

$$\rho^{(1)} = \text{Tr}_{\mathcal{L}_{abc}\mathcal{R}_{abc}} (|\mathcal{A}_t^{W_{abc}, \mathcal{D}}\rangle \langle \mathcal{A}_t^{W_{abc}, \mathcal{D}}|_{AB\mathcal{L}_{abc}\mathcal{R}_{abc}CD}) \quad (\text{D.18})$$

$$\rho^{(2)} = \text{Tr}_{\mathcal{L}_{abc}\mathcal{R}_{abc}} (|\mathcal{A}_t^{W'_{abc}, \mathcal{D}}\rangle \langle \mathcal{A}_t^{W'_{abc}, \mathcal{D}}|_{AB\mathcal{L}_{abc}\mathcal{R}_{abc}CD}) \quad (\text{D.19})$$

$$\rho^{(3)} = \text{Tr}_{\text{L}_{ab}\text{L}_{bc}\text{R}_{ab}\text{R}_{bc}\text{CD}} \left(|\mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}} \rangle \langle \mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}}|_{\text{ABL}_{ab}\text{L}_{bc}\text{R}_{ab}\text{R}_{bc}\text{CD}} \right) \quad (\text{D.20})$$

$$\rho^{(4)} = \text{Tr}_{\text{L}_{ab}\text{L}_{bc}\text{R}_{ab}\text{R}_{bc}\text{CD}} \left(|\mathcal{A}_t^{V_{bc}V_{ab}, \mathcal{D}} \rangle \langle \mathcal{A}_t^{V_{bc}V_{ab}, \mathcal{D}}|_{\text{ABL}_{ab}\text{L}_{bc}\text{R}_{ab}\text{R}_{bc}\text{CD}} \right) \quad (\text{D.21})$$

$$\rho^{(5)} = \mathbb{E}_{U_{ab}, U_{bc} \sim H} \left(|\mathcal{A}_t^{U_{bc}U_{ab}, \mathcal{D}} \rangle \langle \mathcal{A}_t^{U_{bc}U_{ab}, \mathcal{D}}|_{\text{ABCD}} \right) \quad (\text{D.22})$$

The first density matrix is the expected output state of an experiment that queries a Haar-random unitary U_{abc} (and its inverse, conjugate, and transpose). The last density matrix is the expected output of an experiment that queries $U_{bc}U_{ab}$.

The intermediary density matrices denote the output state of experiments in which the action of each unitary is replaced with a path-recording oracle. In particular, in the third step, $|\mathcal{A}_t^{W'_{abc}, \mathcal{D}} \rangle$ denotes the state in which each application of W_{abc} , $W_{abc}^\dagger$, $\overline{W}_{abc}$, $\overline{W}_{abc}^\dagger$ is replaced by the operators,

$$W'_{abc} \equiv \Pi^{\text{locbij}} \cdot W_{abc} \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \quad (\text{D.23})$$

$$(W_{abc}^\dagger)' \equiv \Pi^{\text{locbij}} \cdot W_{abc}^\dagger \cdot \Pi^{\notin \text{Im} \rightarrow \notin \text{locIm}} \quad (\text{D.24})$$

$$\overline{W}'_{abc} \equiv \Pi^{\text{locbij}} \cdot \overline{W}_{abc} \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \quad (\text{D.25})$$

$$(\overline{W}_{abc}^\dagger)' \equiv \Pi^{\text{locbij}} \cdot \overline{W}_{abc}^\dagger \cdot \Pi^{\notin \text{Im} \rightarrow \notin \text{locIm}}, \quad (\text{D.26})$$

respectively. Similarly, in the fourth step, $|\mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}} \rangle$ denotes the state in which each application of $W_{bc}W_{ab}$, $W_{ab}^\dagger W_{bc}^\dagger$, $\overline{W}_{bc}\overline{W}_{ab}$, $\overline{W}_{ab}^\dagger \overline{W}_{bc}^\dagger$ is replaced by,

$$(W_{bc}W_{ab})' \equiv \Pi^{\text{paired}} \cdot W_{bc}W_{ab} \cdot \tilde{\Pi}^{\mathcal{D}(W_{abc})} \cdot \tilde{\Pi}^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \quad (\text{D.27})$$

$$(W_{ab}^\dagger W_{bc}^\dagger)' \equiv \Pi^{\text{paired}} \cdot W_{ab}^\dagger W_{bc}^\dagger \cdot \tilde{\Pi}^{\mathcal{D}(W_{abc}^\dagger)} \cdot \tilde{\Pi}^{\notin \text{Im} \rightarrow \notin \text{locIm}} \quad (\text{D.28})$$

$$(\overline{W}_{bc}\overline{W}_{ab})' \equiv \Pi^{\text{paired}} \cdot \overline{W}_{bc}\overline{W}_{ab} \cdot \tilde{\Pi}^{\mathcal{D}(\overline{W}_{abc})} \cdot \tilde{\Pi}^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \quad (\text{D.29})$$

$$(\overline{W}_{ab}^\dagger \overline{W}_{bc}^\dagger)' \equiv \Pi^{\text{paired}} \cdot \overline{W}_{ab}^\dagger \overline{W}_{bc}^\dagger \cdot \tilde{\Pi}^{\mathcal{D}(\overline{W}_{abc}^\dagger)} \cdot \tilde{\Pi}^{\notin \text{Im} \rightarrow \notin \text{locIm}}, \quad (\text{D.30})$$

respectively. Here, we let $\tilde{\Pi} \equiv \text{Compress}^\dagger \cdot \Pi \cdot \text{Compress}$, for any projector Π .

We bound the trace distance between each pair of density matrices as follows.

$$1. \quad \|\rho^{(0)} - \rho^{(1)}\|_1 \leq 9t(t+2)/N_{abc}^{1/8} + 2t^{1/4}\varepsilon^{1/4} \quad (\text{Theorem 10 and Lemma 25})$$

$$2. \quad \|\rho^{(1)} - \rho^{(2)}\|_1 \leq 17t^2/N_{abc}^{1/8} + 7t^{3/2}/(\min_\alpha N_\alpha)^{1/2} + 6t^{5/4}\varepsilon^{1/4} \quad (\text{Section D.1.3})$$

$$3. \quad \|\rho^{(2)} - \rho^{(3)}\|_1 \leq t^2/N_{ab} + t^2/N_{bc} \quad (\text{Section D.1.4})$$

$$4. \quad \|\rho^{(3)} - \rho^{(4)}\|_1 \leq 2t \sqrt{\frac{17t^2}{N_{abc}^{1/8}} + \frac{7t^{3/2}}{(\min_\alpha N_\alpha)^{1/2}} + \frac{2t^2}{N_{ab}} + \frac{2t^2}{N_{bc}} + \frac{9t}{N_{abc}^{1/8}} + 8t^{5/4}\varepsilon^{1/4}} \quad (\text{Section D.1.5})$$

$$5. \quad \|\rho^{(4)} - \rho^{(5)}\|_1 \leq 9t(t+1)/N_{ab}^{1/8} + 9t(t+1)/N_{bc}^{1/8} \quad (\text{Theorem 10})$$

By the triangle inequality, the total trace distance, $\|\rho^{(0)} - \rho^{(5)}\|_1$, is less than the sum of the five distances above. If each local Hilbert space has dimension at least $N_\alpha \geq 2^\xi$, then we have $\|\rho^{(0)} - \rho^{(5)}\|_1 \leq \mathcal{O}(t^2/2^{(3/16)\xi}) + \mathcal{O}(t^{5/8}\varepsilon^{1/8})$ as claimed. $\square$

D.1.3 Twirled W_{abc} is indistinguishable from twirled projected W_{abc}

We will prove that

$$\text{TD}_t \equiv \text{TD} \left(|\mathcal{A}_t^{W_{abc}, \mathcal{D}} \rangle \langle \mathcal{A}_t^{W_{abc}, \mathcal{D}}|, |\mathcal{A}_t^{W'_{abc}, \mathcal{D}} \rangle \langle \mathcal{A}_t^{W'_{abc}, \mathcal{D}}| \right) \leq \frac{2\sqrt{70}t^2}{N_{abc}^{1/8}} + \frac{4\sqrt{3}t^{3/2}}{(\min_\alpha N_\alpha)^{1/2}} + 6t^{5/4}\varepsilon^{1/4}. \quad (\text{D.31})$$

This implies that $\|\rho^{(1)} - \rho^{(2)}\|_1$ is less than the same value since the 1-norm cannot increase after tracing out $L_{abc}R_{abc}$. The claim follows since $2\sqrt{70} < 17$ and $4\sqrt{3} < 7$.

We proceed by induction. The statement holds trivially at $t = 0$. To prove the inductive step, suppose that the Eq. (D.31) holds up to time $t-1$ for any $t \geq 1$. Without loss of generality, we assume that the forward unitary is applied at time t . The case when the inverse or conjugate or transpose are applied follow by symmetric arguments. The states at time t are obtained from the states at time $t-1$ as follows,

$$|\mathcal{A}_t^{W_{abc}, \mathcal{D}}\rangle = cD \cdot W_{abc} \cdot cC \cdot A_t \cdot |\mathcal{A}_{t-1}^{W_{abc}, \mathcal{D}}\rangle \quad (D.32)$$

$$|\mathcal{A}_t^{W'_{abc}, \mathcal{D}}\rangle = cD \cdot \Pi^{\text{locbij}} \cdot W_{abc} \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \cdot cC \cdot A_t \cdot |\mathcal{A}_{t-1}^{W'_{abc}, \mathcal{D}}\rangle \quad (D.33)$$

We have

$$\begin{aligned} \text{TD}_t &\leq \text{TD}_t + 2 \left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot cC \cdot A_t |\mathcal{A}_{t-1}^{W_{abc}, \mathcal{D}}\rangle \right\|_2 \\ &\quad + 2 \left\| (1 - \Pi^{\text{locbij}}) \cdot W_{abc} \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \cdot cC \cdot A_t \cdot |\mathcal{A}_{t-1}^{W'_{abc}, \mathcal{D}}\rangle \right\|_2, \end{aligned} \quad (D.34)$$

where the first term accounts for the error up to time t , the second term for the error induced by the projector $\Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}$ [using Eq. (B.18)], and the third term for the error induced by the projector Π^{locbij} [again using Eq. (B.18)].

We bound the second term as follows. From Eq. (9.55) and Claim 18 of Ref. [42] (see also the modification of Claim 18 to strong approximate designs in the proof of Lemma 25), we have

$$\left\| |\mathcal{A}_{t-1}^{W_{abc}, \mathcal{D}}\rangle - cQ \cdot |\mathcal{A}_{t-1}^{V_{abc}}\rangle \right\|_2 \leq \frac{\sqrt{70}t}{N_{abc}^{1/8}} + 2t^{1/4}\varepsilon^{1/4}. \quad (D.35)$$

This yields,

$$\begin{aligned} &\left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot cC \cdot A_t \cdot |\mathcal{A}_{t-1}^{W_{abc}, \mathcal{D}}\rangle \right\|_2 \\ &\leq \left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot cC \cdot A_t \cdot cQ \cdot |\mathcal{A}_{t-1}^{V_{abc}}\rangle \right\|_2 + \frac{\sqrt{70}t}{N_{abc}^{1/8}} + 2t^{1/4}\varepsilon^{1/4}. \end{aligned} \quad (D.36)$$

The latter state norm can be written out explicitly, as

$$\begin{aligned} &\left\| (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot cC \cdot A_t \cdot cQ \cdot |\mathcal{A}_{t-1}^{V_{abc}}\rangle \right\|_2 \\ &= \sqrt{\langle \mathcal{A}_{t-1}^{V_{abc}} | \cdot A_t^\dagger \cdot cQ^\dagger \cdot cC^\dagger \cdot (1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}) \cdot cC \cdot cQ \cdot A_t \cdot |\mathcal{A}_{t-1}^{V_{abc}} \rangle}. \end{aligned} \quad (D.37)$$

where we used that A_t and cQ act on distinct registers to commute them past one another.

To proceed, we first apply the operator inequality,

$$1 - \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \preceq \sum_{\alpha} \sum_{i \in [\ell]} \Pi_{A_{\alpha} L_{X_{\alpha}, i}}^{\text{eq}} \Pi_{A_{\bar{\alpha}} L_{X_{\bar{\alpha}}, i}}^{\text{neq}} + \sum_{\alpha} \sum_{j \in [r]} \Pi_{A_{\alpha} R_{X_{\alpha}, j}}^{\text{eq}} \Pi_{A_{\bar{\alpha}} R_{X_{\bar{\alpha}}, j}}^{\text{neq}}, \quad (D.38)$$

where $\Pi_{A_{\alpha} L_{X_{\alpha}, i}}^{\text{eq}}$ projects onto states with the same bitstring on A_{α} as on $L_{X_{\alpha}, i}^{(\ell)}$, and

$$\Pi_{A_{\bar{\alpha}} L_{X_{\bar{\alpha}}, i}}^{\text{neq}} \equiv 1 - \Pi_{A_{\bar{\alpha}} L_{X_{\bar{\alpha}}, i}}^{\text{eq}} \quad (D.39)$$

does the reverse on $\bar{\alpha}$ (where we define $\bar{\alpha} \equiv \text{bc}$ if $\alpha = \text{a}$, and analogous for $\alpha = \text{b}, \text{c}$). For each individual term with $i \in [\ell]$, we have

$$\begin{aligned} & \langle \mathcal{A}_{t-1}^{V_{\text{abc}}} | \cdot A_t^\dagger \cdot \text{cQ}_{\text{CDL}_{\text{abc}} R_{\text{abc}}}^\dagger \cdot \text{cC}_{\text{CA}}^\dagger \cdot \Pi_{A_\alpha L_{X_\alpha, i}}^{\text{eq}} \Pi_{A_{\bar{\alpha}} L_{X_{\bar{\alpha}}, i}}^{\text{neq}} \cdot \text{cC}_{\text{CA}} \cdot \text{cQ}_{\text{CDL}_{\text{abc}} R_{\text{abc}}} \cdot A_t \cdot | \mathcal{A}_{t-1}^{V_{\text{abc}}} \rangle \\ &= \langle \mathcal{A}_{t-1}^{V_{\text{abc}}} | \cdot A_t^\dagger \cdot \text{cC}_{\text{CL}_{X_{\bar{\alpha}}, i}}^{\dagger(\ell)} \cdot \text{cC}_{\text{CA}}^\dagger \cdot \Pi_{A_\alpha L_{X_\alpha, i}}^{\text{eq}} \Pi_{A_{\bar{\alpha}} L_{X_{\bar{\alpha}}, i}}^{\text{neq}} \cdot \text{cC}_{\text{CA}} \cdot \text{cC}_{\text{CL}_{X_{\bar{\alpha}}, i}}^{(\ell)} \cdot A_t \cdot | \mathcal{A}_{t-1}^{V_{\text{abc}}} \rangle, \end{aligned} \quad (\text{D.40})$$

where all but one of the Clifford unitaries in cQ cancel, since the middle term in the expectation value acts only on register $L_{X_\alpha, i}$. For terms with $j \in [r]$, we have instead

$$\begin{aligned} & \langle \mathcal{A}_{t-1}^{V_{\text{abc}}} | \cdot A_t^\dagger \cdot \text{cQ}_{\text{CDL}_{\text{abc}} R_{\text{abc}}}^\dagger \cdot \text{cC}_{\text{CA}}^\dagger \cdot \Pi_{A_\alpha R_{X_\alpha, j}}^{\text{eq}} \Pi_{A_{\bar{\alpha}} R_{X_{\bar{\alpha}}, j}}^{\text{neq}} \cdot \text{cC}_{\text{CA}} \cdot \text{cQ}_{\text{CDL}_{\text{abc}} R_{\text{abc}}} \cdot A_t \cdot | \mathcal{A}_{t-1}^{V_{\text{abc}}} \rangle \\ &= \langle \mathcal{A}_{t-1}^{V_{\text{abc}}} | \cdot A_t^\dagger \cdot \text{c}\bar{\text{C}}_{\text{CR}_{X_{\bar{\alpha}}, j}}^{\dagger(r)} \cdot \text{cC}_{\text{CA}}^\dagger \cdot \Pi_{A_\alpha R_{X_\alpha, j}}^{\text{eq}} \Pi_{A_{\bar{\alpha}} R_{X_{\bar{\alpha}}, j}}^{\text{neq}} \cdot \text{cC}_{\text{CA}} \cdot \text{c}\bar{\text{C}}_{\text{CR}_{X_{\bar{\alpha}}, j}}^{(r)} \cdot A_t \cdot | \mathcal{A}_{t-1}^{V_{\text{abc}}} \rangle. \end{aligned} \quad (\text{D.41})$$

We can upper bound the latter expectation values by performing the twirl over C . From Eq. (B.21) and Eq. (B.22), this yields an upper bound of $1/N_\alpha$ on both Eq. (D.40) and Eq. (D.41). Therefore, in total, we have an upper bound

$$\left\| (1 - \Pi^{\text{Dom} \rightarrow \text{locDom}}) \cdot \text{cC} \cdot A_t \cdot \text{cQ} \cdot | \mathcal{A}_{t-1}^{V_{\text{abc}}} \rangle \right\|_2 \leq \sqrt{(\ell + r) \sum_{\alpha} (1/N_\alpha + \varepsilon)} \leq \sqrt{3t / \min_{\alpha} N_\alpha + 3t\varepsilon}.$$

The third term in Eq. (D.34) is simpler to bound. The input state to W_{abc} lies in the subspace $\Pi_{\leq t}^{\text{locbij}}$ by construction. Therefore, the output of W_{abc} lies in the subspace $\Pi^{\mathcal{I}(W_{\text{abc}} \Pi_{\leq t}^{\text{locbij}})}$. This latter subspace is spanned by two classes of states. The first class is,

$$|y_a y_b y_c\rangle_A |L\rangle_{L_{\text{abc}}} |R\rangle_{R_{\text{abc}}}, \quad (\text{D.42})$$

for any $\ell + r \leq t$, where $\text{Dom}(L \cup R)_\alpha$ is distinct, $\text{Im}(L \cup R)_\alpha$ is distinct, and $y_\alpha \notin \text{Im}(L \cup R)_\alpha$. These arise if the $W_{\text{abc}}^{R, \dagger}$ branch of W_{abc} is applied. The second class is,

$$\frac{1}{\sqrt{N_{\text{abc}} - \ell - r}} \sum_{y_a y_b y_c \notin \text{Im}(L \cup R)} |y_a y_b y_c\rangle_A |L \cup (x_a x_b x_c, y_a y_b y_c)\rangle_{L_{\text{abc}}} |R\rangle_{R_{\text{abc}}}, \quad (\text{D.43})$$

for $\ell + r \leq t$, where $\text{Dom}(L \cup R)_\alpha$ is distinct, $\text{Im}(L \cup R)_\alpha$ is distinct, and $x_\alpha \notin \text{Dom}(L \cup R)_\alpha$. These arise if the W_{abc}^L branch of W_{abc} is applied. The states above are mutually orthogonal to one another as well as between different ℓ, r .

The first class of states is invariant under Π^{locbij} . Thus, the projector Π^{locbij} acts trivially and incurs no error. Meanwhile, on the second class of states, we have

$$\begin{aligned} & \Pi^{\text{locbij}} \frac{1}{\sqrt{N_{\text{abc}} - \ell - r}} \sum_{y_a y_b y_c \notin \text{Im}(L \cup R)} |y_a y_b y_c\rangle_A |L \cup (x_a x_b x_c, y_a y_b y_c)\rangle_{L_{\text{abc}}} |R\rangle_{R_{\text{abc}}} \\ &= \frac{1}{\sqrt{N_{\text{abc}} - \ell - r}} \sum_{\substack{y_a \notin \text{Im}(L \cup R)_a \\ y_b \notin \text{Im}(L \cup R)_b \\ y_c \notin \text{Im}(L \cup R)_c}} |y_a y_b y_c\rangle_A |L \cup (x_a x_b x_c, y_a y_b y_c)\rangle_{L_{\text{abc}}} |R\rangle_{R_{\text{abc}}}. \end{aligned} \quad (\text{D.44})$$

The final state is orthogonal to the first class of states, as well as between different ℓ, r . The state has norm $(\prod_{\alpha} (N_\alpha - \ell - r)) / (N - \ell - r) \geq 1 - 3t / \min_{\alpha} N_\alpha$. The above analysis establishes that $\Pi^{\text{locbij}} \Pi^{\mathcal{I}(W_{\text{abc}} \Pi_{\leq t}^{\text{locbij}})}$ is block diagonal between the two classes of input and output states, as well as

between different ℓ, r . Therefore, the desired error is given by the maximum error within each block. From the above, the maximum is achieved at $\ell + r = t$, which yields,

$$\left\| (1 - \Pi^{\text{locbij}}) \cdot W_{\text{abc}} \cdot \Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{W'_{\text{abc}}, \mathfrak{D}}\rangle \right\|_2 \leq \sqrt{3t / \min_{\alpha} N_{\alpha}}. \quad (\text{D.45})$$

In total, we have shown that the error in Eq. (D.34) is upper bounded by,

$$\text{TD}_t \leq \text{TD}_t + \frac{2\sqrt{70}t}{N_{\text{abc}}^{1/8}} + 2t^{1/4}\varepsilon^{1/4} + 4\sqrt{\frac{3t}{\min_{\alpha} N_{\alpha}}} + 2\sqrt{3t\varepsilon} \leq \frac{2\sqrt{70}t^2}{N_{\text{abc}}^{1/8}} + \frac{4\sqrt{3}t^{3/2}}{(\min_{\alpha} N_{\alpha})^{1/2}} + 6t^{5/4}\varepsilon^{1/4}, \quad (\text{D.46})$$

applying the inductive hypothesis. This completes our proof.

D.1.4 Projected W_{abc} is indistinguishable from projected $W_{\text{bc}}W_{\text{ab}}$

We will prove that

$$\left\| \text{Compress}^{\dagger} |\mathcal{A}_t^{W'_{\text{abc}}, \mathfrak{D}}\rangle - |\mathcal{A}_t^{(W_{\text{bc}}W_{\text{ab}})', \mathfrak{D}}\rangle \right\|_2 \leq \frac{t(t-1)}{2N_{\text{ab}}} + \frac{t(t-1)}{2N_{\text{bc}}} \quad (\text{D.47})$$

Using Eq. (B.18), this implies that

$$\text{TD} \left(\text{Compress}^{\dagger} |\mathcal{A}_t^{W'_{\text{abc}}, \mathfrak{D}}\rangle \langle \mathcal{A}_t^{W'_{\text{abc}}, \mathfrak{D}}| \text{Compress}, |\mathcal{A}_t^{(W_{\text{bc}}W_{\text{ab}})', \mathfrak{D}}\rangle \langle \mathcal{A}_t^{(W_{\text{bc}}W_{\text{ab}})', \mathfrak{D}}| \right) \leq \frac{t^2}{N_{\text{ab}}} + \frac{t^2}{N_{\text{bc}}} \quad (\text{D.48})$$

which implies that $\|\rho^{(2)} - \rho^{(3)}\|_1$ is less than the same value since the 1-norm cannot increase after tracing out $L_{\text{ab}}L_{\text{bc}}R_{\text{ab}}R_{\text{bc}}\text{CD}$.

We proceed by induction. The statement holds trivially at $t = 0$. For the inductive step, we assume that Eq. (D.47) holds up to time $t - 1$. We will show that the claim holds for time t as well. Without loss of generality, we assume that the forward unitary is applied at time t . The case when the inverse or conjugate or transpose are applied follow by symmetric arguments.

The states at time t are obtained from the states at time $t - 1$ as follows,

$$|\mathcal{A}_t^{W'_{\text{abc}}, \mathfrak{D}}\rangle = \text{cD} \cdot W'_{\text{abc}} \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{W'_{\text{abc}}, \mathfrak{D}}\rangle \quad (\text{D.49})$$

$$|\mathcal{A}_t^{(W_{\text{bc}}W_{\text{ab}})', \mathfrak{D}}\rangle = \text{cD} \cdot (W_{\text{bc}}W_{\text{ab}})' \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{(W_{\text{bc}}W_{\text{ab}})', \mathfrak{D}}\rangle \quad (\text{D.50})$$

The final projection in W'_{abc} and $(W_{\text{bc}}W_{\text{ab}})'$ guarantees that the input state to the t -th application of W'_{abc} and $(W_{\text{bc}}W_{\text{ab}})'$ obeys,

$$\Pi_{L_{\text{abc}}R_{\text{abc}}}^{\text{locbij}} \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{W'_{\text{abc}}, \mathfrak{D}}\rangle = \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{W'_{\text{abc}}, \mathfrak{D}}\rangle \quad (\text{D.51})$$

$$\Pi_{L_{\text{ab}}L_{\text{bc}}R_{\text{ab}}R_{\text{bc}}}^{\text{paired}} \cdot \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{(W_{\text{bc}}W_{\text{ab}})', \mathfrak{D}}\rangle = \text{cC} \cdot A_t \cdot |\mathcal{A}_{t-1}^{(W_{\text{bc}}W_{\text{ab}})', \mathfrak{D}}\rangle. \quad (\text{D.52})$$

We will now analyze the action of first W'_{abc} and then $(W_{\text{bc}}W_{\text{ab}})'$.

The domain of $W'_{\text{abc}}\Pi^{\text{locbij}}$ contains two classes of states, corresponding to the domain of

$$\Pi^{\mathcal{D}(W'_{\text{abc}})}\Pi^{\text{locbij}} = \Pi^{\mathcal{D}(W_{\text{abc}})}\Pi^{\notin \text{Dom} \rightarrow \notin \text{locDom}}\Pi^{\text{locbij}} = \Pi^{\notin \text{locDom}}\Pi^{\text{locbij}} + \Pi^{\mathcal{I}(W_{\text{abc}}^R)}\Pi^{\text{locbij}}. \quad (\text{D.53})$$

The second equality follows from the domain of W_{abc} ,

$$\Pi^{\mathcal{D}(W_{\text{abc}})} = \Pi^{\notin \text{Dom}}\Pi^{\text{bij}} + \Pi^{\mathcal{I}(W_{\text{abc}}^R)}. \quad (\text{D.54})$$

We will consider the action on each class of states separately. Focusing on the $\mathbf{A}_{\text{abc}}\mathbf{R}_{\text{abc}}$ registers, a complete basis for the first class of states is given by,

$$|x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}\rangle_{\mathbf{A}} |L\rangle_{\mathbf{L}_{\text{abc}}} |R\rangle_{\mathbf{R}_{\text{abc}}}, \quad (\text{D.55})$$

where $\text{Dom}(L \cup R)_{\alpha}$ is distinct, $\text{Im}(L \cup R)_{\alpha}$ is distinct, and $x_{\alpha} \notin \text{Dom}(L \cup R)_{\alpha}$. We then have,

$$\begin{aligned} W'_{\text{abc}} |x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}\rangle_{\mathbf{A}} |L\rangle_{\mathbf{L}_{\text{abc}}} |R\rangle_{\mathbf{R}_{\text{abc}}} &= \Pi^{\text{locbij}} W_{\text{abc}} |x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}\rangle_{\mathbf{A}} |L\rangle_{\mathbf{L}_{\text{abc}}} |R\rangle_{\mathbf{R}_{\text{abc}}} \\ &= \Pi^{\text{locbij}} \frac{1}{\sqrt{N_{\text{abc}} - \ell - r}} \sum_{y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}} \notin \text{Im}(L \cup R)} |y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}}\rangle_{\mathbf{A}} |L \cup (x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}, y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}})\rangle_{\mathbf{L}_{\text{abc}}} |R\rangle_{\mathbf{R}_{\text{abc}}} \\ &= \frac{1}{\sqrt{N_{\text{abc}} - \ell - r}} \sum_{\substack{y_{\mathbf{a}} \notin \text{Im}(L \cup R)_{\mathbf{a}} \\ y_{\mathbf{b}} \notin \text{Im}(L \cup R)_{\mathbf{b}} \\ y_{\mathbf{c}} \notin \text{Im}(L \cup R)_{\mathbf{c}}}} |y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}}\rangle_{\mathbf{A}} |L \cup (x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}, y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}})\rangle_{\mathbf{L}_{\text{abc}}} |R\rangle_{\mathbf{R}_{\text{abc}}}. \end{aligned} \quad (\text{D.56})$$

Meanwhile, a complete basis for the second class of states is given by

$$\frac{1}{\sqrt{\prod_{\alpha} (N_{\alpha} - \ell - r)}} \sum_{\substack{x_{\mathbf{a}} \notin \text{Dom}(L \cup R)_{\mathbf{a}} \\ x_{\mathbf{b}} \notin \text{Dom}(L \cup R)_{\mathbf{b}} \\ x_{\mathbf{c}} \notin \text{Dom}(L \cup R)_{\mathbf{c}}}} |x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}\rangle_{\mathbf{A}} |L\rangle_{\mathbf{L}_{\text{abc}}} |R \cup (x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}, y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}})\rangle_{\mathbf{R}_{\text{abc}}}, \quad (\text{D.57})$$

where $\text{Dom}(L \cup R)_{\alpha}$ is distinct, $\text{Im}(L \cup R)_{\alpha}$ is distinct, and $y_{\alpha} \notin \text{Im}(L \cup R)_{\alpha}$. We then have,

$$\begin{aligned} W'_{\text{abc}} \cdot \frac{1}{\sqrt{\prod_{\alpha} (N_{\alpha} - \ell - r)}} \sum_{\substack{x_{\mathbf{a}} \notin \text{Dom}(L \cup R)_{\mathbf{a}} \\ x_{\mathbf{b}} \notin \text{Dom}(L \cup R)_{\mathbf{b}} \\ x_{\mathbf{c}} \notin \text{Dom}(L \cup R)_{\mathbf{c}}}} |x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}\rangle_{\mathbf{A}} |L\rangle_{\mathbf{L}_{\text{abc}}} |R \cup (x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}, y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}})\rangle_{\mathbf{R}_{\text{abc}}} \\ = \Pi^{\text{locbij}} W_{\text{abc}}^{R, \dagger} \cdot \frac{1}{\sqrt{\prod_{\alpha} (N_{\alpha} - \ell - r)}} \sum_{\substack{x_{\mathbf{a}} \notin \text{Dom}(L \cup R)_{\mathbf{a}} \\ x_{\mathbf{b}} \notin \text{Dom}(L \cup R)_{\mathbf{b}} \\ x_{\mathbf{c}} \notin \text{Dom}(L \cup R)_{\mathbf{c}}}} |x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}\rangle_{\mathbf{A}} |L\rangle_{\mathbf{L}_{\text{abc}}} |R \cup (x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}, y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}})\rangle_{\mathbf{R}_{\text{abc}}} \\ = \left(\frac{\sqrt{\prod_{\alpha} (N_{\alpha} - \ell - r)}}{\sqrt{N_{\text{abc}} - \ell - r}} \right) \Pi^{\text{locbij}} |y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}}\rangle_{\mathbf{A}} |L\rangle_{\mathbf{L}_{\text{abc}}} |R\rangle_{\mathbf{R}_{\text{abc}}} \\ = \left(\frac{\sqrt{\prod_{\alpha} (N_{\alpha} - \ell - r)}}{\sqrt{N_{\text{abc}} - \ell - r}} \right) |y_{\mathbf{a}}y_{\mathbf{b}}y_{\mathbf{c}}\rangle_{\mathbf{A}} |L\rangle_{\mathbf{L}_{\text{abc}}} |R\rangle_{\mathbf{R}_{\text{abc}}}, \end{aligned} \quad (\text{D.58})$$

where the factor in parentheses arises from the decrease in normalization when the projector $\Pi^{\mathcal{I}(W_{\text{abc}}^R)}$ is applied (through $W_{\text{abc}}^{R, \dagger} = W_{\text{abc}}^{R, \dagger} \Pi^{\mathcal{I}(W_{\text{abc}}^R)}$).

Let us now turn to $(W_{\text{bc}}W_{\text{ab}})'$. The input state to $W_{\text{bc}}W_{\text{ab}}$ is contained within the domain of

$$\tilde{\Pi}^{\mathcal{D}(W_{\text{abc}})} \tilde{\Pi}^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \Pi^{\text{paired}} = \tilde{\Pi}^{\notin \text{locDom}} \Pi^{\text{paired}} + \tilde{\Pi}^{\mathcal{I}(W_{\text{abc}}^R)} \Pi^{\text{paired}}. \quad (\text{D.59})$$

As before, we must consider two classes of input states, corresponding to the domain of each term on the right side above. Focusing on the $\mathbf{L}_{\text{ab}}\mathbf{L}_{\text{bc}}\mathbf{R}_{\text{ab}}\mathbf{R}_{\text{bc}}$ registers, a complete basis for the first class of states is given by,

$$\frac{1}{\sqrt{N_{\mathbf{b}}^{\ell+r}}} \sum_{z_{\ell}, z_r} |x_{\mathbf{a}}x_{\mathbf{b}}x_{\mathbf{c}}\rangle_{\mathbf{A}} |L_{\text{ab}}^{z_{\ell}}\rangle_{\mathbf{L}_{\text{ab}}} |L_{\text{bc}}^{z_{\ell}}\rangle_{\mathbf{L}_{\text{bc}}} |R_{\text{ab}}^{z_r}\rangle_{\mathbf{R}_{\text{ab}}} |R_{\text{bc}}^{z_r}\rangle_{\mathbf{R}_{\text{bc}}}, \quad (\text{D.60})$$

where $\text{Dom}(L \cup R)_\alpha$ is distinct, $\text{Im}(L \cup R)_\alpha$ is distinct, and $x_\alpha \notin \text{Dom}(L \cup R)_\alpha$. (We refer to Section D.1.1 for the definitions of $L_{ab}^{z_\ell}$, $L_{bc}^{z_\ell}$, $R_{ab}^{z_r}$, $R_{bc}^{z_r}$, L , R .) Focusing on the $\text{AL}_{ab}\text{R}_{ab}$ registers, the application of W_{ab} gives,

$$W_{ab} |x_a x_b x_c\rangle_A |L_{ab}^{z_\ell}\rangle_{L_{ab}} |R_{ab}^{z_r}\rangle_{R_{ab}} = \frac{1}{\sqrt{N_{ab} - \ell - r}} \sum_{y_a z_b \notin \text{Im}(L_{ab} \cup R_{ab})} |y_a z_b x_c\rangle_A |L_{ab}^{z_\ell} \cup (x_a x_b, y_a z_b)\rangle_{L_{ab}} |R_{ab}^{z_r}\rangle_{R_{ab}}. \quad (\text{D.61})$$

Focusing on the $\text{AL}_{bc}\text{R}_{bc}$ registers, the ensuing application of W_{bc} gives,

$$W_{bc} |y_a z_b x_c\rangle_A |L_{bc}^{z_\ell}\rangle_{L_{bc}} |R_{bc}^{z_r}\rangle_{R_{bc}} = \frac{1}{\sqrt{N_{bc} - \ell - r}} \sum_{y_b y_c \notin \text{Im}(L_{bc} \cup R_{bc})} |y_a y_b y_c\rangle_A |L_{bc}^{z_\ell} \cup (z_b x_c, y_b y_c)\rangle_{L_{bc}} |R_{bc}^{z_r}\rangle_{R_{bc}}. \quad (\text{D.62})$$

In total, we have the state,

$$\frac{1}{\sqrt{\mathcal{N}_1}} \sum_{\substack{z_\ell, z_r \\ y_a z_b \notin \text{Im}(L_{ab} \cup R_{ab}) \\ y_b y_c \notin \text{Im}(L_{bc} \cup R_{bc})}} |y_a y_b y_c\rangle_A |L_{ab}^{z_\ell} \cup (x_a x_b, y_a z_b)\rangle_{L_{ab}} |L_{bc}^{z_\ell} \cup (z_b x_c, y_b y_c)\rangle_{L_{bc}} |R_{ab}^{z_r}\rangle_{R_{ab}} |R_{bc}^{z_r}\rangle_{R_{bc}}, \quad (\text{D.63})$$

where $\mathcal{N}_1 \equiv N_b^{\ell+r} (N_{ab} - \ell - r) (N_{bc} - \ell - r)$. Applying the final projection Π^{paired} forces the y_α to be locally distinct, which yields,

$$\frac{1}{\sqrt{\mathcal{N}_1}} \sum_{\substack{z_\ell, z_r, z_b \\ y_a \notin \text{Im}(L \cup R)_a \\ y_b \notin \text{Im}(L \cup R)_b \\ y_c \notin \text{Im}(L \cup R)_c}} |y_a y_b y_c\rangle_A |L_{ab}^{z_\ell} \cup (x_a x_b, y_a z_b)\rangle_{L_{ab}} |L_{bc}^{z_\ell} \cup (z_b x_c, y_b y_c)\rangle_{L_{bc}} |R_{ab}^{z_r}\rangle_{R_{ab}} |R_{bc}^{z_r}\rangle_{R_{bc}}, \quad (\text{D.64})$$

where the sum over z_b is unrestricted, since $y_a \notin \text{Im}(L \cup R)_a$ implies that $y_a z_b \notin \text{Im}(L_{ab} \cup R_{ab})$. Applying **Compress** to the state yields the state in Eq. (D.56) up to a normalization difference,

$$\left| \sqrt{\frac{N_b \prod_\alpha (N_\alpha - \ell - r)}{(N_{ab} - \ell - r)(N_{bc} - \ell - r)}} - \sqrt{\frac{\prod_\alpha (N_\alpha - \ell - r)}{N - \ell - r}} \right| \leq \frac{\ell + r}{N_{ab}} + \frac{\ell + r}{N_{bc}}, \quad (\text{D.65})$$

where the first inequality holds for $(\ell + r)/N_{ab} + (\ell + r)/N_{bc} \leq 1/2$.

We now turn to the second class of states. A complete basis is given by

$$\frac{1}{\sqrt{\mathcal{N}_2}} \sum_{\substack{z_\ell, z_r, z_b \\ x_a \notin \text{Dom}(L \cup R)_a \\ x_b \notin \text{Dom}(L \cup R)_b \\ x_c \notin \text{Dom}(L \cup R)_c}} |x_a x_b x_c\rangle_A |L_{ab}^{z_\ell}\rangle_{L_{ab}} |L_{bc}^{z_\ell}\rangle_{L_{bc}} |R_{ab}^{z_r} \cup (x_a x_b, y_a z_b)\rangle_{R_{ab}} |R_{bc}^{z_r} \cup (z_b x_c, y_b y_c)\rangle_{R_{bc}}, \quad (\text{D.66})$$

where $\text{Dom}(L \cup R)_\alpha$ is distinct, $\text{Im}(L \cup R)_\alpha$ is distinct, $y_\alpha \notin \text{Im}(L \cup R)_\alpha$, and the normalization is given by $\mathcal{N}_2 \equiv N_b^{\ell+r+1} \prod_\alpha (N_\alpha - \ell - r)$. The application of $\tilde{\Pi}^{\mathcal{I}(W_{abc}^R)}$ gives,

$$\frac{1}{\sqrt{\mathcal{N}_3}} \sum_{\substack{z_\ell, z_r, z_b \\ x_a x_b x_c \notin \text{Dom}(L \cup R)}} |x_a x_b x_c\rangle_A |L_{ab}^{z_\ell}\rangle_{L_{ab}} |L_{bc}^{z_\ell}\rangle_{L_{bc}} |R_{ab}^{z_r} \cup (x_a x_b, y_a z_b)\rangle_{R_{ab}} |R_{bc}^{z_r} \cup (z_b x_c, y_b y_c)\rangle_{R_{bc}}, \quad (\text{D.67})$$

where $\mathcal{N}_3 = N_b^{\ell+r+1}(N_{abc} - \ell - r)^2 / \prod_\alpha (N_\alpha - \ell - r)$. The application of W_{ab} gives,

$$\sqrt{\frac{N_{ab} - \ell - r}{\mathcal{N}_3}} \sum_{\substack{z_\ell, z_r, z_b \\ x_c}} |y_a z_b x_c\rangle_A |L_{ab}^{z_\ell}\rangle_{L_{ab}} |L_{bc}^{z_\ell}\rangle_{L_{bc}} |R_{ab}^{z_r}\rangle_{R_{ab}} |R_{bc}^{z_r} \cup (z_b x_c, y_b y_c)\rangle_{R_{bc}}, \quad (D.68)$$

where the sum over x_c is unconstrained because the application of $W_{ab}^{R, \dagger}$ enforces that $x_a x_b \notin \text{Dom}(L_{ab} \cup R_{ab})$, which implies that $x_a x_b x_c \notin \text{Dom}(L \cup R)$. The application of W_{bc} then gives,

$$\sqrt{\frac{(N_{ab} - \ell - r)(N_{bc} - \ell - r)}{\mathcal{N}_3}} \sum_{z_\ell, z_r} |y_a y_b y_c\rangle_A |L_{ab}^{z_\ell}\rangle_{L_{ab}} |L_{bc}^{z_\ell}\rangle_{L_{bc}} |R_{ab}^{z_r}\rangle_{R_{ab}} |R_{bc}^{z_r}\rangle_{R_{bc}}. \quad (D.69)$$

The state is invariant under the final projection Π^{paired} . Applying **Compress** to the state yields the state in Eq. (D.58) up to a normalization difference,

$$\left| \sqrt{\frac{(N_{ab} - \ell - r)(N_{bc} - \ell - r) \prod_\alpha (N_\alpha - \ell - r)}{N_b(N - \ell - r)^2}} - \sqrt{\frac{\prod_\alpha (N_\alpha - \ell - r)}{(N_{abc} - \ell - r)}} \right| \leq \frac{\ell + r}{N}, \quad (D.70)$$

where the first inequality holds for $\ell + r \leq 2N_{abc}$.

Note that both $\text{Compress}^\dagger \cdot \overline{W_{abc}} \cdot \Pi^{\text{locbij}} \cdot \text{Compress}$ and $\overline{W_{bc} W_{ab}} \cdot \Pi^{\text{paired}}$ are block diagonal in ℓ and r , as well as between the two classes of states considered in the above analysis. Thus, the spectral norm of the difference of the two operators is given by the maximum spectral norm of the difference within each block. From the above analysis, the maximum is achieved for the first class of states, at $\ell + r = t - 1$. The spectral norm is thus bounded by

$$\left\| \text{Compress}^\dagger \cdot \overline{W_{abc}} \cdot \Pi^{\text{locbij}} \cdot \text{Compress} \cdot \Pi^{\leq t-1} - \overline{W_{bc} W_{ab}} \cdot \Pi^{\text{paired}} \cdot \Pi^{\leq t-1} \right\|_\infty \leq \frac{(t-1)}{N_{ab}} + \frac{(t-1)}{N_{bc}},$$

where $\Pi^{\leq t-1}$ restricts to relation state register lengths $\ell + r \leq t - 1$. We have,

$$\begin{aligned} & \left\| \text{Compress}^\dagger |\mathcal{A}_t^{W'_{abc}, \mathcal{D}}\rangle - |\mathcal{A}_t^{(W_{bc} W_{ab})', \mathcal{D}}\rangle \right\|_2 \\ & \leq \left\| \text{Compress}^\dagger |\mathcal{A}_{t-1}^{W'_{abc}, \mathcal{D}}\rangle - |\mathcal{A}_{t-1}^{(W_{bc} W_{ab})', \mathcal{D}}\rangle \right\|_2 \\ & \quad + \left\| \text{Compress}^\dagger \cdot \overline{W_{abc}} \cdot \Pi^{\text{locbij}} \cdot \text{Compress} \cdot \Pi^{\leq t-1} - (W_{bc} W_{ab})' \cdot \Pi^{\text{paired}} \cdot \Pi^{\leq t-1} \right\|_\infty \\ & \leq \text{TD}_{t-1} + (t-1)/N_{ab} + (t-1)/N_{bc} \end{aligned}$$

as claimed. This completes our proof of step 2.

D.1.5 Twirled projected $W_{bc} W_{ab}$ is indistinguishable from twirled $V_{bc} V_{ab}$

Our proof of step 4 follows quickly from the results of steps 1-3. We use that W_{bc} and W_{ab} are restrictions of V_{bc} and V_{ab} to write,

$$(W_{bc} W_{ab})' = \Pi^{\text{paired}} \cdot V_{bc} \cdot \Pi^{\mathcal{D}(W_{bc})} \cdot V_{ab} \cdot \Pi^{\mathcal{D}(W_{bc})} \cdot \tilde{\Pi}^{\mathcal{D}(W_{abc})} \cdot \tilde{\Pi}^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \quad (D.71)$$

$$(W_{ab}^\dagger W_{bc}^\dagger)' = \Pi^{\text{paired}} \cdot V_{ab}^\dagger \cdot \Pi^{\mathcal{I}(W_{ab})} \cdot V_{bc}^\dagger \cdot \Pi^{\mathcal{I}(W_{bc})} \cdot \tilde{\Pi}^{\mathcal{D}(W_{abc}^\dagger)} \cdot \tilde{\Pi}^{\notin \text{Im} \rightarrow \notin \text{locIm}} \quad (D.72)$$

$$(\overline{W_{bc}} \overline{W_{ab}})' = \Pi^{\text{paired}} \cdot \overline{V_{bc}} \cdot \Pi^{\mathcal{D}(\overline{W_{bc}})} \cdot \overline{V_{ab}} \cdot \Pi^{\mathcal{D}(\overline{W_{bc}})} \cdot \tilde{\Pi}^{\mathcal{D}(\overline{W_{abc}})} \cdot \tilde{\Pi}^{\notin \text{Dom} \rightarrow \notin \text{locDom}} \quad (D.73)$$

$$(\overline{W_{ab}^\dagger} \overline{W_{bc}^\dagger})' = \Pi^{\text{paired}} \cdot \overline{V_{ab}^\dagger} \cdot \Pi^{\mathcal{I}(\overline{W_{ab}})} \cdot \overline{V_{bc}^\dagger} \cdot \Pi^{\mathcal{I}(\overline{W_{bc}})} \cdot \tilde{\Pi}^{\mathcal{D}(\overline{W_{abc}^\dagger})} \cdot \tilde{\Pi}^{\notin \text{Im} \rightarrow \notin \text{locIm}} \quad (D.74)$$

Therefore, the state $|\mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}}\rangle$ differs from the state $|\mathcal{A}_t^{V_{bc}V_{ab}, \mathcal{D}}\rangle$ solely by the insertion of projectors throughout the time evolution.

From Eq. (B.18) and the sequential gentle measurement lemma (Lemma 10), the difference between the two states is bounded as,

$$\|\rho^{(3)} - \rho^{(4)}\|_1 \leq 2 \left\| |\mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}}\rangle - |\mathcal{A}_t^{V_{bc}V_{ab}, \mathcal{D}}\rangle \right\|_2 \leq 2t \sqrt{1 - \langle \mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}} | \mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}} \rangle}. \quad (\text{D.75})$$

From our proofs of step 2 and step 3, we have that

$$\begin{aligned} \text{TD} \left(|\mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}}\rangle \langle \mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}}|, \text{Compress}^\dagger |\mathcal{A}_t^{W_{abc}, \mathcal{D}}\rangle \langle \mathcal{A}_t^{W_{abc}, \mathcal{D}}| \text{Compress} \right) \\ \leq \frac{17t^2}{N_{abc}^{1/8}} + \frac{7t^{3/2}}{(\min_\alpha N_\alpha)^{1/2}} + \frac{2t^2}{N_{ab}} + \frac{2t^2}{N_{bc}}. \end{aligned} \quad (\text{D.76})$$

Meanwhile, from Lemma 9.3 of Ref. [42] [see in particular Eqs. (9.58), (9.59)], we have

$$\text{TD} \left(|\mathcal{A}_t^{W_{abc}, \mathcal{D}}\rangle \langle \mathcal{A}_t^{W_{abc}, \mathcal{D}}|, \text{cQ} \cdot |\mathcal{A}_t^{V_{abc}, \mathcal{D}}\rangle \langle \mathcal{A}_t^{V_{abc}, \mathcal{D}}| \cdot \text{cQ} \right) \leq \frac{9t}{N_{abc}^{1/8}}. \quad (\text{D.77})$$

The state $\text{cQ} \cdot |\mathcal{A}_t^{V_{abc}, \mathcal{D}}\rangle$ is obtained from solely unitary time-evolution, and thus has norm one. Combining the two above equations therefore yields,

$$\langle \mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}} | \mathcal{A}_t^{(W_{bc}W_{ab})', \mathcal{D}} \rangle \geq 1 - \left(\frac{17t^2}{N_{abc}^{1/8}} + \frac{7t^{3/2}}{(\min_\alpha N_\alpha)^{1/2}} + \frac{2t^2}{N_{ab}} + \frac{2t^2}{N_{bc}} \right) - \frac{9t}{N_{abc}^{1/8}} \quad (\text{D.78})$$

which, from Eq. (D.75), implies that

$$\begin{aligned} \|\rho^{(3)} - \rho^{(4)}\|_1 &\leq 2t \sqrt{\frac{17t^2}{N_{abc}^{1/8}} + \frac{7t^{3/2}}{(\min_\alpha N_\alpha)^{1/2}} + \frac{2t^2}{N_{ab}} + \frac{2t^2}{N_{bc}} + \frac{9t}{N_{abc}^{1/8}}} \\ &\leq \frac{2\sqrt{17}t^2}{N_{abc}^{1/16}} + \frac{2\sqrt{7}t^{7/4}}{(\min_\alpha N_\alpha)^{1/4}} + \frac{2\sqrt{2}t^2}{N_{ab}^{1/2}} + \frac{2\sqrt{2}t^2}{N_{bc}^{1/2}} + \frac{6t^{3/2}}{N_{abc}^{1/16}}, \end{aligned} \quad (\text{D.79})$$

where in the second line we use that the square root is subadditive. This completes the proof.

D.2 Proof of Theorems 5 and 6

Our proof of Theorems 5 and 6 follow immediately from Lemma 1. The extension of Theorem 5 to the blocked fast scrambling circuit follows immediately from Lemma 2.

Proof of Theorem 5. Iterating Lemma 1 $m = n/\xi$ times, we can replace the two-layer circuit with a Haar-random unitary up to a measurable error $(n/\xi)(\varepsilon/n) + \mathcal{O}(nk^2/2^{(3/16)\xi\xi})$. The first term is less than $\varepsilon/2$ whenever $\xi \geq 2$. The second term is less than $\varepsilon/2$ if $\xi \geq \frac{16}{3} \log_2(nk^2/\varepsilon) + \mathcal{O}(1)$. This completes the proof. $\square$

Remark. The proof immediately extends to a modified blocked fast scrambling circuit in Section 4.4 of the main text, in which we replace the exact n -qubit unitary 2-designs with blocked fast scrambling circuits composed of small strong $\frac{\varepsilon_2}{n}$ -approximate unitary 2-designs. From Lemma 2, this blocked fast scrambling circuit forms a strong ε_2 -approximate unitary 2-design when $\xi \geq \log_2(5n/\varepsilon_2)$. Iterating Lemma 1 $m = n/\xi$ times, we can replace the two-layer circuit with a Haar-random unitary up to a measurable error $(n/\xi)(\varepsilon/n) + \mathcal{O}(nk^2/2^{(3/16)\xi\xi}) + \mathcal{O}(nk^{5/8}\varepsilon_2^{1/8})$. The first term is less than $\varepsilon/3$ whenever $\xi \geq 3$. The second term is less than $\varepsilon/3$ if $\xi \geq \frac{16}{3} \log_2(nk^2/\varepsilon) + \mathcal{O}(1)$. The third term is less than $\varepsilon/3$ if $\varepsilon_2 = \mathcal{O}(\varepsilon^8/n^8k^5)$, which requires $\xi \geq \log_2(n^9k^5/\varepsilon^8) + \mathcal{O}(1) = \mathcal{O}(\log nk/\varepsilon)$. $\square$

Proof of Theorem 6. By assumption, each individual small PRU in the two-layer circuit is indistinguishable from a small Haar-random unitary by any poly n -time quantum experiment. Hence, following identical steps to the proof of Theorem 2 in Ref. [36], the scrambled two-layer circuit of small PRUs is indistinguishable from a scrambled two-layer circuit of small Haar-random unitaries. From Theorem 6, the latter ensemble forms an ε -approximate strong unitary k -design for any $k^2/\varepsilon \leq \mathcal{O}(2^\xi/n)$. Setting $\xi = \omega(\log n)$ yields a design for any $k, 1/\varepsilon = \text{poly } n$. Hence, from the definition of strong approximate unitary k -designs, the scrambled two-layer circuit of small Haar-random unitaries is indistinguishable from a Haar-random unitary by any poly n -time quantum experiment. $\square$

D.3 Proof of Theorems 1 and 2

The combination of Theorem 3 and Theorem 5 immediately yield Theorem 1 on the circuit depth of strong unitary designs.

Proof of Theorem 1. The second and third statements of Theorem 1 follows immediately from Theorem 3 and the circuit depth required to implement the LRFC ensemble with $2k$ -wise independent functions [39]. The first statement of Theorem 1 follows from Theorem 5 and Lemma 3. $\square$

The combination of Theorem 4 and Theorem 6 immediately yield Theorem 2 on the circuit depth of strong pseudorandom unitaries.

Proof of Theorem 2. The first statement of Theorem 2 follows immediately from Theorem 4 and the circuit depth required to implement the LRFC ensemble with pseudorandom functions [36]. The second statement of Theorem 2 follows from Theorem 4 and Theorem 6. The derivation of the circuit depth is described in the main text. $\square$

E Ancilla-free pseudorandom unitaries

In this section, we give the first constructions of ancilla-free (strong) pseudorandom unitaries. Our main cryptographic building block will be pseudorandom functions [77] computable in the complexity class “logspace-uniform TC^1 .” A function is computable in logspace-uniform TC^1 if (1) it is computable by a family of $O(\log n)$ -depth circuits with large fan-in threshold gates and (2) this family of circuits is output by a logspace Turing machine on the input 1^n . Crucially, it is known that such PRFs exist under the LWE assumption [78], and that this construction is post-quantum secure [74].

Our main technical result about ancilla-free computation is as follows.

Theorem 12. *Let $f : \{0, 1\}^n \rightarrow \mathbb{Z}_q^m$ be any logspace-uniform TC^1 -computable function, where $q = O(1)$. Then, there is a $\text{poly}(n, m)$ -size reversible circuit implementing the permutation*

$$(x, y, a) \mapsto (x, y + f(x) \pmod{q}, a), \quad (\text{E.1})$$

where a denotes an arbitrary setting of the ancilla register.

By combining Theorem 12 with the LRFC construction of Section 4.1, obtain the following intermediate result: a PRU family with an efficient ancilla-free implementation of the unitary $U_k \otimes \text{Id}$ (rather than U_k alone). We call such PRUs “ancilla-independent.”

Theorem 13. *Assuming polynomially secure (respectively, sub-exponentially secure) post-quantum PRFs computable in logspace-uniform TC^1 , there exist polynomially secure (respectively, sub-exponentially secure) ancilla-independent strong PRUs.*

Finally, combining Theorem 14 with the strong PRU gluing lemma (and its corollary, Theorem 6), we obtain ancilla-free strong PRUs. This approach works because when gluing ancilla-independent PRU implementations, one can use the ancilla register of one unitary as part of the *input* register of another unitary. In the end, the resulting glued circuit will compute a PRU on its entire domain.

Theorem 14. *Assuming post-quantum PRFs computable in TC^1 , there exist ancilla-free strong PRUs. Moreover, assuming sub-exponentially secure post-quantum PRFs computable in TC^1 , there exist ancilla-free strong PRUs computable in depth $\text{poly}(\log n)$ with all-to-all circuits.*

Since logspace-uniform TC^1 -computable PRFs are known under the standard LWE assumption [78], we obtain instantiations of our results under LWE.

Corollary 2. *Assuming the post-quantum hardness of LWE, there exist ancilla-free PRUs. Assuming the sub-exponential post-quantum hardness of LWE, there exist ancilla-free strong PRUs computable in depth $\text{poly}(\log n)$ with all-to-all circuits.*

The rest of this section is devoted to proving Theorems 12 to 14.

E.1 Ancilla-preserving reversible computation of functions

Let $f : \mathcal{X} \rightarrow \mathbb{Z}_q$ denote a function with $q = O(1)$. We study different “ancilla-respecting” reversible circuit implementations of the computation

$$|x, y\rangle \mapsto |x, y + f(x) \pmod{q}\rangle. \quad (\text{E.2})$$

We will use bra-ket notation to describe the action of these reversible circuits, but we note that they only use Toffoli gates and thus correspond to classical reversible computation, i.e., permutations.

Our reversible circuits will operate on four registers:

- Let $\mathbf{X}$ denote an n -qubit register whose standard basis states correspond to $\mathcal{X}$.
- Let $\mathbf{Y}$ denote an output register with standard basis in bijection with $\mathbb{Z}_q$.
- Let $\mathbf{A}$ denote an ℓ -qubit *trusted* ancilla register. This means that (at least initially), our computations will rely on the ancilla being initialized to the $|0^\ell\rangle$ state.
- Let $\mathbf{W}$ denote an *untrusted* (or catalytic) ancilla register of size $\text{poly } n$.

Definition 43. *We say that a reversible circuit C acting on $(\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{W})$ is an ancilla-preserving implementation of f with trusted space $\mathbf{A}$ and untrusted space $\mathbf{W}$ if it maps*

$$|x, y, a, w\rangle \mapsto |x, y + g(x, a, w), a, w\rangle, \quad (\text{E.3})$$

where g is any function that agrees with f when $a = 0$. That is, $g(x, 0^\ell, w) = f(x)$, but otherwise $g(x, a, w)$ may be arbitrary.

Here, “ancilla-preserving” refers to the fact that C never changes the values stored in the $\mathbf{A}$ and $\mathbf{W}$ register, regardless of what they are initialized to. We say that $\mathbf{A}$ is “trusted space”, since $g(x, a, w)$ is only guaranteed to compute the output $f(x)$ correctly when $\mathbf{A}$ is initialized properly to 0^ℓ . $\mathbf{W}$ is “untrusted” because we require that $g(x, 0, w)$ correctly compute $f(x)$ for any choice of w .

As we will show, the following lemma is an easy consequence of recent work on logspace catalytic classical computation [79, 101].

Lemma 31. *For every function $f : \{0, 1\}^n \rightarrow \mathbb{Z}_q$ computable in logspace-uniform TC^1 , there is a $\text{poly}(n)$ -size ancilla-preserving reversible circuit C that implements f with an $\ell = O(\log n)$ -size trusted ancilla space $\mathcal{A}$ and a $\text{poly}(n)$ -size untrusted ancilla space $\mathcal{W}$.*

Proof. According to [79], for $f : \{0, 1\}^n \rightarrow \mathbb{Z}_q$ computable in logspace-uniform TC^1 , there is a $\text{poly}(n)$ -size reversible circuit C' that maps

$$|x, y, a, w\rangle \mapsto |p(x, y, a, w)\rangle \quad (\text{E.4})$$

where $p(x, 0, 0^\ell, w) = (x', f(x), a', w)$, but on other inputs, $p(x, y, a, w)$ may be arbitrary. Given such a circuit C' , we can implement C satisfying Definition 43, where the trusted ancilla is now size $\ell + O(1)$, using standard techniques from reversible computation:

1. On input $|x, y, a, w\rangle$, parse a as (y', a') , where $y' \in \mathbb{Z}_q$ and a' is length ℓ . Run C' on (x, y', a', w) . This step does not affect the y register, and the effect on $|x, a, w\rangle$ is:

$$|x, a = (y', a'), w\rangle \mapsto |p(x, y', a', w)\rangle. \quad (\text{E.5})$$

2. Parse $p(x, y', a', w)$ as $p(x, y', a', w) = (x_{\text{out}}, y'_{\text{out}}, a'_{\text{out}}, w_{\text{out}})$. Add the value of y'_{out} onto $|y\rangle$.
3. Apply the inverse of C' .

The result is that we have performed the map

$$|x, y, a, w\rangle \mapsto |x, y + y'_{\text{out}}, a, w\rangle, \quad (\text{E.6})$$

where y'_{out} is a function of $(x, a = (y', a'), w)$, which equals $f(x)$ when $a = (y', a') = (0, 0^\ell)$. $\square$

We will now define two further restricted classes of ancilla-preserving implementations, and we will show how to compile circuits satisfying Definition 43 into circuits satisfying these more restricted notions.

Recall that an ancilla-preserving implementation of f is a circuit C that maps (x, y, a, w) to $(x, y + g(x, a, w), a, w)$, where g is *any function* that agrees with f when $a = 0$. We now define two more restrictive notions where we impose further requirements on g .

Definition 44 (Stronger versions of ancilla-preserving implementations). *Let C be an ancilla-preserving implementation of f , and let g be as in Definition 43. Then we say that C is:*

- an **ancilla-controlled** implementation of f if $g(x, a, w) = f(x) \cdot \chi_{a=0^\ell}$ and is 0 otherwise.
- an **ancilla-independent** implementation of f if $g(x, a, w) = f(x)$ for all a, w .

E.1.1 Converting ancilla-preserving to ancilla-controlled

Next, we show that an ancilla-preserving implementation of a function f ,

$$|x, y, a, w\rangle \mapsto |x, y + g(x, a, w), a, w\rangle,$$

can be efficiently converted into an ancilla-controlled implementation of f ,

$$|x, y, a, w'\rangle \mapsto |x, y + \chi_{a=0^\ell} \cdot f(x), a, w'\rangle,$$

where the trusted ancilla space $\mathcal{A}$ is unchanged and $\mathcal{W}' = \mathcal{W} \times \mathbb{Z}_q$.

Lemma 32. *Let $g(x, a, w)$ be any function such that $g(x, 0, w) = f(x)$ for all (x, w) . Then, if there is a circuit C implementing the map $|x, y, a, w\rangle \mapsto |x, y + g(x, a, w), a, w\rangle$, there is another circuit C' implementing the map $|x, y, a, w'\rangle \mapsto |x, y + \chi_{a=0^\ell} \cdot f(x), a, w'\rangle$.*

Moreover, the size and depth of C' is bounded in terms of C :

- $|C'| = O(|C|) + 2^{O(\ell)}$,⁹ and
- $\text{depth}(C') = O(\text{depth}(C)) + 2^{O(\ell)}$

Proof. Let us introduce a new register Q supported on states $|z\rangle$ for $z \in \mathbb{Z}_q$. Suppose we could implement the following maps:

$$O : |z\rangle_Q |x, y, a, w\rangle \mapsto |z\rangle_Q |x, y + z \cdot g(x, a, w), a, w\rangle \quad (\text{E.7})$$

$$W : |z\rangle_Q |x, y, a, w\rangle \mapsto |z - \chi_{a=0^\ell}\rangle_Q |x, y, a, w\rangle, \quad (\text{E.8})$$

where $\chi_{a=0^\ell}$ is the element $1 \in \mathbb{Z}_q$ if $a = 0^\ell$ and is $0 \in \mathbb{Z}_q$ otherwise. Since

$$WO : |z\rangle_Q |x, y, a, w\rangle \mapsto |z - \chi_{a=0^\ell}\rangle_Q |x, y + z \cdot g(x, a, w), a, w\rangle, \quad (\text{E.9})$$

$$W^\dagger O^\dagger : |z\rangle_Q |x, y, a, w\rangle \mapsto |z + \chi_{a=0^\ell}\rangle_Q |x, y - z \cdot g(x, a, w), a, w\rangle, \quad (\text{E.10})$$

we can compose these operations to obtain the desired ancilla-controlled implementation:

$$W^\dagger O^\dagger WO : |z\rangle_Q |x, y, a, w\rangle \mapsto |z\rangle_Q |x, y + z \cdot g(x, a, w) - (z - \chi_{a=0^\ell}) \cdot g(x, a, w), a, w\rangle \quad (\text{E.11})$$

$$= |z\rangle_Q |x, y + \chi_{a=0^\ell} f(x), a, w\rangle. \quad (\text{E.12})$$

In the last equality, we used the fact that g satisfies $\chi_{a=0^\ell} \cdot f(x) = \chi_{a=0^\ell} \cdot g(x, a, w)$. It remains to show how to implement O and W .

Implementing O . For $i \in \mathbb{Z}_q$ let $C^{(i)}$ be the circuit that applies C controlled on element z in the Q register satisfying $z \leq i$. Given an implementation of C , we can implement $C^{(i)}$ by replacing each gate g with the gate $g^{(i)}$, which implements g controlled on the element z in the Q register satisfying $z \leq i$. Since $q = O(1)$, this only requires a constant number of additional elementary gates. Then O can be implemented as $O = C^{(q)} C^{(q-1)} \dots C^{(1)}$.

Implementing W . W is an $\ell + O(1)$ qubit unitary, so it has a $2^{O(\ell)}$ -size ancilla-free implementation. $\square$

E.1.2 Converting ancilla-controlled to ancilla-independent

Finally, we give a simple transformation from ancilla-controlled implementations to ancilla-independent implementations of f . The transformation preserves the ancilla registers but has a size and depth blowup of 2^ℓ .

Lemma 33. *Let C be an ancilla-controlled implementation of f , i.e., it implements the map $|x, y, a, w\rangle \mapsto |x, y + \chi_{a=0^\ell} \cdot f(x), a, w\rangle$. There is an ancilla-independent implementation of f , i.e., a circuit C' that maps $|x, y, a, w\rangle \mapsto |x, y + f(x), a, w\rangle$, with size $\Theta(2^\ell \cdot |C|)$ and depth $\Theta(2^\ell \cdot \text{depth}(C))$.*

Proof. Let $R := \sum_{a \in \mathcal{A}} |a+1\rangle\langle a|$ be the increment operator acting on A . Then we claim that $C' = (R \cdot C)^{2^\ell}$ is an ancilla-independent implementation of f . This works because $R \cdot C$ maps $|x, y, a, w\rangle$ to

$$|x, y + \chi_{a=0^\ell} \cdot f(x), a + 1, w\rangle, \quad (\text{E.13})$$

⁹We believe it should be possible to improve the $2^{O(\ell)}$ dependence to $\text{poly}(\ell)$, but due to a subsequent $2^{O(\ell)}$ overhead, it makes no difference for our purposes.

so repeating this 2^ℓ times maps $|x, y, a, w\rangle$ to

$$|x, y + \sum_{i \in \mathcal{A}} \chi_{(a+i)=0^\ell} \cdot f(x), a, w\rangle = |x, y + f(x), a, w\rangle. \quad (\text{E.14})$$

□

E.1.3 Completing the proof of Theorem 12

By combining Lemmas 31 to 33, we obtain Theorem 12 in the special case of $m = 1$. That is, we have an ancilla-free implementation of any logspace-uniform TC^1 function $f : \{0, 1\}^n \rightarrow \mathbb{Z}_q$ with size poly n . To complete the proof of Theorem 12, it suffices to extend this to $f : \{0, 1\}^n \rightarrow \mathbb{Z}_q$ with $m > 1$. However, this turns out to be simple: compute each output symbol one-at-a-time in sequence (using a different output register for each symbol). It is clear that the ancilla-independent implementations compose, completing the proof.

E.2 Constructing ancilla-independent PRUs

In this section, we proceed from studying ancilla-independent implementations of *functions* to studying ancilla-independent implementations of *unitaries*. We say that C is an ancilla-independent implementation of a unitary U (acting on Hilbert space X) if C implements the map $U_{\mathsf{X}} \otimes \text{Id}_{\mathsf{A}}$.

Definition 45 (Ancilla-independent PRU). *We say that a PRU family $\{U_k\}$ is an ancilla-independent PRU family if for every key k , there is a polynomial-size quantum circuit C_k that is an ancilla-independent implementation of U_k . Moreover, we require that C_k is efficiently computable from k .*

Our goal in this section is to prove the following result

Theorem 15. *Assume the existence of a post-quantum PRF that has a polynomial-size ancilla-independent implementation. Then, there exists an ancilla-independent PRU family. Moreover, if the PRF family is sub-exponentially secure, so is the PRU.*

To prove this theorem, we wish to make use of the LRFC construction (Theorem 4). To do so, we must first give an ancilla-independent implementation of a pseudorandom *ternary phase oracle*. This is achieved via the following lemma.

Lemma 34. *Let $f : \{0, 1\}^n \rightarrow \mathbb{Z}_q$ be a function with $q = O(1)$. Given an ancilla-independent implementation C of $|x, y\rangle \mapsto |x, y + f(x)\rangle$, there is an ancilla-independent implementation C' of $|x\rangle \mapsto \omega_q^{f(x)} |x\rangle$. Moreover, we have that $|C'| = O(|C|)$ and $\text{depth}(C') = O(\text{depth}(C))$.*

Proof. Let C be an ancilla-independent circuit implementation of $|x\rangle |y\rangle \mapsto |x\rangle |y + f(x)\rangle$ with ancilla register A . Then, to implement $|x\rangle \mapsto \omega_q^{f(x)} |x\rangle$, we use an ancilla register $\mathsf{A}' = \mathsf{A} \otimes \mathsf{Y}$. We then implement the map

$$O = (\text{Id}_{\mathsf{X}, \mathsf{A}} \otimes F_q) C (\text{Id}_{\mathsf{X}, \mathsf{A}} \otimes F_q^\dagger) \quad (\text{E.15})$$

where F_q denotes the q -ary Fourier transform on register Y . This is equivalent to the map

$$|x, y, a\rangle \mapsto |x\rangle \otimes \frac{1}{\sqrt{q}} F_q \sum_{z \in \mathbb{F}_q} \omega_q^{-z \cdot y} |z + f(x)\rangle \otimes |a\rangle = \omega_q^{y \cdot f(x)} |x, y, a\rangle. \quad (\text{E.16})$$

Finally, we observe that, letting R_{Y} denote the increment operator on Y ,

$$R_{\mathsf{Y}} \cdot O^\dagger \cdot R_{\mathsf{Y}}^\dagger \cdot O = \sum_{x, y, a} \omega_q^{f(x)} |x, y, a\rangle \langle x, y, a|, \quad (\text{E.17})$$

yielding the desired ancilla-independent implementation of $|x\rangle \mapsto \omega_q^{f(x)} |x\rangle$. $\square$

Proofs of Theorems 13 and 15. We now prove Theorem 15 by appealing to the LRFC construction of Theorem 4. That is, unitaries in the PRU family have the form

$$U = D \cdot S_R \cdot F \cdot S_L \cdot C. \quad (\text{E.18})$$

where D and C are 2-designs, F is a pseudorandom ternary phase oracle, and S_L, S_R are pseudorandom bit-flip permutations $|x_L, x_R\rangle \mapsto |x_L \oplus f(x_R), x_R\rangle$ and $|x_L, x_R\rangle \mapsto |x_L, x_R \oplus g(x_L)\rangle$. By Theorem 12 and Lemma 34, we know that there exist ancilla-independent pseudorandom instantiations of S_L, S_R, F . Moreover, it is known that approximate 2-designs have efficient ancilla-independent (even ancilla-free) implementations [102]. Thus, by invoking Theorem 4, we obtain Theorem 15. Moreover, by combining Theorem 15 with Theorem 12, we immediately obtain Theorem 13. $\square$

E.3 Constructing ancilla-free PRUs

Finally, we prove Theorem 14 by combining Theorem 13 with Theorem 6. Recall that Theorem 6 states that the following construction yields a strong PRU when its building block unitaries are instantiated with strong PRUs:

- Apply a 2-design.
- Apply two brickwork layers of building block unitary gates.
- Apply an independent 2-design.

We will use this construction *twice* to prove Theorem 14. First, we instantiate a high-depth version of the construction, where:

- The building block unitaries act on $2 \cdot n^\epsilon$ qubits.
- The input register is divided into $n^{1-\epsilon}$ blocks of n^ϵ qubits.
- Given an ancilla-independent implementation of the building block unitary using $n^{\alpha-\epsilon}$ ancilla qubits (for some constant $\alpha > 0$), we construct a circuit from the glued unitary in which each building block unitary uses adjacent registers as its ancilla space.

This construction results in a quantum circuit implementation of a distribution of unitaries that is pseudorandom on its entire domain by the gluing lemma. However, its depth is large, especially because all gates in the “brickwork layers” must now be concatenated sequentially due to the circuit implementations having overlapping registers. Nevertheless, this yields the high-depth case of Theorem 14. Moreover, if the initial ancilla-independent PRU family is sub-exponentially secure, then so is the ancilla-free PRU family.

Finally, under this sub-exponential security assumption, we can plug our ancilla-free PRU back into Theorem 6, using block size $\text{poly}(\log n)$, yielding an ancilla-free PRU family of depth $\text{poly}(\log n)$.

F Analysis of the mixed Haar twirl

In this Appendix, we provide further details on our analysis of the mixed Haar twirl. This completes our proof of the additive-to-relative error translation result (Lemma 7) for strong unitary designs. We also provide several additional results on the mixed Haar twirl not used in this work.

F.1 Reformulating the mixed Haar twirl

In this section, we provide the full details of the derivation of our reformulation of the mixed Haar twirl [Eq. (A.19)], which was used to prove Lemma 7 in Appendix A.2.3. Our derivation uses only basic properties of the partially transposed permutations. Nonetheless, it requires several detailed steps to formally construct the partial isometries $\tilde{I}_\ell$ and prove their essential properties.

For the ease of the reader, we structure this section in a pedagogical format. We first motivate and introduce the relevant objects one-by-one. We then provide a series of short proofs of their key properties, which leads to our reformulated expression for the mixed Haar twirl. We hope that our analysis may be useful in future works on the mixed Haar twirl, even beyond the context of strong unitary designs.

F.1.1 The partially transposed permutations (PTPs)

As previously discussed, we can write the exact expression for the mixed Haar twirl in terms of the partially transposed permutations (PTPs),

$$\Phi_H^{(p,q)}(X) = \sum_{\sigma, \tau \in S_k^\Gamma} \widetilde{\mathcal{W}}_{\mathbf{g}_{\sigma, \tau}} \cdot \text{tr}(X \sigma^\dagger) \cdot \tau, \quad (\text{F.1})$$

where $\sigma = \pi^\Gamma$ and $\tau = (\tilde{\pi})^\Gamma$ correspond to the original permutation operators with the partial transpose Γ applied on the right q copies. The summation is over all $(p+q)!$ possible PTPs for both σ and τ . We also let $\widetilde{\text{Wg}}_{\sigma,\tau} \equiv \text{Wg}_{\pi,\tilde{\pi}}$ denote the analog of the Weingarten matrix elements for the PTPs.

Let us begin by reviewing a few basic facts regarding the PTPs. We denote a *mixed tensor unitary* (MTU) acting on $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ as,

$$\mathcal{U}_q^p \equiv U^{\otimes p} \otimes U^{*, \otimes q}, \quad (\text{F.2})$$

for any $U \in U(D)$ with $D = 2^n$. We can draw each PTP using tensor network notation,

$$\sigma = \begin{array}{c} \text{diagram 1} \end{array} = \begin{array}{c} \text{diagram 2} \end{array} \Gamma, \quad (\text{F.3})$$

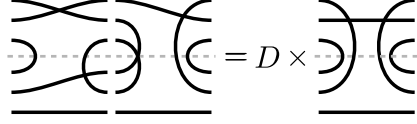
where the “left” p copies are depicted above the dashed line of the diagram, and the “right” q copies are depicted below the dashed line. One can easily verify that any PTP commutes with any MTU,

$$\sigma \mathcal{U}_q^p = \begin{array}{c} \text{Diagram 1} \end{array} = \begin{array}{c} \text{Diagram 2} \end{array} = \begin{array}{c} \text{Diagram 3} \end{array} = \mathcal{U}_q^p \sigma. \quad (\text{F.4})$$

This is especially clear in the diagrammatic depiction of the PTP. Each U in the MTU either slides from the right to left of the PTP, or cancels with a U^* acting on a paired leg of the PTP. The PTPs form a generating set for the commutant of the MTUs, i.e. any operator that commutes with every MTU can be written as a sum of PTPs¹⁰.

¹⁰An operator commutes with all MTUs if and only if its partial transpose commutes with all tensor power unitaries $U^{\otimes(p+q)}$. The statement that the PTPs form the commutant of the MTUs then follows from the well-known fact that the set of permutations $\pi \in S_k$ generates the commutant of the set of tensor power unitaries. This implies that the partial transpose of the aforementioned operator can be written as a sum of permutations, and hence the operator can be written as a sum of PTPs.

The PTPs form a representation of the so-called “walled Brauer algebra”, $\mathcal{B}_{p,q}^D$. The multiplication rules of the algebra can be computed by connecting the legs of the associated PTPs. For example,

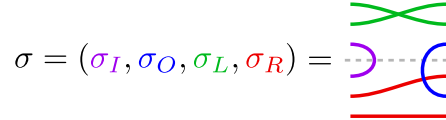


$$\text{Diagram} = D \times \text{Diagram} \quad (\text{F.5})$$

where each closed loop contributes a factor of the Hilbert space dimension D . The representation is *faithful* whenever $D \geq p + q$, i.e. a linear combination of PTPs is equal to zero, $\sum_{\sigma} c_{\sigma} \sigma = 0$, if and only if each coefficient is zero¹¹, $c_{\sigma} = 0$.

F.1.2 Constructing complete orthogonal projectors from the PTPs

Having defined the PTPs, we now begin our own analysis. Let us first introduce some useful notation. We can uniquely label each PTP by a set of four quantities, depicted as follows,



$$\sigma = (\sigma_I, \sigma_O, \sigma_L, \sigma_R) = \text{Diagram} \quad (\text{F.6})$$

The first quantity, σ_I , specifies the input legs that are paired under σ (purple). We term the number of pairs in σ_I the *size* of the PTP, and denote it as $\ell_{\sigma} = |\sigma_I|$, where $|\cdot|$ counts the number of pairs. We have $0 \leq \ell_{\sigma} \leq \min(p, q)$. The second quantity, σ_O , specifies the output legs that are paired under σ (blue). The number of output pairs is also ℓ_{σ} , equal to the number of input pairs. The third quantity, $\sigma_L \in S_{p-\ell_{\sigma}}$, specifies a permutation acting on the remaining $p - \ell_{\sigma}$ legs on the left side (green). Similarly, the fourth quantity, $\sigma_R \in S_{q-\ell_{\sigma}}$, specifies a permutation acting on the remaining $q - \ell_{\sigma}$ legs on the right side (red).

The main aim of this section is to show that the PTPs naturally decompose the Hilbert space $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ into a tensor sum of orthogonal subspaces. Our derivation of this decomposition requires several steps. To begin, we note that a subset of the PTPs with $\sigma_L = \sigma_R = \mathbb{1}$ and $\sigma_I = \sigma_O \equiv \alpha$ (for any set of pairs α), are proportional to projectors. Namely, we have $\sigma^2 = D^{\ell_{\sigma}} \sigma$ for any such PTP where $\ell_{\sigma} = |\alpha|$. This allows us to define the “bare” projectors,

$$P_{\alpha} = \frac{1}{D^{|\alpha|}} (\alpha, \alpha, \mathbb{1}, \mathbb{1}). \quad (\text{F.7})$$

Each P_{α} projects onto the EPR state on each pair in α , and acts as the identity on copies not in α .

In general, the bare projectors are not orthogonal to one another. For example, whenever $\alpha \supset \beta$, the subspace defined by P_{α} is strictly contained within the subspace defined by P_{β} (i.e. $P_{\alpha} P_{\beta} = P_{\alpha}$). This fact can make working with the bare projectors somewhat inconvenient. To address this, we will need to orthogonalize the bare projectors.

We do so by introducing a new object: the *no-EPR projector*. For any subset β of the $p + q$ copies, we define the no-EPR projector, Π_{β}^{nE} , as the projector onto the subspace of the Hilbert space of β that is orthogonal to every EPR projector on β . That is, we let Π_{β}^{nE} project onto the orthogonal complement of $\{P_{\alpha} : \alpha \supseteq \beta\}$. In the special case when β contains every copy, we simply write Π^{nE} , which is the projector onto the orthogonal complement of $\{P_{\alpha} : \forall \alpha \neq \emptyset\}$. We will write down an

¹¹This follows from the well-known fact that the representation of the permutation group S_k on $\mathcal{H}^{\otimes k}$ is faithful when $D \geq k$. A linear combination of PTPs is equal to zero if and only if its partial transpose is equal to zero. Since the representation of the permutation group is faithful, this can be true only if every coefficient is equal to zero.

explicit expression for the no-EPR projector at the end of this subsection. For now, we simply note that the no-EPR projector can be written as a sum of PTPs supported on β , since it commutes with every MTP unitary and acts as the identity on $\bar{\beta}$.

We can use the no-EPR projector to (partially) remedy the non-orthogonality of the bare projectors. For each set of pairs α , we define the “nearly-orthogonal” projectors,

$$P_\alpha^{\text{nE}} = |E_\alpha\rangle\langle E_\alpha| \otimes \Pi_{\bar{\alpha}}^{\text{nE}} = \text{[Diagram]} \quad (\text{F.8})$$

where $|E_\alpha\rangle$ denotes the EPR state on all pairs in α . Here, the slash represents the no-EPR projector on $\bar{\alpha}$, and each diamond represents a factor of the inverse square root Hilbert space dimension, $1/\sqrt{D}$, arising from the normalization of $|E_\alpha\rangle$. By definition, the nearly-orthogonal projector projects onto all states in P_α that are not contained in any P_β for $\alpha \supset \beta$. We can also write $P_\alpha^{\text{nE}} = P_\alpha \Pi_{\bar{\alpha}}^{\text{nE}} = \Pi_{\bar{\alpha}}^{\text{nE}} P_\alpha$.

A simple argument shows that any two P_α^{nE} and P_β^{nE} are orthogonal whenever the size of α and β differ. We prove this in Appendix F.1.4.

Proposition 4 (Nearly-orthogonal projectors). *Two nearly-orthogonal projectors P_α^{nE} and P_β^{nE} are orthogonal, $P_\alpha^{\text{nE}} P_\beta^{\text{nE}} = 0$, if $|\alpha| \neq |\beta|$.*

However, the nearly-orthogonal projectors are *not* orthogonal to one another when $|\alpha| = |\beta|$.

To address this latter fact, we can define a final set of “orthogonal” projectors, $\tilde{P}_\alpha$. We do so via the Gram-Schmidt process. For each size $\ell = 0, \dots, \min(p, q)$, we consider any ordering, $\{\alpha_0, \alpha_1, \dots\}$, of the pairings α with size $|\alpha| = \ell$. We then proceed α -by- α through the ordering, and at each step define the orthogonal projector $\tilde{P}_\alpha$ as,

$$\tilde{P}_\alpha |\psi\rangle = \begin{cases} 1, & \text{if } |\psi\rangle \in \text{span}(\{P_{\alpha'}^{\text{nE}} : \alpha' \leq \alpha\}) \text{ and } |\psi\rangle \notin \text{span}(\{P_{\alpha'}^{\text{nE}} : \alpha' < \alpha\}) \\ 0, & \text{else} \end{cases} \quad (\text{F.9})$$

In the special case where $\alpha = \emptyset$ is the empty set, we have $\tilde{P}_\emptyset = \Pi^{\text{nE}}$. The projectors $\tilde{P}_\alpha$ are mutually orthogonal by definition. They are also complete, $\sum_\alpha \tilde{P}_\alpha = \mathbb{1}$, by definition. Finally, it will be convenient to also define the projector onto the *union* of all $\tilde{P}_\alpha$ of a given size $|\alpha| = \ell$. We term this the ℓ -EPR projector,

$$\tilde{P}_\ell = \sum_{\alpha: |\alpha|=\ell} \tilde{P}_\alpha. \quad (\text{F.10})$$

Unlike the individual orthogonal projectors $\tilde{P}_\alpha$, the projector $\tilde{P}_\ell$ is uniquely defined, independent of our ordering of the pairings α within each size ℓ .

We can now demonstrate several useful properties of the orthogonal projectors. We begin by proving (Appendix F.1.5) that the orthogonal projectors can be written as a sum of PTPs.

Proposition 5 (Orthogonal projectors). *Each projector $\tilde{P}_\alpha$ can be written as a sum of PTPs with either (i) size greater than $|\alpha|$, or (ii) size equal to $|\alpha|$ and $\alpha_I, \alpha_O \leq \alpha$ with respect to the ordering in Eq. (F.9).*

Intuitively, this follows because the Gram-Schmidt process constructs an orthogonal vector by taking a linear combination of the current vector and all vectors previous to it.

We also have the following useful fact (Appendix F.1.6).

Proposition 6 (The ℓ -EPR projector). *The projector $\tilde{P}_\ell$ commutes with every PTP.*

This does not apply to the individual orthogonal projectors $\tilde{P}_\alpha$.

We can also characterize the rank of each orthogonal subspace. To do so, for any p and q , we let

$$N_{\text{EPR}}^{(p,q)} = \text{rank} \left(\sum_{\alpha \neq \emptyset} P_\alpha \right), \quad (\text{F.11})$$

count the number of states on $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ that contain at least one EPR pair. That is, the number of states in the span of any non-trivial bare projector P_α . We then show (Appendix F.1.7),

Proposition 7 (Rank of the orthogonal projectors). *For any $D \geq p + q$. Each projector P_α^{nE} and $\tilde{P}_\alpha$ has rank $D^{p+q-2|\alpha|} - N_{\text{EPR}}^{(p-|\alpha|, q-|\alpha|)}$.*

The positive term $D^{p+q-2|\alpha|}$ is the rank of the bare projector P_α . The negative term $N_{\text{EPR}}^{(p-|\alpha|, q-|\alpha|)}$ counts the number of states in P_α that are contained in $P_{\alpha'}$ for any $\alpha' \supset \alpha$. These states are removed from P_α^{nE} and $\tilde{P}_\alpha$ and hence are subtracted from the rank. The fact that the rank of P_α^{nE} and $\tilde{P}_\alpha$ is the same implies that every state in P_α^{nE} is outside the span of P_β^{nE} for all $\beta \neq \alpha$. The proposition immediately implies that the rank of the ℓ -EPR projector $\tilde{P}_\ell$ is equal to

$$D_\ell \equiv \text{rank } \tilde{P}_\ell = \binom{p}{\ell} \binom{q}{\ell} \ell! \cdot \left(D^{p+q-2\ell} - N_{\text{EPR}}^{(p-\ell, q-\ell)} \right), \quad (\text{F.12})$$

where $\binom{p}{\ell} \binom{q}{\ell} \ell!$ counts the number of α with size ℓ . The value of $N_{\text{EPR}}^{(p,q)}$ is tricky to compute in general. However, one has an immediate upper bound, $N_{\text{EPR}}^{(p',q')} \leq \sum_{|\alpha|=1} \text{rank}(P_\alpha) = pq \cdot D^{p'+q'-2}$.

Before proceeding, we pause to provide the following explicit expression for the no-EPR projector Π^{nE} . This expression is not needed for any of the results in the preceding sections; we mention it solely for completeness for the interested reader. The expression is as follows (Appendix F.1.8).

Proposition 8 (Expression for the no-EPR projector). *For any $p + q \leq D$. The inner product of the no-EPR projector, Π^{nE} , with a permutation operator, $\pi_L \otimes \pi_R$, is given by,*

$$\text{tr}(\Pi^{\text{nE}}(\pi_L \otimes \pi_R)^{-1}) = [\hat{\text{Wg}}|_{\text{perm}}]_{1, \pi_L \otimes \pi_R}^{-1}, \quad (\text{F.13})$$

where $\hat{\text{Wg}}|_{\text{perm}}$ is the $(p!q!) \times (p!q!)$ sub-matrix obtained by restricting the $(p+q)! \times (p+q)!$ Weingarten matrix, $\hat{\text{Wg}}$, to the permutation operators. As a consequence, the no-EPR projector can be written as a sum of PTPs with coefficients,

$$\Pi^{\text{nE}} = \sum_{\sigma} \left(\sum_{\pi_L, \pi_R} [\hat{\text{Wg}}|_{\text{perm}}]_{1, \pi_L \otimes \pi_R}^{-1} \text{Wg}_{\pi_L \otimes \pi_R, \sigma} \right) \sigma. \quad (\text{F.14})$$

The expression for the no-EPR projector is not particularly easy to work with, given that it involves the inverse of a sub-matrix of the Weingarten matrix. We provide further discussion and applications in Appendix F.2

F.1.3 Partial isometries and reformulation of the mixed Haar twirl

The mixed Haar twirl has a particularly simple action on the orthogonal subspaces constructed in the previous subsection. To show this, let us first discuss the bare projectors, and then turn to the

orthogonal projectors. Each bare projector P_α naturally defines a *partial isometry* from the $(p+q)$ -copy Hilbert space to a smaller $(p+q-2|\alpha|)$ -copy Hilbert space,

$$P_\alpha = \overbrace{\text{---} \text{---} \text{---}}^{\text{---}} \text{---} \text{---} \text{---} = \overbrace{\text{---} \text{---} \text{---}}^{\text{---}} \text{---} \text{---} \text{---} = I_\alpha^\dagger I_\alpha. \quad (\text{F.15})$$

The $p+q-2|\alpha|$ copies correspond to the legs of the PTP that are not paired in α . The isometries are unitary-equivariant,

$$I_\alpha \mathcal{U}_q^p = \overbrace{\text{---} \text{---} \text{---}}^{\text{---}} \text{---} \text{---} \text{---} = \overbrace{\text{---} \text{---} \text{---}}^{\text{---}} \text{---} \text{---} \text{---} = \mathcal{U}_{q-\ell}^{p-\ell} I_\alpha, \quad (\text{F.16})$$

meaning that the action of any MTU on the $(p+q)$ -copy Hilbert space translates to a corresponding smaller MTU on the $(p+q-2|\alpha|)$ -copy Hilbert space.

We will now show that an analogous set of isometries can be constructed for the orthogonal projectors $\tilde{P}_\alpha$. We define these carefully in the following manner. To begin, we expand each orthogonal projector as follows,

$$\tilde{P}_\alpha = \tilde{P}_\alpha \tilde{P}_\alpha \tilde{P}_\alpha = \tilde{P}_\alpha \left(\sum_{\pi_L, \pi_R} c_{\pi_L, \pi_R} \cdot (\alpha, \alpha, \pi_L, \pi_R) \right) \tilde{P}_\alpha, \quad (\text{F.17})$$

where, in the rightmost expression, we write the center $\tilde{P}_\alpha$ as a linear combination of PTPs and keep only the PTPs, $(\alpha, \alpha, \pi_L, \pi_R)$, that have both input and output pairs equal to α (since all other PTPs vanish upon conjugation by $\tilde{P}_\alpha$). By definition, each PTP $(\alpha, \alpha, \pi_L, \pi_R)$ is proportional to the EPR projector, $|E_\alpha\rangle\langle E_\alpha|$, on subsystem α . To proceed, we insert the following resolution of the identity on the complement of α ,

$$\mathbb{1}_{\bar{\alpha}} = \sum_{\gamma} \tilde{P}_\gamma^{(\bar{\alpha})} = \Pi_{\bar{\alpha}}^{\text{nE}} + \sum_{\gamma \neq \emptyset} \tilde{P}_\gamma^{(\bar{\alpha})}, \quad (\text{F.18})$$

where γ runs over sets of pairs in $\bar{\alpha}$, and the superscript denotes that the orthogonal projector is constructed from PTPs that act only on $\bar{\alpha}$. From Proposition 5, each $\tilde{P}_\gamma^{(\bar{\alpha})}$ can be written as a sum of PTPs on $\bar{\alpha}$ with size at least 1. Thus, the tensor product, $\tilde{P}_\gamma^{(\bar{\alpha})} \otimes |E_\alpha\rangle\langle E_\alpha|$, can be written as a sum of PTPs with size at least $|\alpha|+1$. This implies that $\tilde{P}_\gamma^{(\bar{\alpha})} \otimes |E_\alpha\rangle\langle E_\alpha|$ vanishes upon left or right multiplication with $\tilde{P}_\alpha$, which yields,

$$\tilde{P}_\alpha = \tilde{P}_\alpha \mathbb{1}_{\bar{\alpha}} \left(\sum_{\pi_L, \pi_R} c_{\pi_L, \pi_R} \cdot (\alpha, \alpha, \pi_L, \pi_R) \right) \mathbb{1}_{\bar{\alpha}} \tilde{P}_\alpha = \tilde{P}_\alpha \Pi_{\bar{\alpha}}^{\text{nE}} \left(\sum_{\pi_L, \pi_R} c_{\pi_L, \pi_R} \cdot (\alpha, \alpha, \pi_L, \pi_R) \right) \Pi_{\bar{\alpha}}^{\text{nE}} \tilde{P}_\alpha. \quad (\text{F.19})$$

To proceed, let us take the square root of the middle operators,

$$M_\alpha = \left(\sum_{\pi_L, \pi_R} c_{\pi_L, \pi_R} \cdot \Pi_{\bar{\alpha}}^{\text{nE}}(\alpha, \alpha, \pi_L, \pi_R) \Pi_{\bar{\alpha}}^{\text{nE}} \right)^{1/2} \equiv M'_\alpha \otimes |E_\alpha\rangle\langle E_\alpha|, \quad (\text{F.20})$$

where M'_α acts on $\bar{\alpha}$. We prove that the square root is well-defined within the proof of Proposition 9 (Appendix F.1.9), by showing that the operator inside the parentheses is a positive operator. From the right hand side, we can see that $M_\alpha = M_\alpha P_\alpha = P_\alpha M_\alpha$. Thus, we can write

$$\tilde{P}_\alpha = \tilde{P}_\alpha \tilde{P}_\alpha \tilde{P}_\alpha = \tilde{P}_\alpha M_\alpha M_\alpha \tilde{P}_\alpha = \tilde{P}_\alpha M_\alpha P_\alpha M_\alpha \tilde{P}_\alpha = (\tilde{P}_\alpha M_\alpha I_\alpha^\dagger)(I_\alpha M_\alpha \tilde{P}_\alpha). \quad (\text{F.21})$$

This decomposition immediately allows us to write $\tilde{P}_\alpha$ in terms of the “orthogonal” isometry,

$$\tilde{I}_\alpha = I_\alpha M_\alpha \tilde{P}_\alpha, \quad (\text{F.22})$$

where we have $\tilde{P}_\alpha = \tilde{I}_\alpha^\dagger \tilde{I}_\alpha$ from Eq. (F.21). This completes our definition of the partial isometries.

We establish a few key properties of the partial isometries (Appendix F.1.9).

Proposition 9 (Partial isometries). *For any $D \geq p + q$, the map $\tilde{I}_\alpha$ is well-defined and is an isometry from the support of $\tilde{P}_\alpha$ to the no-EPR subspace of $\mathcal{H}^{\otimes p-|\alpha|} \otimes \mathcal{H}^{\otimes q-|\alpha|}$. The isometry is unitary-equivariant, $\tilde{I}_\alpha(\mathcal{U}_q^p) = (\mathcal{U}_{q-\ell}^{p-\ell}) \tilde{I}_\alpha$.*

The range of the isometry is restricted to the no-EPR subspace of $\mathcal{H}^{\otimes p-|\alpha|} \otimes \mathcal{H}^{\otimes q-|\alpha|}$, in contrast the bare isometry defined earlier which maps to the entire space. This reflects the smaller size of $\tilde{P}_\alpha$ compared to P_α .

We can also define a final set of partial isometries, $\tilde{I}_\ell$, associated to the ℓ -EPR projectors $\tilde{P}_\ell$. These will play a particularly important role since, as aforementioned, the definition of $\tilde{P}_\ell$ is unique and independent of our ordering of the α , in contrast to $\tilde{P}_\alpha$. The support of $\tilde{P}_\ell$ is equal to the tensor sum of the support of each $\tilde{P}_\alpha$ with size $|\alpha| = \ell$. Hence, the partial isometry $\tilde{I}_\ell$ will map from this domain to the $\binom{p}{\ell} \binom{q}{\ell} \ell!$ -fold tensor sum of the range of each $\tilde{I}_\alpha$. Each $\tilde{I}_\alpha$ has range equal to the no-EPR subspace of $\mathcal{H}^{\otimes p-|\alpha|} \otimes \mathcal{H}^{\otimes q-|\alpha|}$. Hence, the range of $\tilde{I}_\ell$ will be equal to,

$$\left[\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)} \right]_{\text{nE}} \otimes \mathcal{A}_\ell, \quad (\text{F.23})$$

where $|\mathcal{A}_\ell| = \binom{p}{\ell} \binom{q}{\ell} \ell!$ counts the number of α with size $|\alpha| = \ell$, i.e. the number of terms in the tensor sum. The first term denotes the no-EPR subspace of $\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)}$. With the range defined, we write the partial isometry as,

$$\tilde{I}_\ell = \sum_{\alpha: |\alpha|=\ell} \tilde{I}_\alpha, \quad (\text{F.24})$$

with the convention that each $\tilde{I}_\alpha$ maps from the support of $\tilde{P}_\alpha$ to $[\mathcal{H}^{\otimes(p-\ell)} \otimes \mathcal{H}^{\otimes(q-\ell)}]_{\text{nE}} \otimes |\alpha\rangle\langle\alpha|$ for $|\alpha\rangle \in \mathcal{A}_\ell$. From Proposition 9, the orthogonal isometries $\tilde{I}_\ell$ are unitary-equivariant, in the sense that $\tilde{I}_\ell(\mathcal{U}_q^p) = (\mathcal{U}_{q-\ell}^{p-\ell} \otimes \mathbb{1}_{\mathcal{A}_\ell}) \tilde{I}_\ell$ for any MTU.

The partial isometries allow us to reformulate the mixed Haar twirl as follows. Let us begin by inserting the resolution of the identity, $\mathbb{1} = \sum_\ell \tilde{I}_\ell^\dagger \tilde{I}_\ell$, twice in the definition of the mixed Haar twirl,

$$\Phi_H^{(p,q)}(X) \equiv \mathbb{E}_{U \sim H} \left[\left(\sum_\ell \tilde{I}_\ell^\dagger \tilde{I}_\ell \right) (\mathcal{U}_q^p) X (\mathcal{U}_q^p)^\dagger \left(\sum_{\ell'} \tilde{I}_{\ell'}^\dagger \tilde{I}_{\ell'} \right) \right] = \sum_{\ell, \ell'} \mathbb{E}_{U \sim H} \left[\tilde{I}_\ell^\dagger ((\mathcal{U}_{q-\ell}^{p-\ell})) \tilde{I}_\ell X \tilde{I}_{\ell'}^\dagger (\mathcal{U}_{p-\ell', q-\ell'}^\dagger) \tilde{I}_{\ell'} \right],$$

where on the right side, we move the action of the MTU to the inside of the partial isometry. We suppress the $\mathcal{A}_\ell, \mathcal{A}_{\ell'}$ registers for brevity, since the MTU acts trivially on these registers. We can now apply the formula for the mixed Haar twirl in terms of PTPs to each term ℓ, ℓ' above. This yields,

$$\Phi_H^{(p,q)}(\rho) = \sum_\ell \tilde{I}_\ell^\dagger \left[\sum_{\pi_L \pi_R} \sum_{\tilde{\pi}_L \tilde{\pi}_R} \text{tr} \left(\tilde{I}_\ell \rho \tilde{I}_\ell^\dagger (\pi_L \otimes \pi_R)^{-1} \right) \cdot \text{Wg}_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_L}^{(p+q-2\ell)} \cdot (\tilde{\pi}_L \otimes \tilde{\pi}_R) \right] \tilde{I}_\ell, \quad (\text{F.25})$$

where $\text{Wg}_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_L}^{(p+q-2\ell)}$ denotes the Weingarten matrix on $p+q-2\ell$ copies. To compute this expression, we note that any PTP with size greater than zero vanishes upon conjugation by $\tilde{I}_\ell$, since the range of $\tilde{I}_\ell$ is the no-EPR subspace (Proposition 9) and PTPs with size greater than zero involve at least one EPR projector. This implies that the terms with $\ell \neq \ell'$ vanish, and that the remaining $\ell = \ell'$ terms

involve only tensor products permutation operators between the left and right side, $\pi_L, \tilde{\pi}_L \in S_{p-\ell}$ and $\pi_R, \tilde{\pi}_R \in S_{q-\ell}$.

This completes our derivation of the reformulation of the mixed Haar twirl. In the remaining subsections, we provide the detailed proofs of each proposition above.

F.1.4 Proof of Proposition 4: Nearly-orthogonal projectors

Let us first establish a simple fact regarding the PTPs. Namely, the size of a PTP can only increase under multiplication.

Fact 5. *The product of a size ℓ PPT and a size ℓ' PPT has size at least $\max(\ell, \ell')$.*

Proof. Call the two PPTs σ and σ' , respectively, and let σ_I denote the input pairs of σ , and σ'_O denote the output pairs of σ' . We have $|\sigma_I| = \ell$ and $|\sigma'_O| = \ell'$. One can easily see that the product $\sigma\sigma'$ is a PPT β with input pairs $\beta_I \supseteq \sigma_I$ and output pairs $\beta_O \supseteq \sigma'_O$. The size of $\sigma\sigma'$ is given by $|\beta_I| = |\beta_O| \geq \max(|\sigma_I|, |\sigma'_O|) = \max(\ell, \ell')$. $\square$

We can now prove Proposition 4. Assume $|\beta| > |\alpha|$ without loss of generality. We know that the product of the bare projectors, $P_\alpha P_\beta$, is proportional to a PTP γ with $\gamma_I \supseteq \alpha$. From Fact 5, the PTP has size at least $|\gamma_I| = |\gamma_O| = |\beta|$. Since $|\beta| > |\alpha|$, this implies $\gamma_I \supsetneq \alpha$. This implies that γ_I contains at least one pair on $\bar{\alpha}$. Thus, we have $\Pi_{\bar{\alpha}}^{\text{nE}}(P_\alpha P_\beta) = 0$ and hence, $P_\alpha^{\text{nE}} P_\beta^{\text{nE}} = \Pi_{\bar{\alpha}}^{\text{nE}} P_\alpha P_\beta \Pi_{\bar{\beta}}^{\text{nE}} = 0$. $\square$

F.1.5 Proof of Proposition 5: Orthogonal projectors

We first note that each $\tilde{P}_\alpha$ commutes with any MTU, $\mathcal{U}_q^p = U^{\otimes p} \otimes U^{*, \otimes q}$. To see this, recall that each bare projector P_α commutes with $\mathcal{U}_q^p$. Hence, if $|\psi\rangle$ is in the span of P_α , then $\mathcal{U}_q^p |\psi\rangle$ is also in the span of P_α . Similarly, it follows that if $|\psi\rangle$ is in span $(\{P_{\alpha'} : \alpha' \leq \alpha\})$, then $\mathcal{U}_q^p |\psi\rangle$ is also in the same span. Observing the definition of $\tilde{P}_\alpha$ [Eq. (F.9)], we see that $\tilde{P}_\alpha \mathcal{U}_q^p |\psi\rangle = \mathcal{U}_q^p |\psi\rangle$ if and only if $\tilde{P}_\alpha |\psi\rangle = |\psi\rangle$. Hence, $\tilde{P}_\alpha$ commutes with $\mathcal{U}_q^p$.

To complete our proof, let $\{|\phi\rangle\}$ denote an orthonormal basis for the unit eigenspace of $\tilde{P}_\alpha$. From the definition of $\tilde{P}_\alpha$, each vector $|\phi\rangle$ can be written as a sum, $|\phi\rangle = \sum_{\alpha' \leq \alpha} |E_{\alpha'}\rangle \otimes |\phi_{\alpha'}^c\rangle$, of vectors in $P_{\alpha'}$ for $\alpha' \leq \alpha$. Since $\tilde{P}_\alpha$ commutes with $\mathcal{U}_q^p$, we have $\tilde{P}_\alpha = \mathbb{E}_{U \sim H} [\mathcal{U}_q^p \tilde{P}_\alpha (\mathcal{U}_q^p)^\dagger]$. Expressed in terms of the orthonormal basis $\{|\phi\rangle\}$, this gives

$$\tilde{P}_\alpha = \sum_{\phi} \mathbb{E}_{U \sim H} \left[(\mathcal{U}_q^p |\phi\rangle \langle \phi| (\mathcal{U}_q^p)^\dagger) \right] = \sum_{\phi} \sum_{\alpha', \alpha'' \leq \alpha} \mathbb{E}_{U \sim H} \left[(\mathcal{U}_q^p |\phi_{\alpha'}\rangle \langle \phi_{\alpha''}| (\mathcal{U}_q^p)^\dagger) \right]. \quad (\text{F.26})$$

By definition, we can write $|\phi_\alpha\rangle = |E_\alpha\rangle \otimes |\phi_\alpha^c\rangle$, where $|E_\alpha\rangle$ is the EPR projector on α , and $|\phi_\alpha^c\rangle$ is a state on the complement of α . When we apply $\mathcal{U}_q^p$ to this state, the factors acting on α cancel, leaving

$$\mathcal{U}_q^p |\phi_\alpha\rangle = |E_\alpha\rangle \otimes \mathcal{U}_{q-|\alpha'|}^{p-|\alpha'|} |\phi_\alpha^c\rangle. \quad (\text{F.27})$$

Applying the formula for the mixed Haar twirl to $\mathcal{U}_{q-|\alpha'|}^{p-|\alpha'|}$, one finds that each state

$$\mathbb{E}_{U \sim H} \left[\mathcal{U}_q^p |\phi_{\alpha'}\rangle \langle \phi_{\alpha''}| (\mathcal{U}_q^p)^\dagger \right] \quad (\text{F.28})$$

can be expressed as a sum of PTPs σ with $\sigma_I \supseteq \alpha'$ and $\sigma_O \supseteq \alpha''$. This implies that $\sigma_I \leq \alpha'$ and $\sigma_O \leq \alpha''$, since our ordering of pairs was strictly decreasing. Hence, we obtain an expression for $\tilde{P}_\alpha$ as a sum of PTPs with $\sigma_I, \sigma_O \leq \alpha$. $\square$

F.1.6 Proof of Proposition 6: The ℓ -EPR projector

One can generate any PTP from a product of permutations, $\pi_L \otimes \pi_R$, and a single EPR projector, Π_{ij} , onto a copy i on the left side and a copy j on the right side. Hence, to prove that $\tilde{P}_\ell$ commutes with any PTP, it suffices to prove that $\tilde{P}_\ell$ commutes with each permutation, as well as Π_{ij} . The former follows from the definition of $\tilde{P}_\ell$, since conjugation by a permutation simply amounts to a re-ordering of the α within each size, and the projector $\tilde{P}_\ell$ is manifestly independent of this ordering. Thus, it remains only to show that $\tilde{P}_\ell$ commutes with Π_{ij} .

Since $\tilde{P}_\ell$ can be written as a sum of PTPs with size greater than or equal to ℓ (Proposition 5), the operator $\Pi_{ij}\tilde{P}_\ell$ can also be written as a sum of PTPs with such size (using Fact 5). This implies that $\tilde{P}_{\ell'}\Pi_{ij}\tilde{P}_\ell = 0$ for any $\ell' > \ell$, since $\tilde{P}_{\ell'}$ is orthogonal to any PTP with size greater than ℓ by definition. Applying the same argument to the Hermitian conjugate, $(\tilde{P}_{\ell'}\Pi_{ij}\tilde{P}_\ell)^\dagger = \tilde{P}_{\ell'}\Pi_{ij}\tilde{P}_\ell$, we have that $\tilde{P}_{\ell'}\Pi_{ij}\tilde{P}_\ell = 0$ for any $\ell' < \ell$, and hence $\ell' \neq \ell$. The desired commutation follows immediately. We write

$$\tilde{P}_\ell \Pi_{ij} \tilde{P}_\ell = (\mathbb{1} - \sum_{\ell' \neq \ell} \tilde{P}_{\ell'}) \Pi_{ij} \tilde{P}_\ell = \Pi_{ij} \tilde{P}_\ell, \quad (\text{F.29})$$

where in the first equality we use that the projectors form a complete basis, $\sum_{\ell'} \tilde{P}_{\ell'} = \mathbb{1}$, and in the second equality we use that $\tilde{P}_{\ell'} \Pi_{ij} \tilde{P}_\ell = 0$ if $\ell' \neq \ell$. Taking the Hermitian conjugate of both sides above yields $\tilde{P}_\ell \Pi_{ij} \tilde{P}_\ell = \tilde{P}_\ell \Pi_{ij}$. Thus, we have $\Pi_{ij} \tilde{P}_\ell = \tilde{P}_\ell \Pi_{ij} \tilde{P}_\ell = \tilde{P}_\ell \Pi_{ij}$, i.e. $\tilde{P}_\ell$ and Π_{ij} commute. This completes the proof. $\square$

F.1.7 Proof of Proposition 7: Rank of the orthogonal projectors

Let $\Pi_{\bar{\alpha}}^{\geq 1\text{E}} = \mathbb{1} - \Pi_{\bar{\alpha}}^{\text{nE}} = \sum_{\gamma \neq \emptyset} \tilde{P}_\gamma^{(\bar{\alpha})}$ denote the projector onto states with at least one EPR pair on $\bar{\alpha}$. We have

$$P_\alpha = |E_\alpha\rangle\langle E_\alpha| \otimes (\Pi_{\bar{\alpha}}^{\text{nE}} + \Pi_{\bar{\alpha}}^{\geq 1\text{E}}). \quad (\text{F.30})$$

Only the first term contains states that contribute to $\tilde{P}_\alpha$. To see this, we apply Proposition 5 to subsystem $\bar{\alpha}$, which shows that $\Pi_{\bar{\alpha}}^{\geq 1\text{E}}$ can be written as a sum of PTPs on $\bar{\alpha}$ with at least one EPR projector. After taking the tensor product with $|E_\alpha\rangle\langle E_\alpha|$, we obtain a sum of PTPs with at least $|\alpha| + 1$ EPR projectors. Thus, we have $\text{span}(|E_\alpha\rangle\langle E_\alpha| \otimes \Pi_{\bar{\alpha}}^{\geq 1\text{E}}) \subseteq \text{span}(\{P_{\alpha'} : \alpha' < \alpha\})$, which is orthogonal to $\text{span}(\tilde{P}_\alpha)$ by definition. Since P_α has rank $D^{p+q-2|\alpha|}$ and $\Pi_{\bar{\alpha}}^{\geq 1\text{E}}$ has rank $N_{\text{EPR}}^{(p-|\alpha|, q-|\alpha|)}$, this implies that the rank of $\tilde{P}_\alpha$ is upper bounded by $D^{p+q-2|\alpha|} - N_{\text{EPR}}^{(p-|\alpha|, q-|\alpha|)}$.

To show that the rank is equal to this value, we must show that every non-zero vector in $\text{span}(|E_\alpha\rangle\langle E_\alpha| \otimes \Pi_{\bar{\alpha}}^{\text{nE}})$ is outside of $\text{span}(\{\tilde{P}_{\alpha'} : \alpha' < \alpha\})$. We provide a proof by contradiction. Suppose that a non-zero vector $|\psi\rangle$ in P_α^{nE} is inside of $\text{span}(\{P_{\alpha'} : \alpha' \leq \alpha\})$. This implies that we can write both $|\psi\rangle = |E_\alpha\rangle \otimes |\psi_{\bar{\alpha}}\rangle$ for some $|\psi_{\bar{\alpha}}\rangle \in \Pi_{\bar{\alpha}}^{\text{nE}}$, as well as $|\psi\rangle = \sum_{\alpha' < \alpha} |E_{\alpha'}\rangle \otimes |\psi_{\bar{\alpha}'}\rangle$ for some $|\psi_{\bar{\alpha}'}\rangle$. Since both P_α and P_α^{nE} commute with any mixed tensor unitary $\mathcal{U}_q^p$, we also have that $\mathcal{U}_q^p |\psi\rangle$ is in both $\text{span}(P_\alpha^{\text{nE}})$ and $\text{span}(\{P_{\alpha'} : \alpha' \leq \alpha\})$. Thus, we are free to average over U to obtain

$$\begin{aligned} \mathbb{E}_{U \sim H} \left[\mathcal{U}_q^p |\psi\rangle\langle\psi| (\mathcal{U}_q^p)^\dagger \right] &= \mathbb{E}_{U \sim H} \left[|E_\alpha\rangle\langle E_\alpha| \otimes \mathcal{U}_{q-\ell}^{p-\ell} |\psi_{\bar{\alpha}}\rangle\langle\psi_{\bar{\alpha}}| (\mathcal{U}_{q-\ell}^{p-\ell})^\dagger \right] \\ &= \sum_{\pi_L, \pi_R} c_{\pi_L \pi_R} \Pi_{\text{noEPR}}^{\bar{\alpha}}(\alpha, \alpha, \pi_L, \pi_R) \Pi_{\bar{\alpha}}^{\text{nE}} \end{aligned} \quad (\text{F.31})$$

using our first decomposition of $|\psi\rangle$. Here, we have used that $|\psi_{\bar{\alpha}}\rangle \in \Pi_{\bar{\alpha}}^{\text{nE}}$, i.e. $|\psi_{\bar{\alpha}}\rangle = \Pi_{\bar{\alpha}}^{\text{nE}} |\psi_{\bar{\alpha}}\rangle$, to insert the no-EPR projector on $\bar{\alpha}$. The coefficients $c_{\pi_L \pi_R}$ are obtained from the Haar twirl over $|\psi_{\bar{\alpha}}\rangle\langle\psi_{\bar{\alpha}}|$. In a similar manner, we can obtain

$$\mathbb{E}_{U \sim H} \left[(\mathcal{U}_q^p) |\psi\rangle\langle\psi| (\mathcal{U}_q^p)^\dagger \right] = \sum_{\substack{\alpha_I < \alpha \\ \alpha_O < \alpha}} \sum_{\pi_L, \pi_R} d_{\pi_L \pi_R}^{\alpha_I \alpha_O} \cdot (\alpha_I, \alpha_O, \pi_L, \pi_R), \quad (\text{F.32})$$

using our second decomposition of $|\psi\rangle$. The coefficients $d_{\pi_L\pi_R}^{\alpha_I\alpha_O}$ are obtained from the Haar twirl over the various $(|E_{\alpha_I}\rangle \otimes |\psi_{\tilde{\alpha}_I}\rangle)(\langle E_{\alpha_O}| \otimes \langle \psi_{\tilde{\alpha}_O}|)$.

Note that the latter expression, Eq. (F.32), contains only PTPs with $\alpha_I, \alpha_O < \alpha$. Since the representation of the walled Brauer algebra is faithful for $D \geq p + q$, this implies that the former expression, Eq. (F.31), must also contain only such PTPs. This follows because the PTPs are linearly independent operators when the representation is faithful. We will now show that this leads to a contradiction. To begin, recall that we can write $\Pi_{\tilde{\alpha}}^{\text{nE}} = \mathbb{1} - \Pi_{\tilde{\alpha}}^{\geq 1\text{E}}$, and that $|E_{\alpha}\rangle\langle E_{\alpha}| \otimes \Pi_{\geq 1\text{EPR}}^{\tilde{\alpha}}$ can be expressed as a sum of diagrams with $\alpha_I, \alpha_O < \alpha$. Thus, Eq. (F.31) can be written as

$$\sum_{\pi_L, \pi_R} c_{\pi_L\pi_R} \Pi_{\text{noEPR}}^{\tilde{\alpha}}(\alpha, \alpha, \pi_L, \pi_R) \Pi_{\tilde{\alpha}}^{\text{nE}} = \sum_{\pi_L, \pi_R} c_{\pi_L\pi_R}(\alpha, \alpha, \pi_L, \pi_R) + (\text{PTPs with } \alpha_I < \alpha \text{ or } \alpha_O < \alpha). \quad (\text{F.33})$$

The first term contains solely PTPs with $\alpha_I = \alpha_O = \alpha$. Thus, if Eq. (F.31) can be written as a sum of PTPs with $\alpha_I, \alpha_O < \alpha$, we must have $c_{\pi_L\pi_R} = 0$ for all π_L, π_R . This implies that $\langle \psi_{\tilde{\alpha}} | \psi_{\tilde{\alpha}} \rangle$ is zero, which implies that $|\psi\rangle$ is zero, which is a contradiction. We conclude that every non-zero vector in $\text{span}(P_{\alpha}^{\text{nE}})$ is outside $\text{span}(\{P_{\alpha'} : \alpha' \leq \alpha\})$. This implies that the rank of $\tilde{P}_{\alpha}$ is equal to the rank of P_{α}^{nE} , which proves the proposition. $\square$

F.1.8 Proof of Proposition 8: Expression for the no-EPR projector

Let us first prove Eq. (F.13). We know from Proposition 5 that the no-EPR projector can be written as a sum of PTPs. Hence, we can write,

$$\Pi^{\text{nE}} = \sum_{\sigma, \tau} \widetilde{W}_{g_{\sigma, \tau}} \cdot \text{tr}(\Pi^{\text{nE}} \sigma^{\dagger}) \cdot \tau, \quad (\text{F.34})$$

where σ, τ run over the $(p + q)!$ PTPs. We can simplify this expression in two ways. First, we use that $\text{tr}(\Pi^{\text{nE}} \sigma) = 0$ unless σ is a permutation, $\sigma = \pi_L \otimes \pi_R$. Second, we can use that $(\Pi^{\text{nE}})^2 = \Pi^{\text{nE}}$ to multiply the right hand side by Π^{nE} . This similarly restricts the sum over τ , since $\tau \Pi^{\text{nE}} = 0$ unless τ is a permutation, $\tau = \tilde{\pi}_L \otimes \tilde{\pi}_R$. Together, these give

$$\Pi^{\text{nE}} = \sum_{\pi_L \pi_R} \sum_{\tilde{\pi}_L \tilde{\pi}_R} W_{g_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_R}} \cdot \text{tr}(\Pi^{\text{nE}} (\pi_L \otimes \pi_R)^{-1}) \cdot (\tilde{\pi}_L \otimes \tilde{\pi}_R) \Pi^{\text{nE}}. \quad (\text{F.35})$$

To proceed, consider the operators, $\{(\tilde{\pi}_L \otimes \tilde{\pi}_R) \Pi^{\text{nE}}\}$, appearing on the right side of Eq. (F.35). We will prove that these operators are linearly independent. Suppose that there exists coefficients, $c_{\tilde{\pi}}$, for $\tilde{\pi} \equiv \tilde{\pi}_L \otimes \tilde{\pi}_R$, such that $\sum_{\tilde{\pi}} c_{\tilde{\pi}} \tilde{\pi} \Pi^{\text{nE}} = 0$. Now, the no-EPR projector can be written as $\Pi^{\text{nE}} = \mathbb{1} - \sum_{\ell=1}^{\min(p, q)} \tilde{P}_{\ell}$, where each projector $\tilde{P}_{\ell}$ can be written as a sum of PTPs with size greater than or equal to $\ell \geq 1$. Hence, we can write $\sum_{\tilde{\pi}} c_{\tilde{\pi}} \tilde{\pi} \Pi^{\text{nE}} = \sum_{\tilde{\pi}} c_{\tilde{\pi}} \tilde{\pi} + \Delta$, where Δ is a sum of PTPs with size ≥ 1 . If the left side of this expression were to vanish, as supposed, then the first term on the right side must vanish as well, since the PTPs are linearly independent for $p + q \leq D$, and the first term has only PTPs of size zero and the second term has only PTPs of size ≥ 1 . However, this requires $c_{\tilde{\pi}} = 0$ for all $\tilde{\pi}$, since the permutation operators are linearly independent as well. This establishes that the operators, $\{(\tilde{\pi}_L \otimes \tilde{\pi}_R) \Pi^{\text{nE}}\}$, are linearly independent.

We can use this linear independence to complete our proof. Observing Eq. (F.35), the only way in which the two sides of the equation can be equal is if,

$$\sum_{\pi_L \pi_R} W_{g_{\pi_L \otimes \pi_R, \tilde{\pi}_L \otimes \tilde{\pi}_R}} \cdot \text{tr}(\Pi^{\text{nE}} (\pi_L \otimes \pi_R)^{-1}) = \delta_{\mathbb{1}, \tilde{\pi}_L \otimes \tilde{\pi}_R} \quad (\text{F.36})$$

for every $\tilde{\pi}_L, \tilde{\pi}_R$. The second term on the left side of the equation are the matrix elements of $\hat{W}g|_{\text{perm}}$. Applying the matrix inverse of $\hat{W}g|_{\text{perm}}$ to the left and right side, we obtain Eq. (F.13), as desired.

The second statement of the proposition, Eq. (F.14), follows immediately from the first statement and Eq. (F.34). As before, we note that $\text{tr}(\Pi^{\text{nE}}\sigma) = 0$ unless $\sigma = \pi_L \otimes \pi_R$, and we substitute the first statement, Eq. (F.13), in for $\text{tr}(\Pi^{\text{nE}}\sigma) = \text{tr}(\Pi^{\text{nE}}(\pi_L \otimes \pi_R)^{-1})$. $\square$

F.1.9 Proof of Proposition 9: Partial isometries

To show that the isometry is well-defined, we simply need to show that the quantity within the parentheses in Eq. (F.20) is positive. To do so, let us expand the operator as a sum over its eigenvectors, $|\lambda\rangle \otimes |E_\alpha\rangle$, and eigenvalues, λ ,

$$\Pi_{\bar{\alpha}}^{\text{nE}} \sum_{\pi_L, \pi_R} c_{\pi_L \pi_R} \cdot (\alpha, \alpha, \pi_L, \pi_R) \Pi_{\bar{\alpha}}^{\text{nE}} = \sum_{\lambda} \lambda |\lambda \otimes E_\alpha\rangle \langle \lambda \otimes E_\alpha|. \quad (\text{F.37})$$

To show that the eigenvalues are positive, we first use the fact that when we conjugate the operator above by $\tilde{P}_\alpha$, we obtain $\tilde{P}_\alpha$. The conjugation maps each rank-1 projector to a new rank-1 operator, $\mathcal{N}_\lambda |\tilde{\lambda}\rangle \langle \tilde{\lambda}|$, in $\tilde{P}_\alpha$,

$$\tilde{P}_\alpha = \tilde{P}_\alpha \Pi_{\bar{\alpha}}^{\text{nE}} \sum_{\pi_L, \pi_R} c_{\pi_L \pi_R} \cdot (\alpha, \alpha, \pi_L, \pi_R) \Pi_{\bar{\alpha}}^{\text{nE}} \tilde{P}_\alpha = \sum_{\lambda} \lambda \cdot \tilde{P}_\alpha |\lambda \otimes E_\alpha\rangle \langle \lambda \otimes E_\alpha| \tilde{P}_\alpha = \sum_{\lambda} \lambda \cdot \mathcal{N}_\lambda |\tilde{\lambda}\rangle \langle \tilde{\lambda}|$$

with normalization $\mathcal{N}_\lambda = \langle \lambda \otimes E_\alpha | \tilde{P}_\alpha | \lambda \otimes E_\alpha \rangle$, $0 \leq \mathcal{N}_\lambda \leq 1$. Now, we note that there are at most $D^{p+q-2|\alpha|} - N_{\text{EPR}}^{(p-|\alpha|, q-|\alpha|)}$ non-zero eigenvalues λ , corresponding to the dimension of the no-EPR subspace on $\bar{\alpha}$. However, from Proposition 7, this is also the rank of $\tilde{P}_\alpha$. Hence, there must be precisely this number of non-zero eigenvalues, and the set of conjugated vectors, $\{|\tilde{\lambda}\rangle\}$, must be linearly independent. To determine the eigenvalues λ , let us apply $\tilde{P}_\alpha$ to $|\tilde{\lambda}'\rangle$ for any $\tilde{\lambda}'$. We have $|\tilde{\lambda}'\rangle = \tilde{P}_\alpha |\tilde{\lambda}'\rangle = \sum_{\lambda} \lambda \cdot \mathcal{N}_\lambda \langle \tilde{\lambda} | \tilde{\lambda}' \rangle |\tilde{\lambda}\rangle$. Since the $\{|\tilde{\lambda}\rangle\}$ are linearly independent, we must have $\langle \tilde{\lambda} | \tilde{\lambda}' \rangle = \delta_{\tilde{\lambda}, \tilde{\lambda}'}$ and $\lambda \cdot \mathcal{N}_\lambda = 1$. Hence, $\lambda = 1/\mathcal{N}_\lambda$, so every eigenvalue is positive and greater than one.

To show that $\tilde{I}_\alpha$ is an isometry as described, we must show that $\tilde{I}_\alpha^\dagger \tilde{I}_\alpha = \tilde{P}_\alpha$ and $\tilde{I}_\alpha \tilde{I}_\alpha^\dagger = \Pi_{\bar{\alpha}}^{\text{nE}}$. The first equality follows by construction [see Eqs. (F.21) and (F.22)]. To establish the second equality, we compute

$$(\tilde{I}_\alpha \tilde{I}_\alpha^\dagger)^2 = I_\alpha M_\alpha \tilde{P}_\alpha (\tilde{P}_\alpha M_\alpha I_\alpha^\dagger I_\alpha M_\alpha \tilde{P}_\alpha) \tilde{P}_\alpha M_\alpha I_\alpha^\dagger = I_\alpha M_\alpha \tilde{P}_\alpha (\tilde{P}_\alpha) \tilde{P}_\alpha M_\alpha I_\alpha^\dagger = \tilde{I}_\alpha \tilde{I}_\alpha^\dagger. \quad (\text{F.38})$$

This shows that $\tilde{I}_\alpha \tilde{I}_\alpha^\dagger$ is a projector, and hence $\tilde{I}_\alpha$ is a partial isometry.

To establish the range of $\tilde{I}_\alpha$ (i.e. on what subspace of $\bar{\alpha}$ does $\tilde{I}_\alpha \tilde{I}_\alpha^\dagger$ project onto), we first note that the range is contained in the no-EPR subspace on $\bar{\alpha}$. This follows because the insertion of any EPR projector inside the isometry yields zero,

$$\tilde{I}_\alpha^\dagger P_\gamma \tilde{I}_\alpha = \tilde{P}_\alpha M_\alpha I_\alpha^\dagger P_\gamma I_\alpha M_\alpha \tilde{P}_\alpha = \tilde{P}_\alpha M_\alpha P_{\alpha \cup \gamma} M_\alpha \tilde{P}_\alpha = 0, \quad (\text{F.39})$$

for all non-empty $\gamma \subseteq \bar{\alpha}$. The final expression is zero because $P_{\alpha \cup \gamma}$ has size $|\alpha| + |\gamma|$, which implies that $M_\alpha P_{\alpha \cup \gamma} M_\alpha$ is a sum of diagrams with size $|\alpha| + |\gamma|$, all of which vanish after conjugation by $\tilde{P}_\alpha$. Hence, the range of $\tilde{I}_\alpha$ is contained in the orthogonal complement of $\text{span}(\{P_\gamma : \gamma \subseteq \bar{\alpha}\})$ on $\bar{\alpha}$, which is the definition of the no-EPR subspace. To show that the range is equal to the no-EPR subspace, we simply note that the ranks of $\Pi_{\bar{\alpha}}^{\text{nE}}$ (restricted to subspace $\bar{\alpha}$) and $\tilde{I}_\alpha \tilde{I}_\alpha^\dagger$ are equal via Proposition 7. Namely, we apply Proposition 7 for p, q, ℓ for $\tilde{P}_\alpha$, and for $p - \ell, q - \ell, 0$ for $\Pi_{\bar{\alpha}}^{\text{nE}}$. The rank of $\tilde{I}_\alpha \tilde{I}_\alpha^\dagger$ is equal to the rank of $\tilde{P}_\alpha = \tilde{I}_\alpha^\dagger \tilde{I}_\alpha$ since $\tilde{I}_\alpha$ is an isometry. Thus, we have $\tilde{I}_\alpha \tilde{I}_\alpha^\dagger = \Pi_{\bar{\alpha}}^{\text{nE}}$, as claimed.

Finally, the isometry is unitary-equivariant,

$$\tilde{I}_\alpha \mathcal{U}_q^p = I_\alpha M_\alpha \tilde{P}_\alpha \mathcal{U}_q^p = \mathcal{U}_{q-\ell}^{p-\ell} I_\alpha M_\alpha \tilde{P}_\alpha = \mathcal{U}_{q-\ell}^{p-\ell} \tilde{I}_\alpha, \quad (\text{F.40})$$

since $\mathcal{U}_q^p$ commutes with $\tilde{P}_\alpha$ and M_α , and I_α is unitary-equivariant. The fact that $\mathcal{U}_q^p$ commutes with M_α follows because the square of M_α can be written as a sum of diagrams, and if A and B commute, then A and $\sqrt{B}$ also commute, for any A, B . $\square$

F.2 Additional results on the mixed Haar twirl

In this section, we present several additional results on the objects appearing in the mixed Haar twirl. These results are not used in any of our main results in either the main text or the appendices. They were derived during an early unsuccessful attempt to prove the strong gluing lemma using only properties of the partially transposed permutations. This attempt was aborted and replaced with the current proof via the path-recording framework after the introduction of this framework by Ref. [42]. We include these results here in case they may be useful in future work on the mixed Haar twirl or partially transposed permutations.

F.2.1 Approximate orthogonality of the EPR projectors

The main result of this section is a proof that the “nearly-orthogonal” projectors defined in Appendix F are indeed nearly orthogonal, whenever the Hilbert space dimension D is large. This implies that the nearly-orthogonal projectors are approximately equal to the orthogonal projectors, $P_\alpha^{\text{nE}} \approx \tilde{P}_\alpha$. This can enable much easier analyses owing to the simpler definition of each P_α^{nE} .

To quantify the orthogonality of the nearly-orthogonal projectors, for each ℓ , we define the $\binom{p}{\ell} \binom{q}{\ell} \ell! \times \binom{p}{\ell} \binom{q}{\ell} \ell!$ matrix with elements,

$$G_{\alpha\beta}^{(\ell)} = \begin{cases} \|P_\alpha^{\text{nE}} P_\beta^{\text{nE}}\|_\infty, & \alpha \neq \beta, \\ 0, & \alpha = \beta. \end{cases} \quad (\text{F.41})$$

The matrix $\hat{G}^{(\ell)}$ would be zero if the projectors were perfectly orthogonal. We will show that in the limit of large D , its spectral norm is very small. For each $\ell' \leq \ell$, we also consider the $\binom{p}{\ell} \binom{q}{\ell} \ell! \times \binom{p}{\ell} \binom{q}{\ell} \ell!$ matrix with elements,

$$F_{\alpha\beta}^{(\ell, \ell')} = \begin{cases} \frac{1}{\binom{\ell}{\ell'}} \sum_{\gamma: |\gamma|=\ell'} \|P_\alpha^{\text{nE}} P_\gamma P_\beta^{\text{nE}}\|_\infty, & \alpha \neq \beta, \\ \frac{1}{\binom{\ell}{\ell'}} \sum_{\gamma: |\gamma|=\ell', \gamma \not\subseteq \alpha} \|P_\alpha^{\text{nE}} P_\gamma P_\alpha^{\text{nE}}\|_\infty, & \alpha = \beta. \end{cases} \quad (\text{F.42})$$

We will show that the spectral norm of this matrix is also small.

We can now formally state our result on the approximate orthogonality of the projectors.

Theorem 16 (Approximate orthogonality of EPR projectors). *The matrices $\hat{G}^{(\ell)}$ and $\hat{F}^{(\ell, \ell')}$ have small spectral norm,*

$$\|\hat{G}^{(\ell)}\|_\infty \leq e^{\frac{\ell(p+q)}{D}} - 1, \quad \text{and} \quad \|\hat{F}^{(\ell, \ell')}\|_\infty \leq e^{\frac{(\ell+\ell')(p+q)}{D}} - 1. \quad (\text{F.43})$$

for any $(p+q)^2 \leq D$.

From Theorem 16, we prove the following approximations for the orthogonal subspace projectors.

Corollary 3 (Approximate expressions for the orthogonal projectors). *The following approximations hold for any $(p+q)^2 \leq D$. First,*

$$\tilde{P}_\alpha = P_\alpha^{\text{nE}} + E_\alpha, \quad \text{with } \|E_\alpha\|_\infty \leq 2 \left(\frac{\ell(p+q)}{D} \right) + 10.78 \left(\frac{\ell(p+q)}{D} \right)^2, \quad (\text{F.44})$$

where $E_\alpha = \tilde{P}_\ell E_\alpha \tilde{P}_\ell$ and $\ell = |\alpha|$. Second,

$$\tilde{P}_\ell = P_\ell^{\text{nE}} + E_\ell, \quad \text{with } \|E_\ell\|_\infty \leq \left(\frac{\ell(p+q)}{D} \right) + 10.18 \left(\frac{\ell(p+q)}{D} \right)^2, \quad (\text{F.45})$$

where $E_\ell = \tilde{P}_\ell E_\ell \tilde{P}_\ell$. Third, for each ℓ' ,

$$\sum_{\ell \geq \ell'} \binom{\ell}{\ell'} \tilde{P}_\ell = \sum_{\gamma: |\gamma|=\ell'} P_\gamma + \sum_{\ell \geq \ell'} \binom{\ell}{\ell'} E_\ell^{(\ell')}, \quad \text{with } \|E_\ell^{(\ell')}\|_\infty \leq \left(\frac{(\ell + \ell')(p + q)}{D} \right) + 7.06 \left(\frac{(\ell + \ell')(p + q)}{D} \right)^2 \quad (\text{F.46})$$

where $E_\ell^{(\ell')} = \tilde{P}_\ell E_\ell^{(\ell')} \tilde{P}_\ell$ for each ℓ .

We remark that the error bounds in Eqs. (F.45) and (F.46) are much tighter than would be obtained from applying Eq. (F.44) term by term.

The final result in Corollary 3, Eq. (F.46), is especially notable in the case $\ell = 1$. For this value of ℓ' , the equation simplifies to

$$N_E \equiv \sum_{\ell \geq \ell'} \ell \tilde{P}_\ell = \sum_{\gamma: |\gamma|=1} P_\gamma + \sum_{\ell \geq \ell'} \ell E_\ell, \quad (\text{F.47})$$

where we define N_E to equal the left hand side. The operator N_E simply counts the number of EPR pairs ℓ in a state. From Corollary 3, we see N_E can be approximated as a sum over all two-wise EPR projectors P_γ .

F.2.2 Bound on the inverse Weingarten sub-matrix

To establish our bounds in the previous section, we utilize the following bound on the inverse sub-matrix of the Weingarten matrix, whenever the Hilbert space dimension D is large. This bound will be useful since the inverse sub-matrix appears in the expression for the no-EPR projector (Proposition 8).

Lemma 35 (Bound on the inverse Weingarten sub-matrix). *For any $(p + q)^2 \leq D/2$. The sum of the absolute values of the matrix elements of the inverse of $\hat{W}g_{\text{perm}}$ are bounded as*

$$\frac{1}{p!q!} \sum_{\pi, \tilde{\pi}} \left| \delta_{\pi, \tilde{\pi}} - \frac{1}{D^{p+q}} [\hat{W}g_{\text{perm}}^{-1}]_{\pi, \tilde{\pi}} \right| \leq 2 \frac{(p + q)^2}{D}, \quad (\text{F.48})$$

where we abbreviate $\pi = \pi_L \otimes \pi_R$, $\tilde{\pi} = \tilde{\pi}_L \otimes \tilde{\pi}_R$.

Proof. Since $\hat{W}g|_{\text{perm}}$ is a sub-matrix of $\hat{W}g$, its maximum eigenvalue is upper bounded by the maximum eigenvalue of $\hat{W}g$, and its minimum eigenvalue is lower bounded by the minimum eigenvalue of $\hat{W}g$. This follows since $v^T \hat{W}g v = v|_{\text{perm}}^T \hat{W}g|_{\text{perm}} v|_{\text{perm}}$ for any vector v with support only on the permutation operators. From Ref. [96], the maximum eigenvalue of $\hat{W}g$ is less than $1 + (p + q)^2/D$ and the minimum eigenvalue of $\hat{W}g$ is greater than $1 - (p + q)^2/D$. Hence, the eigenvalues of $\hat{W}g|_{\text{perm}}$ are bounded by these values.

Since the eigenvalues are bounded away from zero, the matrix inverse of $\hat{W}g|_{\text{perm}}$ can be Taylor expanded,

$$\hat{W}g|_{\text{perm}}^{-1} = \sum_{m=0}^{\infty} (\mathbb{1} - \hat{W}g|_{\text{perm}})^m. \quad (\text{F.49})$$

Subtracting this expression from the identity matrix, the $m = 0$ term is canceled, and so we have

$$\mathbb{1} - \hat{W}g|_{\text{perm}}^{-1} = - \sum_{m=1}^{\infty} (\mathbb{1} - \hat{W}g|_{\text{perm}})^m. \quad (\text{F.50})$$

We can bound our quantity of interest, the sum of absolute value matrix elements on the left, by a series of similar sums on the right,

$$\frac{1}{p!q!} \sum_{\pi, \tilde{\pi}} \left| \delta_{\pi, \tilde{\pi}} - \frac{1}{D^{p+q}} [\hat{W}_{\text{g|perm}}^{-1}]_{\pi, \tilde{\pi}} \right| \leq \sum_{m=1}^{\infty} \left(\frac{1}{p!q!} \sum_{\pi, \tilde{\pi}} \left| [(\mathbb{1} - \hat{W}_{\text{g|perm}})^m]_{\pi, \tilde{\pi}} \right| \right), \quad (\text{F.51})$$

which follows from the triangle inequality.

To evaluate the terms within parentheses on the right hand side, we recall that the matrix elements of $\hat{W}_{\text{g|perm}}$ have an alternating pattern of signs, $(-1)^{|\pi_L|+|\pi_R|}$. If we define the diagonal matrix $\hat{P}$ element-wise via $P_{\pi, \pi} = (-1)^{|\pi_L|+|\pi_R|}$, this implies that $\hat{P}\hat{W}_{\text{g|perm}}\hat{P}$ has all positive entries [103]. Since the diagonal elements of $\hat{W}_{\text{g|perm}}$ are greater than one, we further have that $\hat{P}(\hat{W}_{\text{g|perm}} - \mathbb{1})\hat{P}$ has all positive entries [36, 104]. Taking the m -th power, we find that $(\hat{P}(\hat{W}_{\text{g|perm}} - \mathbb{1})\hat{P})^m = \hat{P}(\hat{W}_{\text{g|perm}} - \mathbb{1})^m\hat{P}$ has all positive entries as well. The elements of these matrices have the same absolute values as the elements of the terms $(\mathbb{1} - \hat{W}_{\text{g|perm}})^m$. Hence, the sum over the absolute value of the matrix elements of the latter is equal to the same sum for the former.

The sum over matrix elements of $\hat{P}(\hat{W}_{\text{g|perm}} - \mathbb{1})^m\hat{P}$ is easy to evaluate, since the matrix has all positive elements. By the Perron-Frobenius theorem and the fact that the matrix is invariant under permutations, the maximum eigenvector of $\hat{P}(\hat{W}_{\text{g|perm}} - \mathbb{1})^m\hat{P}$ is the constant vector, $v_{\pi} = 1/\sqrt{p!q!}$ [36]. Hence, the maximum eigenvalue is equal to

$$v^T \left(\hat{P}(\hat{W}_{\text{g|perm}} - \mathbb{1})^m\hat{P} \right) v = \frac{1}{p!q!} \sum_{\pi, \tilde{\pi}} \left| [(\mathbb{1} - \hat{W}_{\text{g|perm}})^m]_{\pi, \tilde{\pi}} \right|, \quad (\text{F.52})$$

which is precisely the sum we would like to bound. From the above expression, we immediately have

$$\frac{1}{p!q!} \sum_{\pi, \tilde{\pi}} \left| [(\mathbb{1} - \hat{W}_{\text{g|perm}})^m]_{\pi, \tilde{\pi}} \right| \leq \left\| \hat{P}(\hat{W}_{\text{g|perm}} - \mathbb{1})^m\hat{P} \right\|_{\infty} = \left\| (\hat{W}_{\text{g|perm}} - \mathbb{1})^m \right\|_{\infty} \leq \left\| \hat{W}_{\text{g|perm}} - \mathbb{1} \right\|_{\infty}^m.$$

We have $\|\hat{W}_{\text{g|perm}} - \mathbb{1}\|_{\infty} \leq (p+q)^2/D$ from our discussion of the eigenvalues of $\hat{W}_{\text{g|perm}}$. Hence, the right side is less than $((p+q)^2/D)^m$.

We can complete our proof by inserting this bound into the Taylor series and performing the sum over m . This yields,

$$\frac{1}{p!q!} \sum_{\pi, \tilde{\pi}} \left| \delta_{\pi, \tilde{\pi}} - \frac{1}{D^{p+q}} [\hat{W}_{\text{g|perm}}^{-1}]_{\pi, \tilde{\pi}} \right| \leq \sum_{m=1}^{\infty} \left(\frac{(p+q)^2}{D} \right)^m = \frac{(p+q)^2/D}{1 - (p+q)^2/D} \leq 2(p+q)^2/D, \quad (\text{F.53})$$

where the final inequality holds if $(p+q)^2 \leq D/2$. This completes our proof. $\square$

F.2.3 Proof of Theorem 16: Approximate orthogonality of EPR projectors

Both $\hat{G}^{(\ell)}$ and $\hat{F}^{(\ell, \ell')}$ have entirely positive matrix elements. The Perron-Frobenius theorem then states that the maximum eigenvalue of each matrix is achieved by an eigenvector with entirely positive elements. Moreover, both $\hat{G}^{(\ell)}$ and $\hat{F}^{(\ell, \ell')}$ possess a “permutation symmetry”,

$$G_{\alpha\beta}^{(\ell)} = \|\pi P_{\alpha}^{\text{nE}} P_{\beta}^{\text{nE}}\|_{\infty} = \|\pi P_{\alpha}^{\text{nE}} \pi^{-1} \pi P_{\beta}^{\text{nE}} \pi^{-1}\|_{\infty} = \|P_{\pi(\alpha)}^{\text{nE}} P_{\pi(\beta)}^{\text{nE}}\|_{\infty} = G_{\pi(\alpha)\pi(\beta)}^{(\ell)}, \quad (\text{F.54})$$

and similar for $\hat{F}^{(\ell, \ell')}$. Here, $\pi = \pi_L \otimes \pi_R$ is any tensor product of permutations on the left and right side. Without loss of generality, we can assume that the maximum eigenvector, v_{α} , is invariant under the permutation symmetry, $v_{\alpha} = v_{\pi(\alpha)}$ for any π . (If not, we simply average the maximum

eigenvector over all of its possible permutations, which produces a symmetric vector with the same eigenvalue.) Since for every α, β , there exists a permutation π such that $\pi(\alpha) = \beta$, we have $v_\alpha = v_\beta$ for all α, β . Hence, the maximum eigenvalues of $\hat{G}^{(\ell)}$ and $\hat{F}^{(\ell, \ell')}$ are achieved by the constant vector, $v_\alpha = 1/(\sum_\alpha 1)^{1/2}$.

Proof of the first statement, Eq. (F.43) left. Let us begin with $\hat{G}$. From the above, the spectral norm is

$$\|\hat{G}\|_\infty = \frac{\sum_\alpha \sum_{\beta \neq \alpha} v_\beta G_{\beta\alpha} v_\alpha}{\sum_\alpha v_\alpha v_\alpha} = \frac{\sum_\alpha \sum_{\beta \neq \alpha} \|P_\alpha^{\text{nE}} P_\beta^{\text{nE}}\|_\infty}{\sum_\alpha 1} = \sum_{\beta \neq \alpha} \|P_\alpha^{\text{nE}} P_\beta^{\text{nE}}\|_\infty. \quad (\text{F.55})$$

In the final expression, α is fixed to an arbitrary value and β is summed over.

To proceed, we compute each term in the sum. Let $L(\beta, \alpha)$ denote the number of loops when the PTPs associated with P_β and P_α are multiplied, and let $\gamma_I \supseteq \beta$ and $\gamma_O \supseteq \alpha$ denote the input and output pairs of the PTP obtained from the multiplication. Then we have,

$$\|P_\beta^{\text{nE}} P_\alpha^{\text{nE}}\|_\infty = \begin{cases} D^{L(\beta, \alpha) - \ell}, & \text{if } \gamma_I = \beta \text{ and } \gamma_O = \alpha \\ 0, & \text{else.} \end{cases} \quad (\text{F.56})$$

We can illustrate this formula with three examples:

$$\text{Diagram 1} = 0, \quad \text{Diagram 2} = \frac{1}{D} \text{Diagram 3}, \quad \text{Diagram 4} = \frac{1}{D^2} \text{Diagram 5}$$

In the first example, the projectors multiply to zero because the red leg forms an EPR projector on $\bar{\beta}$. To derive Eq. (F.56), we write

$$\begin{aligned} P_\beta^{\text{nE}} P_\alpha^{\text{nE}} &= \Pi_\beta^{\text{nE}} P_\beta P_\alpha \Pi_\alpha^{\text{nE}} = D^{-2\ell} \Pi_\beta^{\text{nE}}(\beta, \beta, \mathbb{1}, \mathbb{1})(\alpha, \alpha, \mathbb{1}, \mathbb{1}) \Pi_\alpha^{\text{nE}} \\ &= D^{L(\beta, \alpha) - 2\ell} \Pi_\beta^{\text{nE}}(\gamma_I, \gamma_O, \pi_L, \pi_R) \Pi_\alpha^{\text{nE}}, \end{aligned} \quad (\text{F.57})$$

where $(\gamma_I, \gamma_O, \pi_L, \pi_R)$ is the PTP obtained by multiplying $(\beta, \beta, \mathbb{1}, \mathbb{1})$ and $(\alpha, \alpha, \mathbb{1}, \mathbb{1})$. The second clause in Eq. (F.56) follows because $(\gamma_I, \gamma_O, \pi_L, \pi_R)$ is annihilated by Π_β^{nE} if γ_I contains a pair in $\bar{\beta}$, and similar for Π_α^{nE} and γ_O . The first clause follows because the spectral norm of $\Pi_\beta^{\text{nE}}(\gamma_I, \gamma_O, \pi_L, \pi_R) \Pi_\alpha^{\text{nE}}$ is one if $\gamma_I = \beta, \gamma_O = \alpha$. We note that this condition implies $|\alpha| = |\beta|$, since $|\gamma_I| = |\gamma_O|$.

To bound the sum in Eq. (F.55), we count the number of sets of pairs α that have spectral norm $\|P_\beta^{\text{nE}} P_\alpha^{\text{nE}}\|_\infty = D^{L-\ell}$ with a fixed set of pairs β , for each value of L . Let us denote this number as $N(L, \ell)$. Recall that α is a sequence of ℓ pairs of indices. To determine $N(L, \ell)$, we enumerate the possible α pair-by-pair, as depicted below.

$$\text{Diagram 1} \leftrightarrow \text{Diagram 2} \rightarrow \text{Diagram 3} \rightarrow \text{Diagram 4} \quad (\text{F.58})$$

In more detail, let $\beta^{(0)} = \beta$ consider the “right half” of P_α^{nE} , the isometry $I_\alpha^{\text{nE}} = \Pi_\alpha^{\text{nE}} \otimes \langle E_\alpha |$. The first pair, α_1 , can be placed on any left and any right index, as long as at least one of the indices is contained in $\beta^{(0)}$. (If neither index is contained in $\beta^{(0)}$, then the pair is annihilated by the no-EPR

projector Π_{β}^{nE} .) There are at most $\ell(p+q)$ possible choices of the first pair, since: the index in $\beta^{(0)}$ can come from either the left or right side; on that side, the index corresponds to one of ℓ pairs; and on the other side, the index can be any of either q or p values. Among these possible choices, there are ℓ possible choices of the first pair that produce a loop, since $\beta^{(0)}$ has ℓ pairs.

After the first pair is chosen, we can take the product of P_{β}^{nE} and $|E_{\alpha_1}\rangle$ to obtain a new projector $P_{\beta^{(1)}}^{\text{nE}}$. The new set $P_{\beta^{(1)}}^{\text{nE}}$ acts on $p-1, q-1$ indices, and $\beta^{(1)}$ always contains one fewer pair than $\beta^{(0)}$. To verify the latter statement, note that there are three possible classes of pairs α_1 that can be added. The first class connects one index of a pair in β to one index in $\bar{\beta}$. This action annihilates the pair, and thus reduces the total number of pairs by one. The second class connects one index of a pair in β to another index of another pair in β . This action joins the two pairs, and thus also reduces the number of pairs by one. The final class connects two indices of the same pair in β , producing a loop. Again, this reduces the total number of pairs by one.

We can iterate this process ℓ times to enumerate all possible sequences, α , of ℓ pairs, such that $P_{\beta}^{\text{nE}} P_{\alpha}^{\text{nE}}$ is non-zero. At the j -th step, for $j = 1, \dots, \ell$, there are $(\ell-j+1)(p+q)$ total possible choices for the j -th pair, and, among these, $(\ell-j+1)$ possible choices that produce a loop. At the end of the process, each set of pairs α is over-counted a total of $\ell!$ times, corresponding to the possible orderings of the pairs in α . If one wishes to consider only α that produce exactly L loops, there are $\binom{\ell}{L} = \binom{\ell}{\ell-L}$ possible choices of L steps at which to produce a loop. Putting these three facts together, we have that there are at most,

$$N(L, \ell) \leq \ell! \cdot (p+q)^{\ell-L} \cdot \frac{1}{\ell!} \cdot \binom{\ell}{\ell-L} \leq \frac{\ell^{\ell-L} (p+q)^{\ell-L}}{(\ell-L)!}, \quad (\text{F.59})$$

possible α that produce L loops.

This counting immediately enables us to bound our desired sum,

$$\|\hat{G}\|_{\infty} \leq \sum_{\alpha \neq \beta} \|P_{\beta}^{\text{nE}} P_{\alpha}^{\text{nE}}\|_{\infty} = \sum_{L=1}^{\ell-1} N(L, \ell) D^{-(\ell-L)} \leq \sum_{L=0}^{\ell-1} \frac{1}{(\ell-L)!} \left(\frac{\ell(p+q)}{D} \right)^{\ell-L} \leq e^{\frac{\ell(p+q)}{D}} - 1.$$

The upper bound of the second sum is $\ell-1$ and not ℓ because $\alpha = \beta$ is the sole choice of α that yields ℓ pairs, and this choice is excluded in the first sum.

Proof of the second statement, Eq. (F.43) right. We now turn to $\hat{F}$. The spectral norm is

$$\|\hat{F}\|_{\infty} = \frac{\sum_{\alpha\beta\gamma} v_{\beta} F_{\beta\alpha} v_{\alpha}}{\sum_{\alpha} v_{\alpha} v_{\alpha}} = \sum_{\gamma} \sum_{\beta \neq \alpha} \|P_{\alpha}^{\text{nE}} P_{\gamma} P_{\beta}^{\text{nE}}\|_{\infty} + \sum_{\gamma \not\subseteq \alpha} \|P_{\alpha}^{\text{nE}} P_{\gamma} P_{\alpha}^{\text{nE}}\|_{\infty}. \quad (\text{F.60})$$

To bound the right hand side, we proceed similarly to our analysis for $\hat{G}$, and enumerate all possible γ, β that give a non-zero value of $\|P_{\alpha}^{\text{nE}} P_{\gamma} P_{\beta}^{\text{nE}}\|_{\infty}$. We begin with γ and proceed pair-by-pair as before. Let $\alpha^{(0)} = \alpha$ and $I_{\alpha^{(0)}}^{\text{nE}} = \Pi_{\bar{\alpha}^{(0)}}^{\text{nE}} \otimes \langle E_{\alpha^{(0)}} |$. We place the first pair, γ_1 , on any two of the $p+q$ indices, so long as at least one of the indices is in $\alpha^{(0)}$. (If it is not, then both indices of the pair are in $\bar{\alpha}^{(0)}$, and so are annihilated by the no-EPR projector in $I_{\alpha^{(0)}}^{\text{nE}}$.) This produces a new isometry, $I_{\alpha^{(1)}}^{\text{nE}} = I_{\alpha^{(0)}}^{\text{nE}} |E_{\gamma_1}\rangle$, acting on $p+q-2$ copies with $\ell-1$ EPR projectors, as depicted in Eq. (F.58). We iterate this procedure $j = 1, \dots, \ell'$ times to generate all valid γ with ℓ' pairs. At the j -th step, there are $(\ell-j+1)(p+q-2j)$ possible locations at which to place the j -th pair, and, among these, $(\ell-j+1)$ possible locations that produce a loop. In total, each γ is over-counted a total of $\ell'!$ times, corresponding to the possible orderings of the ℓ' pairs in γ .

At the end of the process above, we obtain an isometry $I_{\alpha^{(\ell')}}^{\text{nE}} = I_{\alpha}^{\text{nE}} |E_{\gamma}\rangle$ acting on $p+q-2\ell'$ copies, with $\ell-\ell'$ EPR projectors. The isometry is given by multiplying the “right half” of P_{α}^{nE} with

the “left half” of P_γ . To proceed to enumerate the valid β , let us multiply this isometry by the “right half” of P_γ , to obtain $I_{\delta(0)}^{\text{nE}} \equiv I_\alpha^{\text{nE}} |E_\gamma\rangle\langle E_\gamma| = I_\alpha^{\text{nE}} P_\gamma$. The isometry $I_{\delta(0)}^{\text{nE}}$ acts on $p+q$ copies with ℓ EPR projectors. We can now enumerate the possible β pair-by-pair, exactly as we did in our analysis of $\hat{G}$. At the j -th step, for $j = 1, \dots, \ell$, there are $(\ell - j + 1)(p + q - 2j)$ possible locations at which to place the j -th pair, and, among these, $(\ell - j + 1)$ possible locations that produce a loop. Each β is over-counted a total of $\ell!$ times, corresponding to the possible orderings of the ℓ pairs in β .

We can now count the total number of γ, β that produce L loops in the multiplication $P_\alpha^{\text{nE}} P_\gamma P_\beta^{\text{nE}}$. Since the enumeration of γ, β contained a total of $\ell' + \ell$ steps, there are $\binom{\ell' + \ell}{L} = \binom{\ell' + \ell}{\ell' + \ell - L}$ possible choices of L steps at which to produce a loop. Thus, we have that there are at most

$$N(L, \ell, \ell') \leq \frac{\ell!}{(\ell - \ell')!} \cdot \ell! \cdot (p + q)^{\ell' + \ell - L} \cdot \frac{1}{\ell'!} \cdot \frac{1}{\ell!} \cdot \binom{\ell' + \ell}{\ell' + \ell - L} \leq \binom{\ell}{\ell'} \frac{(\ell' + \ell)^{\ell' + \ell - L} (p + q)^{\ell' + \ell - L}}{(\ell' + \ell - L)!},$$

possible choices of γ, β that produce L loops.

Turning to the sum in Eq. (F.60), we have

$$\begin{aligned} \|\hat{F}\|_\infty &\leq \frac{1}{\binom{\ell}{\ell'}} \left(\sum_\gamma \sum_{\beta \neq \alpha} \|P_\alpha^{\text{nE}} P_\gamma P_\beta^{\text{nE}}\|_\infty + \sum_{\gamma \not\subseteq \alpha} \|P_\alpha^{\text{nE}} P_\gamma P_\alpha^{\text{nE}}\|_\infty \right) \\ &= \frac{1}{\binom{\ell}{\ell'}} \sum_{L=1}^{\ell' + \ell - 1} N(L, \ell, \ell') D^{-(\ell' + \ell - L)} \\ &\leq \sum_{L=0}^{\ell' + \ell - 1} \frac{1}{(\ell' + \ell - L)!} \left(\frac{(\ell' + \ell)(p + q)}{D} \right)^{\ell' + \ell - L} \\ &\leq \left(e^{\frac{(\ell' + \ell)(p + q)}{D}} - 1 \right). \end{aligned} \tag{F.61}$$

The upper bound of the second sum is $\ell' + \ell - 1$ and not $\ell' + \ell$ because $\beta = \alpha$, $\gamma \subseteq \alpha$ is the sole choice of γ, β that yields $\ell' + \ell$ pairs, and this choice is excluded in the first sum. $\square$

F.2.4 Proof of Corollary 3: Approximate expressions for subspace projectors

As a starting point, we consider a normalized vector $|\psi\rangle \in \tilde{P}_\ell$. By construction, we can write $|\psi\rangle$ as a sum of vectors from each partly-orthogonal subspace α of size ℓ ,

$$|\psi\rangle = \sum_\alpha c_\alpha |\psi_\alpha\rangle = \sum_\alpha c_\alpha |E_\alpha\rangle \otimes |\phi_{\bar{\alpha}}\rangle, \tag{F.62}$$

where each normalized state $|\psi_\alpha\rangle \equiv |E_\alpha\rangle \otimes |\phi_{\bar{\alpha}}\rangle$ is orthogonal to all EPR projectors on $\bar{\alpha}$.

Let us first understand how the normalization of $|\psi\rangle$ is related to the coefficients c_α . We have

$$1 = \langle \psi | \psi \rangle = \sum_\alpha |c_\alpha|^2 + \sum_{\alpha \neq \beta} c_\beta^* c_\alpha \langle \psi_\beta | \psi_\alpha \rangle. \tag{F.63}$$

We can use Theorem 16 to show that the second sum is small,

$$\left| \sum_{\alpha \neq \beta} c_\beta^* c_\alpha \langle \psi_\beta | \psi_\alpha \rangle \right| \leq \sum_{\alpha \neq \beta} |c_\beta| |c_\alpha| \|P_\beta^{\text{nE}} P_\alpha^{\text{nE}}\|_\infty \leq \left(\sum_\alpha |c_\alpha|^2 \right) \cdot \|\hat{G}\|_\infty, \tag{F.64}$$

where the first step follows from the triangle inequality as well as the expression, $|\langle \psi_\beta | \psi_\alpha \rangle| = |\langle \psi_\beta | P_\beta^{\text{nE}} P_\alpha^{\text{nE}} | \psi_\alpha \rangle| \leq \|P_\beta^{\text{nE}} P_\alpha^{\text{nE}}\|_\infty$. Combining Eq. (F.63) and Eq. (F.64) gives

$$e^{-\ell(p+q)/D} \leq \frac{1}{1 + \|\hat{G}\|_\infty} \leq \sum_\alpha |c_\alpha|^2 \leq \frac{1}{1 - \|\hat{G}\|_\infty} \leq \frac{1}{2 - e^{\ell(p+q)/D}}, \tag{F.65}$$

where the outer inequalities follow from Theorem 16. We see that the coefficients are approximately normalized to one, as would be the case if the projectors were perfectly orthogonal.

Proof of the first statement, Eq. (F.44). By definition, both $\tilde{P}_\alpha$ and P_α^{nE} are orthogonal to all subspaces $\tilde{P}_\beta$ with $|\beta| \neq \ell$, or with $|\beta| = \ell$ but $\beta > \alpha$ with respect to the ordering of the orthogonal projectors. Hence, $E_\alpha = \tilde{P}_\ell E_\alpha \tilde{P}_\ell$, and we can restrict our attention to the action of E_α on states in $\text{span}\{\tilde{P}_\beta : |\beta| = \ell, \beta \leq \alpha\}$. Building upon the decomposition in Eq. (F.62), we write

$$|\psi\rangle = c_\alpha |\psi_\alpha\rangle + \sum_{\alpha' \neq \alpha} c_{\alpha'} |\psi_{\alpha'}\rangle = c_\alpha \left(b_\alpha |\tilde{\psi}_\alpha\rangle + \sum_{\alpha' < \alpha} b_{\alpha'} |\tilde{\psi}_{\alpha'}\rangle \right) + \sum_{\alpha' < \alpha} c_{\alpha'} |\psi_{\alpha'}\rangle, \quad (\text{F.66})$$

where on the right hand side, we decompose $|\psi_\alpha\rangle$, which lies in P_α^{nE} , as a sum of vectors, $|\tilde{\psi}_\alpha\rangle, |\tilde{\psi}_{\alpha'}\rangle$, which lie in $\tilde{P}_\alpha, \tilde{P}_{\alpha'}$ for $\alpha' < \alpha$. We have

$$P_\alpha^{\text{nE}} |\psi\rangle = c_\alpha |\psi_\alpha\rangle + \sum_{\alpha' < \alpha} c_{\alpha'} P_\alpha^{\text{nE}} |\psi_{\alpha'}\rangle, \quad (\text{F.67})$$

and

$$\tilde{P}_\alpha |\psi\rangle = c_\alpha b_\alpha |\tilde{\psi}_\alpha\rangle. \quad (\text{F.68})$$

Taking the difference, we have

$$E_\alpha |\psi\rangle = c_\alpha \sum_{\alpha' < \alpha} b_{\alpha'} |\tilde{\psi}_{\alpha'}\rangle + \sum_{\alpha' < \alpha} c_{\alpha'} P_\alpha^{\text{nE}} |\psi_{\alpha'}\rangle. \quad (\text{F.69})$$

We will now show that $E_\alpha |\psi\rangle$ has small norm.

The second term has norm at most,

$$\left\| \sum_{\alpha' < \alpha} c_{\alpha'} P_\alpha^{\text{nE}} |\psi_{\alpha'}\rangle \right\| \leq \sum_{\alpha' < \alpha} |c_{\alpha'}| \cdot \|P_\alpha^{\text{nE}} P_{\alpha'}^{\text{nE}}\|_\infty \leq \left(\sum_{\alpha' < \alpha} |c_{\alpha'}|^2 \right)^{1/2} \|\hat{G}^{(\ell)}\|_\infty \leq \frac{\|\hat{G}^{(\ell)}\|_\infty}{1 - \|\hat{G}^{(\ell)}\|_\infty}, \quad (\text{F.70})$$

where $\|\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$ denotes the vector norm, and the final inequality follows from Eq. (F.65). To bound the first term, we note that

$$\left\| \sum_{\alpha' < \alpha} b_{\alpha'} |\tilde{\psi}_{\alpha'}\rangle \right\| = \max_{|\phi_{<\alpha}\rangle} |\langle\phi_{<\alpha}|\psi_\alpha\rangle|, \quad (\text{F.71})$$

where the maximization is over all states $|\phi_{<\alpha}\rangle$ in the subspace $\text{span}\{P_{\alpha'} : \alpha' < \alpha\}$. The equation follows since the vector on the left hand side is the projection of $|\psi_\alpha\rangle$ onto the subspace. Performing an analogous decomposition for $|\phi_\alpha\rangle$ as in Eq. (F.62), with coefficients $d_{\alpha'}$, we have

$$|\langle\phi_{<\alpha}|\psi_\alpha\rangle| = \left| \sum_{\alpha' < \alpha} d_{\alpha'} \langle\phi_{\alpha'}|\psi_\alpha\rangle \right| \leq \sum_{\alpha' < \alpha} |d_{\alpha'}| \cdot \|P_{\alpha'}^{\text{nE}} P_\alpha^{\text{nE}}\|_\infty \leq \left(\sum_{\alpha' < \alpha} |d_{\alpha'}|^2 \right)^{1/2} \|\hat{G}^{(\ell)}\|_\infty \leq \frac{\|\hat{G}^{(\ell)}\|_\infty}{1 - \|\hat{G}^{(\ell)}\|_\infty},$$

where the final inequality follows from Eq. (F.65). Applying Theorem 16 yields Eq. (F.44),

$$\|E_\alpha\|_\infty \leq \frac{2\|\hat{G}^{(\ell)}\|_\infty}{1 - \|\hat{G}^{(\ell)}\|_\infty} \leq \frac{e^{\ell(p+q)/D} - 1}{1 - \frac{1}{2}e^{\ell(p+q)/D}} \leq 2\left(\frac{\ell(p+q)}{D}\right) + 10.78\left(\frac{\ell(p+q)}{D}\right)^2, \quad (\text{F.72})$$

where in the final inequality we use $(e^x - 1)/(1 - e^x/2) \leq 2x + 10.78x^2$ for $0 \leq x \leq 1/2$, from Taylor's remainder theorem.

Proof of the second statement, Eq. (F.45). Similar to before, both $\tilde{P}_\ell$ and all P_α^{nE} with $|\alpha| = \ell$ are orthogonal to all subspaces $\tilde{P}_\beta$ with $|\beta| \neq \ell$. Hence, $E_\ell = \tilde{P}_\ell E_\ell \tilde{P}_\ell$, and we can restrict our attention to the action of E_ℓ on states in $\tilde{P}_\ell$. To bound the magnitude of E_ℓ , we recall the definition of the spectral norm,

$$\|E_\ell\|_\infty \equiv \max_{|\psi\rangle, |\phi\rangle} \langle\psi| E_\ell |\phi\rangle, \quad (\text{F.73})$$

where we can assume $|\psi\rangle, |\phi\rangle \in \tilde{P}_\ell$. Now, we expand $|\psi\rangle$ and $|\phi\rangle$ as in Eq. (F.62), $|\psi\rangle = \sum_{\alpha:|\alpha|=\ell} c_\alpha |\psi_\alpha\rangle$ and $|\phi\rangle = \sum_{\alpha:|\alpha|=\ell} d_\alpha |\phi_\alpha\rangle$. We have

$$\langle\psi| \tilde{P}_\ell |\phi\rangle = \langle\psi|\phi\rangle = \sum_{\gamma,\alpha} c_\alpha^* d_\beta \langle\psi_\alpha|\phi_\beta\rangle, \quad (\text{F.74})$$

since $\tilde{P}_\ell |\phi\rangle = |\phi\rangle$ by assumption. Meanwhile, we have

$$\langle\psi| \left(\sum_{\gamma:|\gamma|=\ell} P_\gamma^{\text{nE}} \right) |\phi\rangle = \sum_{\alpha\beta\gamma} c_\alpha^* d_\beta \langle\psi_\alpha| P_\gamma^{\text{nE}} |\phi_\beta\rangle = \langle\psi|\phi\rangle + \sum_{\alpha,\beta,\gamma \neq \beta} c_\alpha^* d_\beta \langle\psi_\alpha| P_\gamma^{\text{nE}} |\phi_\beta\rangle, \quad (\text{F.75})$$

where in the third expression we use that $P_\gamma^{\text{nE}} |\psi_\beta\rangle = |\psi_\beta\rangle$ for $\gamma = \beta$. Taking the difference of the two expressions, and applying the triangle inequality, we have

$$|\langle\psi| E_\ell |\phi\rangle| = \sum_{\alpha,\beta,\gamma \neq \beta} c_\alpha^* d_\beta \langle\psi_\alpha| P_\gamma^{\text{nE}} |\phi_\beta\rangle \leq \sum_{\alpha,\beta,\gamma \neq \beta} |c_\alpha| \cdot \|P_\alpha^{\text{nE}} P_\gamma^{\text{nE}}\|_\infty \cdot \|P_\gamma^{\text{nE}} P_\beta^{\text{nE}}\|_\infty \cdot |d_\beta|. \quad (\text{F.76})$$

We can view the second norm, $\|P_\gamma^{\text{nE}} P_\beta^{\text{nE}}\|_\infty$, as the elements of the matrix $\hat{G}^{(\ell)}$, since the diagonal elements, $\gamma = \beta$, are omitted. We can view the first norm, $\|P_\alpha^{\text{nE}} P_\gamma^{\text{nE}}\|_\infty$, as the elements of the matrix, $\hat{\mathbb{1}} + \hat{G}^{(\ell)}$, since it contains its diagonal elements, $\|P_\alpha^{\text{nE}} P_\alpha^{\text{nE}}\|_\infty = 1$. Hence, we have

$$|\langle\psi| E_\ell |\phi\rangle| \leq \left(\sum_\alpha |c_\alpha|^2 \right)^{1/2} \left(\sum_\beta |d_\beta|^2 \right)^{1/2} (1 + \|\hat{G}\|_\infty) \|\hat{G}\|_\infty, \quad (\text{F.77})$$

Applying Eq. (F.65) and Theorem 16 yields Eq. (F.45),

$$\|E_\ell\|_\infty \leq \frac{(1 + \|\hat{G}^{(\ell)}\|_\infty) \|\hat{G}^{(\ell)}\|_\infty}{1 - \|\hat{G}^{(\ell)}\|_\infty} \leq \frac{e^{\ell(p+q)/D} (e^{\ell(p+q)/D} - 1)}{2 - e^{\ell(p+q)/D}} \leq \left(\frac{\ell(p+q)}{D} \right) + 10.18 \left(\frac{\ell(p+q)}{D} \right)^2,$$

where in the final inequality we use $e^x(e^x - 1)/(2 - e^x) \leq x + 10.18x^2$ for $0 \leq x \leq 1/2$, from Taylor's remainder theorem.

Proof of the third statement, Eq. (F.46). Our proof follows in a similar manner to the second statement. Note that both the left hand side of Eq. (F.46), and the first term on the right hand side, commute $\tilde{P}_\ell$ for all ℓ (the latter follows from Proposition 6). Thus, the difference of the two terms can be written as a sum of error terms, $\binom{\ell}{\ell'} E_\ell^{(\ell')}$, within each subspace, $\tilde{P}_\ell$. To quantify each error, let us suppose $|\psi\rangle, |\phi\rangle \in \tilde{P}_\ell$, and write,

$$\langle\psi| \left(\sum_{\ell'' \geq \ell'} \binom{\ell''}{\ell'} \tilde{P}_{\ell''} \right) |\phi\rangle = \binom{\ell}{\ell'} \langle\psi|\phi\rangle. \quad (\text{F.78})$$

Meanwhile, expanding $|\psi\rangle, |\phi\rangle$ as in Eq. (F.62), we have

$$\langle\psi| \left(\sum_{\gamma:|\gamma|=\ell'} P_\gamma \right) |\phi\rangle = \sum_{\alpha\beta\gamma} c_\alpha^* d_\beta \langle\psi_\alpha| P_\gamma |\phi_\beta\rangle = \binom{\ell}{\ell'} \langle\psi|\phi\rangle + \sum_{\alpha,\beta,\gamma \not\subseteq \beta} c_\alpha^* d_\beta \langle\psi_\alpha| P_\gamma |\phi_\beta\rangle. \quad (\text{F.79})$$

Taking the difference and dividing by $\binom{\ell}{\ell'}$, we have

$$\|E_\ell^{(\ell')}\|_\infty = \left| \frac{1}{\binom{\ell}{\ell'}} \sum_{\alpha, \beta, \gamma \not\subseteq \beta} c_\alpha^* d_\beta \langle \psi_\alpha | P_\gamma | \phi_\beta \rangle \right| \leq \frac{1}{\binom{\ell}{\ell'}} \sum_{\alpha, \beta, \gamma \not\subseteq \beta} |c_\alpha| \cdot |d_\beta| \cdot \|P_\alpha^{\text{nE}} P_\gamma P_\beta^{\text{nE}}\|_\infty. \quad (\text{F.80})$$

We are free to add terms to the sum, in order for the indices that are summed over to match those in the matrix $\hat{F}^{(\ell, \ell')}$ [Eq. (F.42)]. Adding in terms where $\gamma \subseteq \beta$ for each $\beta \neq \alpha$, we find

$$\|E_\ell^{(\ell')}\|_\infty \leq \frac{1}{\binom{\ell}{\ell'}} \left(\sum_{\alpha, \beta \neq \alpha, \gamma} + \sum_{\alpha, \gamma \not\subseteq \alpha} \right) |c_\alpha| |d_\beta| \|P_\alpha^{\text{nE}} P_\gamma P_\beta^{\text{nE}}\|_\infty \leq \left(\sum_{\alpha} |c_\alpha|^2 \right)^{1/2} \left(\sum_{\alpha} |d_\alpha|^2 \right)^{1/2} \|\hat{F}^{(\ell, \ell')}\|_\infty.$$

Applying Eq. (F.65) and Theorem 16 yields Eq. (F.46),

$$\|E_\ell^{(\ell')}\|_\infty \leq \frac{\|\hat{F}^{(\ell, \ell')}\|_\infty}{1 - \|\hat{G}^{(\ell)}\|_\infty} \leq \frac{e^{(\ell + \ell')(p+q)/D} - 1}{2 - e^{\ell(p+q)/D}} \leq \left(\frac{(\ell + \ell')(p+q)}{D} \right) + 7.06 \left(\frac{(\ell + \ell')(p+q)}{D} \right)^2,$$

where in the final inequality we use $(e^y - 1)/(2 - e^x) \leq (y + 0.718y^2)(1 + 3.693x) \leq y + 7.06y^2$ for $0 \leq y \leq 1$, $0 \leq x \leq \min(y, 1/2)$, from Taylor's remainder theorem. $\square$

G Fast scrambling

In this Appendix, we provide full details on the applications of strong random unitaries to quantum information scrambling. As mentioned in the main text, each of our results follows fairly immediately from the definition of strong unitary k -designs and strong PRUs.

G.1 Out-of-time-order correlation functions

Let U be a random unitary and $|\psi\rangle$ a fixed quantum state. A time-ordered $2k$ -point correlation function takes the form,

$$C_{\text{TO}}(P_1, \dots, P_{2k}) = \langle \psi | P_{2k} U^\dagger P_{2k-1} U^\dagger P_{2k-2} U^\dagger \dots P_{k+1} U^\dagger P_k U \dots U P_2 U P_1 U | \psi \rangle, \quad (\text{G.1})$$

where we assume that P_i are Pauli operators for simplicity. Any time-ordered correlation function can be measured in an experiment that applies the unitary U k times in sequence. An out-of-time-order $2k$ -point correlation function takes the form,

$$C_{\text{OTO}}(P_1, \dots, P_{2k}) = \langle \psi | P_{2k} U^\dagger P_{2k-1} U P_{2k-2} U^\dagger P_{2k-3} U \dots P_4 U^\dagger P_3 U P_2 U^\dagger P_1 U | \psi \rangle, \quad (\text{G.2})$$

where we again assume that P_i are Pauli operators for simplicity. Any out-of-time-order correlation function can be measured in an experiment that applies U and $U^\dagger$ one after the other $k/2$ times in sequence. Here, we assume k is even. The particular out-of-time-order correlation function shown in Fig. 4 of the main text sets all P_i for even i equal to one another and all P_i for odd i equal as well.

As discussed in the main text, the formation of strong unitary k -designs immediately implies the decay of all local k -point time-ordered and out-of-time-order correlation functions to zero.

Proposition 10. *For any $k = \mathcal{O}(1)$ and $\varepsilon = \Omega(1/2^n)$. Let U be drawn from a strong $\frac{\varepsilon^2 \delta}{\text{poly } n}$ -approximate unitary $2k$ -design and $|\psi\rangle$ be any quantum state. Then with high probability $1 - \delta$, every local $2k$ -point time-ordered and out-of-time-order correlation function decays to within ε of zero under U .*

For example, if we one sets ε and δ to be super-polynomially small in n , i.e. $1/\varepsilon, 1/\delta = \omega(\text{poly } n)$, then the proposition is satisfied whenever the error of the strong unitary, $\varepsilon' = \varepsilon^2 \delta / \text{poly } n$, is also super-polynomially small in n . From Theorem 1, this is achieved in $\mathcal{O}(\log n)$ circuit depth for structured quantum circuits and $\mathcal{O}(\log^3 n)$ circuit for all-to-all connected random circuits.

Proof. We consider the sum of squares of all local time-ordered and out-of-time-order correlation functions,

$$C(U) = \sum_{P_1, \dots, P_{2k}} C_{\text{TO}}(P_1, \dots, P_{2k})^2 + C_{\text{OTO}}(P_1, \dots, P_{2k})^2, \quad (\text{G.3})$$

where each P_i in the sum is non-identity. If each P_i is r -local with $r = \mathcal{O}(1)$, then there are at most $2(3n)^{2rk} = n^{\mathcal{O}(k)}$ correlation functions in the sum. This follows because each Pauli operator can take $3^r \binom{n}{r} \leq (3n)^r$ different values and there are $2k$ Pauli operators to choose. Here, we add in the label U on the left side for specificity; the time-ordered and out-of-time-order correlation functions all implicitly depend on U as well.

The expected value, $\mathbb{E}_{U \sim \mathcal{H}} C(U)$, can be estimated to within $n^{\mathcal{O}(k)} \varepsilon'$ of its Haar-random value, since each individual term can be estimated to within $\mathcal{O}(\varepsilon')$. A straightforward calculation shows that each Haar-random correlation function is exponentially small (see e.g. [105]), and hence $\mathbb{E}_{U \sim \mathcal{H}} C(U) = \mathcal{O}(n^{\mathcal{O}(k)} / 2^n)$. Thus, $\mathbb{E}_{U \sim \mathcal{H}} C(U) = \mathcal{O}(n^{\mathcal{O}(k)} (\varepsilon' + 1/2^n)) = \mathcal{O}(n^{\mathcal{O}(k)} \varepsilon')$. From Markov's inequality, we have

$$\Pr(C(U) \geq \varepsilon^2) \leq \frac{n^{\mathcal{O}(k)} \varepsilon'}{\varepsilon^2}. \quad (\text{G.4})$$

The probability δ that any individual correlation function has absolute value greater than ε is upper bounded by the probability above. Setting $\varepsilon' = \varepsilon^2 \delta / n^{\mathcal{O}(k)}$ completes the proof. $\square$

G.2 Operator size distributions

The size distribution of an operator O evolved under a unitary U is given by

$$P_U(w) = \frac{1}{2^n} \text{tr}(O(t) \mathcal{P}_w [O(t)]), \quad (\text{G.5})$$

where $\mathcal{P}_w$ is a superoperator that projects onto Pauli strings of weight w . We assume without loss of generality that $\frac{1}{2^n} \text{tr}(O^\dagger O) = 1$, which implies that the size distribution is normalized, $\sum_w P_U(w) = 1$. If we consider the quantum state $(O \otimes \mathbb{1}) |\Psi_{\text{EPR}}\rangle$ on two copies of n qubits, then the size distribution corresponds to the expectation value,

$$P_U(w) = \langle \Psi_{\text{EPR}} | (O^\dagger \otimes \mathbb{1}) (U^\dagger \otimes U^T) \mathcal{P}_w (U \otimes U^*) (O \otimes \mathbb{1}) | \Psi_{\text{EPR}} \rangle, \quad (\text{G.6})$$

where $\mathcal{P}_w$ is now an operator on the two-copy system that projects onto the span of states $(Q \otimes \mathbb{1}) |\Psi_{\text{EPR}}\rangle$ where Q is any Pauli operator with weight w .

We can use strong approximate unitary 4-designs to bound the closeness of operator size distributions to their Haar-random values.

Proposition 11. *The expected total variation distance between the operator size distribution of a strong ε -approximate unitary 4-design and the Haar-random operator size distribution is less than $3n^2 \varepsilon$.*

From Theorem 1, strong ε -approximate unitary 4-designs with $\varepsilon = 1/\text{poly } n$ can form in circuit depth $\mathcal{O}(\log n)$ in structured unitary ensembles and circuit depth $\mathcal{O}(\log^2 n)$ in random circuits. This confirms empirical observations that operator size distributions can equilibrate to their Haar-random values in logarithmic depth $\square$.

Proof. We use the Cauchy-Schwarz inequality and the fact that the operator size distribution is the expectation value of a bounded operator $\mathcal{P}_w$ on two copies. The latter allows us to bound $|\mathbb{E}_U P_U(w) - P_H(w)| \leq \varepsilon$ and $|\mathbb{E}_U P_U(w)^2 - P_H(w)^2| \leq \varepsilon$. This yields,

$$\begin{aligned}
\mathbb{E}_{U \sim \mathcal{E}} \text{TVD}(P_U, P_H) &\equiv \mathbb{E}_{U \sim \mathcal{E}} \sum_{w=1}^n |P_U(w) - P_H(w)| \\
&\leq \mathbb{E}_{U \sim \mathcal{E}} n \sum_{w=1}^n |P_U(w) - P_H(w)|^2 \\
&= \mathbb{E}_{U \sim \mathcal{E}} n \sum_{w=1}^n (P_U(w)^2 - 2P_U(w)P_H(w) + P_H(w)^2) \\
&= n \sum_{w=1}^n (\varepsilon + 2\varepsilon) \\
&= 3n^2\varepsilon.
\end{aligned} \tag{G.7}$$

This completes the proof. $\square$

G.3 Entanglement and operator entanglement entropy.

Consider a state $|\psi(t)\rangle \equiv U|\psi\rangle$ and an operator $O(t) \equiv UOU^\dagger$. Let A denote a subsystem of n qubits and B its complement. To define the entanglement entropy and operator entanglement entropy of $|\psi(t)\rangle$ and $O(t)$, respectively, we can first write the Schmidt decomposition of each object between A and B ,

$$|\psi(t)\rangle = \sum_i \sqrt{\lambda_i^\psi} \cdot |\psi_A^i\rangle \otimes |\psi_B^i\rangle, \tag{G.8}$$

where $\langle \psi_A^i | \psi_A^j \rangle = \langle \psi_B^i | \psi_B^j \rangle = \delta_{ij}$, and

$$O(t) = \sum_i \sqrt{\lambda_i^O} \cdot O_A^i \otimes O_B^i, \tag{G.9}$$

where $\frac{1}{2^n} \text{tr}((O_A^i)^\dagger O_A^j) = \frac{1}{2^n} \text{tr}((O_B^i)^\dagger O_B^j) = \delta_{ij}$. We have $\sum_i \lambda_i^\psi = \langle \psi | \psi \rangle = 1$ and $\sum_i \lambda_i^O = \frac{1}{2^n} \text{tr}(O^\dagger O) = 1$ (assuming we normalize O to one). The von Neumann entanglement entropy of $|\psi(t)\rangle$ is equal to $\sum_i \lambda_i^\psi \ln \lambda_i^\psi$ and the von Neumann operator entanglement entropy of $O(t)$ is equal to $\sum_i \lambda_i^O \ln \lambda_i^O$.

The von Neumann entanglement entropy is difficult to analyze using unitary k -designs due to the logarithmic factor. To this end, we consider a Renyi version of the entanglement and operator entanglement entropies. The Renyi-2 entanglement entropy of $|\psi(t)\rangle$ between A and B is given by

$$S_A^{(2)}(|\psi(t)\rangle) = -\ln \left(\sum_i (\lambda_i^\psi)^2 \right) = -\ln \left(\text{tr}_A(\text{tr}_B(|\psi(t)\rangle\langle\psi(t)|)^2) \right), \tag{G.10}$$

while the Renyi-2 operator entanglement entropy of $O(t)$ is given by

$$S_A^{(2)}(O(t)) = -\ln \left(\sum_i (\lambda_i^O)^2 \right). \tag{G.11}$$

The entanglement and operator entanglement entropies are difficult to tightly bound using standard unitary designs. Fundamentally, this is because each quantity requires an exponential overhead to

experimentally measure. Here, we show that strong unitary designs with small *relative error* can nonetheless be used to tightly bound both quantities near their Haar-random values.

We prove that the entanglement entropy and for any initial state $|\psi\rangle$ and the operator entanglement entropy for any initial operator O saturate to their Haar-random values U is drawn from a strong unitary design with relative error.

Proposition 12. *Consider the state $|\psi(t)\rangle \equiv U|\psi\rangle$ formed by applying a strong unitary 2-design with relative error ε to any state $|\psi\rangle$. The Renyi-2 entanglement entropy of any subsystem of $|\psi(t)\rangle$ is equal to its Haar value to within error ε .*

Proposition 13. *Consider the operator $O(t) \equiv UOU^\dagger$ formed by applying a strong unitary 4-design with relative error ε to any operator O . The Renyi-2 operator entanglement entropy of any subsystem of $O(t)$ is equal to its Haar value to within error ε .*

We recall from Theorem 1 that strong unitary 4-designs with relative error ε can be formed in circuit depth $\mathcal{O}(\log n + \log \log 1/\varepsilon)$ in structured circuits. Hence, the entanglement and operator entanglement entropies saturate to within $\varepsilon = 1/\exp n$ of their Haar-random values at $\mathcal{O}(\log n)$ depth.

Proof of Proposition 12. The proposition follows by reformulating the purity as the expectation value of a positive operator on a larger system involving U and U^* . Let us abbreviate $\rho \equiv |\psi(t)\rangle\langle\psi(t)|$. We have

$$\mathrm{tr}_A(\mathrm{tr}_B(\rho)^2) = 2^{|A|} \mathrm{tr}(|\Psi_{\mathrm{EPR}}^A\rangle\langle\Psi_{\mathrm{EPR}}^A| \cdot (\rho \otimes \rho^*)), \quad (\text{G.12})$$

where $|A|$ denotes the number of qubits in subsystem A , and $|\Psi_{\mathrm{EPR}}^A\rangle$ denotes the EPR state between two copies of subsystem A . Note that this formula differs from the standard reformulation of the purity in terms of a swap operator, $\mathrm{tr}_A(\mathrm{tr}_B(\rho)^2) = \mathrm{tr}(\mathcal{S}_A \cdot (\rho \otimes \rho))$. The expression in terms of the EPR state can be obtained from the expression in terms of the swap operator by taking a partial transpose on the second copy of both terms inside the trace.

The state $\rho \otimes \rho^* = (U \otimes U^*)(|\psi\rangle\langle\psi| \otimes |\psi^*\rangle\langle\psi^*|)(U^\dagger \otimes U^T)$ is obtained by evolving the state $|\psi\rangle \otimes |\psi^*\rangle$ under one application of U and one application of U^* . Since $|\Psi_{\mathrm{EPR}}^A\rangle\langle\Psi_{\mathrm{EPR}}^A|$ is positive, the expectation value above is captured within multiplicative error ε by any strong unitary 2-design with relative error ε . $\square$

Proof of Proposition 13. The proposition follows immediately from Proposition 12 by noting that the purity of the operator $O(t)$ is equal to the purity of the state $(O(t) \otimes \mathbb{1})|\Psi_{\mathrm{EPR}}\rangle$ formed by applying $O(t)$ to one side of the EPR state on a two-copy system. The latter state can be written as

$$(O(t) \otimes \mathbb{1})|\Psi_{\mathrm{EPR}}\rangle = (U \otimes U^*)(O \otimes \mathbb{1})|\Psi_{\mathrm{EPR}}\rangle. \quad (\text{G.13})$$

To estimate the purity, from Proposition 12, we use one copy of the state above and one copy of its conjugate. This requires 2 applications of U and 2 applications of U^* . Hence, the expectation value of the purity is captured to within multiplicative error ε by any strong unitary 4-design with relative error ε . $\square$

References

- [1] Joseph Emerson, Robert Alicki, and Karol Życzkowski. Scalable noise estimation with random unitary operators. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(10):S347, 2005.
- [2] Andris Ambainis and Joseph Emerson. Quantum t-designs: t-wise independence in the quantum world. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 129–140. IEEE, 2007.
- [3] Emanuel Knill, Dietrich Leibfried, Rolf Reichle, Joe Britton, R Brad Blakestad, John D Jost, Chris Langer, Roee Ozeri, Signe Seidelin, and David J Wineland. Randomized benchmarking of quantum gates. *Physical Review A*, 77(1):012307, 2008.
- [4] Andreas Elben, Steven T Flammia, Hsin-Yuan Huang, Richard Kueng, John Preskill, Benoît Vermersch, and Peter Zoller. The randomized measurement toolbox. *Nature Reviews Physics*, 5(1):9–24, 2023.
- [5] M Guță, Jonas Kahn, Richard Kueng, and Joel A Tropp. Fast state tomography with optimal error bounds. *Journal of Physics A: Mathematical and Theoretical*, 53(20):204001, 2020.
- [6] Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16(10):1050–1057, 2020.
- [7] Andrew Zhao, Nicholas C Rubin, and Akimasa Miyake. Fermionic partial tomography via classical shadows. *Physical Review Letters*, 127(11):110504, 2021.
- [8] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.
- [9] Alexis Morvan, B Villalonga, X Mi, S Mandra, A Bengtsson, PV Klimov, Z Chen, S Hong, C Erickson, IK Drozdov, et al. Phase transition in random circuit sampling. *arXiv preprint arXiv:2304.11119*, 2023.
- [10] Dmitry A Abanin, Rajeev Acharya, Laleh Aghababaie-Beni, Georg Aigeldinger, Ashok Ajoy, Ross Alcaraz, Igor Aleiner, Trond I Andersen, Markus Ansmann, Frank Arute, et al. Constructive interference at the edge of quantum ergodic dynamics. *arXiv preprint arXiv:2506.10191*, 2025.
- [11] Zhengfeng Ji, Yi-Kai Liu, and Fang 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, pages 126–152. Springer, 2018.
- [12] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In *Annual International Cryptology Conference*, pages 208–236. Springer, 2022.
- [13] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1589–1602, 2023.
- [14] Matthew PA Fisher, Vedika Khemani, Adam Nahum, and Sagar Vijay. Random quantum circuits. *Annual Review of Condensed Matter Physics*, 14:335–379, 2023.

- [15] Adam Nahum, Jonathan Ruhman, Sagar Vijay, and Jeongwan Haah. Quantum Entanglement Growth Under Random Unitary Dynamics. *Phys. Rev. X*, 7:031016, 2017.
- [16] Jordan Cotler, Nicholas Hunter-Jones, and Daniel Ranard. Fluctuations of subsystem entropies at late times. *Physical Review A*, 105(2):022416, 2022.
- [17] J. M. Deutsch. Quantum statistical mechanics in a closed system. *Phys. Rev. A*, 43:2046, 1991.
- [18] Mark Srednicki. Chaos and quantum thermalization. *Phys. Rev. E*, 50:888, 1994.
- [19] Marcos Rigol, Vanja Dunjko, and Maxim Olshanii. Thermalization and its mechanism for generic isolated quantum systems. *Nature*, 452(7189):854–858, 2008.
- [20] Yasuhiro Sekino and Leonard Susskind. Fast scramblers. *Journal of High Energy Physics*, 2008(10):065, 2008.
- [21] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *JHEP*, 2007(09):120, 2007.
- [22] Adam R Brown, Hrant Gharibyan, Stefan Leichenauer, Henry W Lin, Sepehr Nezami, Grant Salton, Leonard Susskind, Brian Swingle, and Michael Walter. Quantum gravity in the lab. i. teleportation by size and traversable wormholes. *PRX quantum*, 4(1):010320, 2023.
- [23] Sepehr Nezami, Henry W Lin, Adam R Brown, Hrant Gharibyan, Stefan Leichenauer, Grant Salton, Leonard Susskind, Brian Swingle, and Michael Walter. Quantum gravity in the lab. ii. teleportation by size and traversable wormholes. *PRX quantum*, 4(1):010321, 2023.
- [24] Thomas Schuster, Bryce Kobrin, Ping Gao, Iris Cong, Emil T Khabiboulline, Norbert M Linke, Mikhail D Lukin, Christopher Monroe, Beni Yoshida, and Norman Y Yao. Many-body quantum teleportation via operator spreading in the traversable wormhole protocol. *Physical Review X*, 12(3):031013, 2022.
- [25] Shenglong Xu and Brian Swingle. Scrambling dynamics and out-of-time-ordered correlators in quantum many-body systems. *PRX quantum*, 5(1):010201, 2024.
- [26] Daniel A Roberts, Douglas Stanford, and Alexandre Streicher. Operator growth in the syk model. *Journal of High Energy Physics*, 2018(6):1–20, 2018.
- [27] Joseph Emerson, Yaakov S Weinstein, Marcos Saraceno, Seth Lloyd, and David G Cory. Pseudo-random unitary operators for quantum information processing. *science*, 302(5653):2098–2100, 2003.
- [28] Joseph Emerson. Random quantum circuits and pseudo-random operators: theory and applications. *arXiv preprint quant-ph/0410087*, 2004.
- [29] David Gross, Koenraad Audenaert, and Jens Eisert. Evenly distributed unitaries: On the structure of unitary designs. *Journal of mathematical physics*, 48(5), 2007.
- [30] Christoph Dankert. Efficient simulation of random quantum states and operators. *arXiv preprint quant-ph/0512217*, 2005.
- [31] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80(1):012304, 2009.

- [32] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346:397–434, 2016.
- [33] Jeongwan Haah, Yunchao Liu, and Xinyu Tan. Efficient approximate unitary designs from random pauli rotations. *arXiv preprint arXiv:2402.05239*, 2024.
- [34] Chi-Fang Chen, Jeongwan Haah, Jonas Haferkamp, Yunchao Liu, Tony Metger, and Xinyu Tan. Incompressibility and spectral gaps of random circuits. *arXiv preprint arXiv:2406.07478*, 2024.
- [35] Nicholas LaRacuente and Felix Leditzky. Approximate unitary k -designs from shallow, low-communication circuits. *arXiv preprint arXiv:2407.07876*, 2024.
- [36] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth. *Science*, 389(6755):92–96, 2025.
- [37] Maxwell West, Diego García-Martín, NL Diaz, M Cerezo, and Martin Larocca. No-go theorems for sublinear-depth group designs. *arXiv preprint arXiv:2506.16005*, 2025.
- [38] Lorenzo Grevink, Jonas Haferkamp, Markus Heinrich, Jonas Helsen, Marcel Hinsche, Thomas Schuster, and Zoltán Zimborás. Will it glue? on short-depth designs beyond the unitary group. *arXiv preprint arXiv:2506.23925*, 2025.
- [39] Laura Cui, Thomas Schuster, Fernando Brandao, and Hsin-Yuan Huang. Unitary designs in nearly optimal depth. *arXiv preprint arXiv:2507.06216*, 2025.
- [40] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t -designs and pseudorandom unitaries. *arXiv preprint arXiv:2404.12647*, 2024.
- [41] Chi-Fang Chen, Adam Bouland, Fernando GSL Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. Efficient unitary designs and pseudorandom unitaries from permutations. *arXiv preprint arXiv:2404.16751*, 2024.
- [42] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. *arXiv preprint arXiv:2410.10116*, 2024.
- [43] Ben Foxman, Natalie Parham, Francisca Vasconcelos, and Henry Yuen. Random unitaries in constant (quantum) time. *arXiv preprint arXiv:2508.11487*, 2025.
- [44] Jordan Cotler, Thomas Schuster, and Masoud Mohseni. Information-theoretic hardness of out-of-time-order correlators. *Physical Review A*, 108(6):062608, 2023.
- [45] Beni Yoshida and Alexei Kitaev. Efficient decoding for the hayden-preskill protocol. *arXiv preprint arXiv:1710.03363*, 2017.
- [46] Mark Zhandry. How to model unitary oracles. Cryptology ePrint Archive, Paper 2025/1072, 2025.
- [47] Thomas Schuster, Chao Yin, Xun Gao, and Norman Y Yao. A polynomial-time classical algorithm for noisy quantum circuits. *arXiv preprint arXiv:2407.12768*, 2024.
- [48] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

- [49] Lana Sheridan, Dmitri Maslov, and Michele Mosca. Approximating fractional time quantum evolution. *Journal of Physics A: Mathematical and Theoretical*, 42(18):185302, 2009.
- [50] Ewin Tang and John Wright. Are controlled unitaries helpful? *arXiv:2508.00055*, 2025.
- [51] Stephen H Shenker and Douglas Stanford. Black holes and the butterfly effect. *Journal of High Energy Physics*, 2014(3):67, 2014.
- [52] Daniel A Roberts, Douglas Stanford, and Leonard Susskind. Localized shocks. *Journal of High Energy Physics*, 2015(3):1–27, 2015.
- [53] Pavan Hosur, Xiao-Liang Qi, Daniel A Roberts, and Beni Yoshida. Chaos in quantum channels. *Journal of High Energy Physics*, 2016(2):1–49, 2016.
- [54] Brian Swingle, Gregory Bentsen, Monika Schleier-Smith, and Patrick Hayden. Measuring the scrambling of quantum information. *Physical Review A*, 94(4):040302, 2016.
- [55] Adam Nahum, Sagar Vijay, and Jeongwan Haah. Operator spreading in random unitary circuits. *Physical Review X*, 8(2):021014, 2018.
- [56] Thomas Schuster and Norman Y Yao. Operator growth in open quantum systems. *Physical Review Letters*, 131(16):160402, 2023.
- [57] Martin Gärttner, Justin G Bohnet, Arghavan Safavi-Naini, Michael L Wall, John J Bollinger, and Ana Maria Rey. Measuring out-of-time-order correlations and multiple quantum spectra in a trapped-ion quantum magnet. *Nature Physics*, 13(8):781–786, 2017.
- [58] Kevin A Landsman, Caroline Figgatt, Thomas Schuster, Norbert M Linke, Beni Yoshida, Norm Y Yao, and Christopher Monroe. Verified quantum information scrambling. *Nature*, 567(7746):61–65, 2019.
- [59] MS Blok, VV Ramasesh, T Schuster, K O’Brien, JM Kreikebaum, D Dahlen, A Morvan, Beni Yoshida, NY Yao, and I Siddiqi. Quantum information scrambling in a superconducting qutrit processor. *arXiv:2003.03307*, 2020.
- [60] Claudia M Sánchez, Ana Karina Chattah, and Horacio M Pastawski. Emergent decoherence induced by quantum chaos in a many-body system: A Loschmidt echo observation through NMR. *arXiv:2112.00607*, 2021.
- [61] Xiao Mi, Pedram Roushan, Chris Quintana, Salvatore Mandrà, Jeffrey Marshall, Charles Neill, Frank Arute, Kunal Arya, Juan Atalaya, Ryan Babbush, et al. Information scrambling in quantum circuits. *Science*, 374(6574):1479–1483, 2021.
- [62] Juan Maldacena and Douglas Stanford. Remarks on the Sachdev-Ye-Kitaev model. *Physical Review D*, 94(10):106002, 2016.
- [63] Alexei Kitaev. A simple model of quantum holography, 2015.
- [64] Winton Brown and Omar Fawzi. Scrambling speed of random quantum circuits. *arXiv preprint arXiv:1210.6644*, 2012.
- [65] Winton Brown and Omar Fawzi. Short random circuits define good quantum error correcting codes. In *2013 IEEE International Symposium on Information Theory*, pages 346–350. IEEE, 2013.

- [66] Winton Brown and Omar Fawzi. Decoupling with random quantum circuits. *Communications in mathematical physics*, 340(3):867–900, 2015.
- [67] Nima Lashkari, Douglas Stanford, Matthew Hastings, Tobias Osborne, and Patrick Hayden. Towards the fast scrambling conjecture. *Journal of High Energy Physics*, 2013(4):1–33, 2013.
- [68] Richard Cleve, Debbie Leung, Li Liu, and Chunhao Wang. Near-linear constructions of exact unitary 2-designs. *arXiv preprint arXiv:1501.04592*, 2015.
- [69] Ron Belyansky, Przemyslaw Bienias, Yaroslav A Kharkov, Alexey V Gorshkov, and Brian Swingle. Minimal model for fast scrambling. *Physical review letters*, 125(13):130601, 2020.
- [70] Gregory Bentsen, Yingfei Gu, and Andrew Lucas. Fast scrambling on sparse graphs. *Proceedings of the National Academy of Sciences*, 116(14):6689–6694, 2019.
- [71] Amit Vikram and Victor Galitski. Exact universal bounds on quantum dynamics and fast scrambling. *Physical Review Letters*, 132(4):040402, 2024.
- [72] Jonas Haferkamp. Random quantum circuits are approximate unitary t -designs in depth $O(t^{5+o(1)})$. *Quantum*, 6:795, September 2022.
- [73] Mark Zhandry. A note on quantum-secure prps. *arXiv preprint arXiv:1611.05564*, 2016.
- [74] Mark Zhandry. How to construct quantum random functions. *J. ACM*, 68(5), aug 2021.
- [75] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.
- [76] Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22(3):265–279, 1981.
- [77] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.
- [78] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 719–737. Springer, 2012.
- [79] Harry Buhrman, Marten Folkertsma, Ian Mertz, Florian Speelman, Sergii Strelchuk, Sathyawageeswar Subramanian, and Quinten Tupker. Quantum catalytic space. *arXiv preprint arXiv:2506.16324*, 2025.
- [80] Bill Fefferman, Soumik Ghosh, and Wei Zhan. Anti-concentration for the unitary haar measure and applications to random quantum circuits. *arXiv preprint arXiv:2407.19561*, 2024.
- [81] Silvia Pappalardi, Laura Foini, and Jorge Kurchan. Eigenstate thermalization hypothesis and free probability. *Physical Review Letters*, 129(17):170603, 2022.
- [82] Michele Fava, Jorge Kurchan, and Silvia Pappalardi. Designs via free probability. *Physical Review X*, 15(1):011031, 2025.
- [83] Neil Dowling, Jacopo De Nardis, Markus Heinrich, Xhek Turkeshi, and Silvia Pappalardi. Free independence and unitary design from random matrix product unitaries. *arXiv preprint arXiv:2508.00051*, 2025.

- [84] Shreya Vardhan and Jinzhao Wang. Free mutual information and higher-point otocs. *arXiv preprint arXiv:2509.13406*, 2025.
- [85] Stephen W Hawking. Breakdown of predictability in gravitational collapse. *Physical Review D*, 14(10):2460, 1976.
- [86] Bryce Kobrin, Thomas Schuster, Maxwell Block, Weijie Wu, Bradley Mitchell, Emily Davis, and Norman Y Yao. A universal protocol for quantum-enhanced sensing via information scrambling. *arXiv preprint arXiv:2411.12794*, 2024.
- [87] Dmitry Grinko and Maris Ozols. Linear programming with unitary-equivariant constraints. *Communications in Mathematical Physics*, 405(12):278, 2024.
- [88] Dmitry Grinko, Adam Burchardt, and Maris Ozols. Gelfand-tsetlin basis for partially transposed permutations, with applications to quantum information. *arXiv preprint arXiv:2310.02252*, 2023.
- [89] Quynh T Nguyen. The mixed schur transform: efficient quantum circuit and applications. *arXiv preprint arXiv:2310.01613*, 2023.
- [90] William Fulton and Joe Harris. *Representation theory: a first course*, volume 129. Springer Science & Business Media, 2013.
- [91] Roe Goodman, Nolan R Wallach, et al. *Symmetry, representations, and invariants*, volume 255. Springer, 2009.
- [92] Antonio Anna Mele. Introduction to haar measure tools in quantum information: A beginner’s tutorial. *Quantum*, 8:1340, 2024.
- [93] Thomas Schuster, Murphy Niu, Jordan Cotler, Thomas O’Brien, Jarrod R McClean, and Masoud Mohseni. Learning quantum systems via out-of-time-order correlators. *Physical Review Research*, 5(4):043284, 2023.
- [94] Jordan S Cotler, Daniel K Mark, Hsin-Yuan Huang, Felipe Hernandez, Joonhee Choi, Adam L Shaw, Manuel Endres, and Soonwon Choi. Emergent quantum state designs from individual many-body wave functions. *PRX quantum*, 4(1):010311, 2023.
- [95] Aram W. Harrow. The church of the symmetric subspace. *arXiv:1308.6595*, 2013.
- [96] Aram W Harrow and Saeed Mehraban. Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates. *Communications in Mathematical Physics*, pages 1–96, 2023.
- [97] Nicholas Hunter-Jones. Unitary designs from statistical mechanics in random quantum circuits. *arXiv preprint arXiv:1905.12053*, 2019.
- [98] Jonas Haferkamp and Nicholas Hunter-Jones. Improved spectral gaps for random quantum circuits: Large local dimensions and all-to-all interactions. *Physical Review A*, 104(2):022417, 2021.
- [99] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 806–809, 2025.
- [100] Zak Webb. The clifford group forms a unitary 3-design. *arXiv preprint arXiv:1510.02769*, 2015.

- [101] Harry Buhrman, Richard Cleve, Michal Koucký, Bruno Loff, and Florian Speelman. Computing with a full memory: catalytic space. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 857–866, 2014.
- [102] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A—Atomic, Molecular, and Optical Physics*, 80(1):012304, 2009.
- [103] Dorit Aharonov, Jordan Cotler, and Xiao-Liang Qi. Quantum algorithmic measurement. *Nature communications*, 13(1):1–9, 2022.
- [104] Benoît Collins and Sho Matsumoto. Weingarten calculus via orthogonality relations: new applications. *arXiv:1701.04493*, 2017.
- [105] Jordan Cotler, Nicholas Hunter-Jones, Junyu Liu, and Beni Yoshida. Chaos, complexity, and random matrices. *Journal of High Energy Physics*, 2017(11):1–60, 2017.