Random unitaries from Hamiltonian dynamics

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

[1] *California Institute of Technology, Pasadena, California 91125, USA*
[2] *Google Quantum AI, Venice, California 90291, USA*
[3] *Institute for Advanced Study, Tsinghua University, Beijing, 100084, China*
[4] *AWS Center for Quantum Computing, Pasadena, California 91125, USA*

(Dated: October 9, 2025)

The nature of randomness and complexity growth in systems governed by unitary dynamics is a fundamental question in quantum many-body physics. This problem has motivated the study of models such as local random circuits and their convergence to Haar-random unitaries in the long-time limit. However, these models do not correspond to any family of physical time-independent Hamiltonians. In this work, we address this gap by studying the indistinguishability of time-independent Hamiltonian dynamics from truly random unitaries. On one hand, we establish a no-go result showing that for any ensemble of constant-local Hamiltonians and any evolution times, the resulting time-evolution unitary can be efficiently distinguished from Haar-random and fails to form a 2-design or a pseudorandom unitary (PRU). On the other hand, we prove that this limitation can be overcome by increasing the locality slightly: there exist ensembles of random polylog-local Hamiltonians in one-dimension such that under constant evolution time, the resulting time-evolution unitary is indistinguishable from Haar-random, i.e. it forms both a unitary k-design and a PRU. Moreover, these Hamiltonians can be efficiently simulated under standard cryptographic assumptions.

I. INTRODUCTION

Characterizing the emergence of universal chaotic and ergodic behaviors is a central goal of quantum many-body physics. Seminal early works, for example, on spectral distributions and single-particle quantum chaos [1–3], and the eigenstate thermalization hypothesis [4, 5], have shown that small amounts of uncertainty in the parameters of a chaotic Hamiltonian can lead to universal fluctuations in its properties and observables. In the last decade, tremendous further progress has been made in *time-dependent* quantum systems, such as random quantum circuits, by capturing the emergence of universal chaotic behaviors using the notions of *unitary k-designs* [6–23] and *pseudorandom unitaries* (PRUs) [16, 20, 24–29]. These objects capture how quickly the properties of a physical system can become indistinguishable from those of a completely Haar-random unitary. Due to their elegance and broad range of physical predictions, unitary designs and PRUs have been widely applied in quantum benchmarking [30–35], demonstrations of quantum advantage [36–38], and even fundamental questions in quantum gravity [39–44]. More generally, they have also been employed to understand properties of physical dynamics through the lens of learnability [16, 45–47], information encoding and scrambling [20, 48–55], sampling complexity [17, 56, 57], computational power [13, 58, 59], and the onset of quantum chaos [60–64].

Despite this success, random quantum circuits are imperfect models of physical systems in important ways. Most prominently, they are time-dependent, and hence do not conserve energy, as any physical Hamiltonian time-evolution would. Useful attempts to bridge this gap have focused on *charge*-conserving random circuits [65–71]; however, such systems still miss many key features of physical Hamiltonian evolution. For example, the conserved charge is usually especially simple and fixed; the conserved charge also does not govern the time-evolution of the system, as a physical Hamiltonian would. Hence, it remains an open question to what extent unitary designs and PRUs can in fact capture the chaotic behaviors of physical time-independent Hamiltonian dynamics. This question is fundamentally important, as most applications of random unitaries in many-body and high-energy physics are primally concerned with time-independent Hamiltonian systems.

In this work, we establish several central results on the formation of unitary designs and PRUs in time-independent Hamiltonian dynamics. Our first result is a broad no-go theorem. We provide a simple and efficient test to distinguish any ensemble of time-evolutions under any constant-local Hamiltonians for any lengths of time from a Haar-random unitary, using only two queries to the time-evolution and minimal classical computation. This proves that time-evolution under constant-local Hamiltonians can never form PRUs, or unitary 2-designs with polynomially small error. Motivated by this fact, our second result considers the behavior of Hamiltonians with a slightly higher locality. In sharp contrast to our results on constant-local Hamiltonians, we prove that ensembles of time-evolution under random Hamiltonians of locality $\omega(\log n)$ can readily form both unitary k-designs and PRUs. This holds even for constant evolution times, $t = \mathcal{O}(1)$. We also prove several additional results on non-adaptive PRUs, which broaden the range of Hamiltonian ensembles to which our results apply.

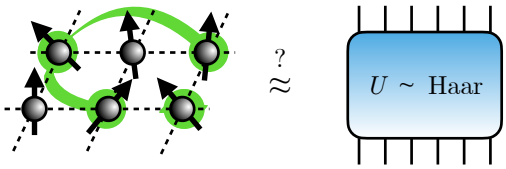

Figure 1: Our work investigates when time-independent Hamiltonian dynamics are asymptotically indistinguishable from random unitary transformations. We find that pseudorandomness cannot arise in any family of Hamiltonians with constant-local interactions, but can be achieved in quasi-local models.

Our results establish a need for nuance when applying random unitary descriptions to physical Hamiltonian dynamics. In the long-term, this emphasizes the need for new and more precise formulations of universal chaotic behaviors that can capture the physics of local Hamiltonian systems. Recent works suggest several promising approaches in this direction [72–75]. Our results on the formation of unitary designs and PRUs also complement other recent discoveries on the robust emergence of ergodic phenomena in Hamiltonians with a slightly increased locality [76]. From an applications perspective, our findings immediately imply fundamental limits on learning properties from time-independent Hamiltonian dynamics. For example, the complexity of learning the parameters of an unknown Hamiltonian [77–82] must grow exponentially in the Hamiltonian locality, even in situations where the Hamiltonian itself possesses an efficient description.

Relation to previous work

Despite considerate interest in the use of random unitaries as models of physical systems [1–5, 39–44, 60–75], there are relatively few existing results on the realization of unitary designs and PRUs from time-independent Hamiltonian evolution. This stems from the notorious difficulty of rigorously analyzing the dynamical properties of many-body quantum Hamiltonians. Several works have considered time-*dependent* Hamiltonians [11, 14]. However, such models do not conserve energy, and share more features in common with random quantum circuits than with time-independent Hamiltonian systems. More relevantly, recent work has shown that time-evolution under a random time-*independent* Hamiltonian, drawn from either the GUE ensemble on n qubits or a pseudorandom variant of it, can become indistinguishable from a Haar-random unitary after a super-polynomially long evolution time, $t = \omega(\mathrm{poly}\, n)$ [64]. Our work substantially expands upon this result, by showing that time-evolution under nearly-local Hamiltonians, of locality $\omega(\log n)$ instead of $\mathcal{O}(n)$, can become indistinguishable from a Haar-random unitary after only very short evolution times, $t = \mathcal{O}(1)$ instead of $t = \omega(\mathrm{poly}\, n)$. Our no-go theorems also highlight the precise limits of this indistinguishability for Hamiltonians of any smaller locality.

II. PRELIMINARIES

Before turning to our results, we provide a short review of the definitions of unitary k-designs and pseudorandom unitaries (PRUs). As aforementioned, both notions seek to capture the closeness of a random unitary ensemble $\mathcal{E}$ to the Haar ensemble, under various metrics of approximation. A Haar-random unitary on n qubits is a random unitary matrix drawn from from the Haar measure on $U(2^n)$.

An approximate unitary k-design is a unitary ensemble $\mathcal{E}$ that reproduces the k-th moment of the Haar ensemble up to a small error. In particular, an ensemble $\mathcal{E}$ is an approximate unitary k-design up to *additive error* ε if its k-th moment, $\Phi_{\mathcal{E}}(\cdot) \equiv U^{\otimes k}(\cdot)U^{\dagger,\otimes k}$, is close to the k-th moment $\Phi_H(\cdot)$ of the Haar ensemble in the diamond norm, $\|\Phi_{\mathcal{E}} - \Phi_H\|_\diamond \equiv \max_\rho \|\Phi_{\mathcal{E}}(\rho) - \Phi_H\|_1 \leq \varepsilon$ [10]. This bounds the distinguishability of a random unitary drawn from $\mathcal{E}$ from a random unitary drawn from the Haar ensemble, by any quantum experiment that queries the random unitary k times in parallel [19]. A more recent and much stronger notion of approximation error for unitary designs is the measurable error [19]. An ensemble $\mathcal{E}$ is an approximate unitary k-design up to *measurable error* ε if the expected output state of any quantum experiment that queries a random unitary drawn from $\mathcal{E}$ is close to the expected output state for the same experiment querying a Haar-random unitary up to small trace-norm error. This bounds the distinguishability in any quantum experiment that queries the random unitary k times and performs arbitrary quantum operations and measurements in between [19]. Unless otherwise specified,

we will utilize this strong form of measurable approximation error throughout our work.

A pseudorandom unitary (PRU) is a unitary ensemble $\mathcal{E}$ that is indistinguishable from the Haar ensemble in any *efficient* quantum experiment. In particular, an ensemble $\mathcal{E}$ is a PRU ensemble with security against any $t(n)$-time quantum adversary if it cannot be distinguished from Haar-random by any quantum experiment that runs in $t(n)$ time, where $t(n)$ is any function of n [24, 28]. Unless otherwise stated, in our work we will consider security against any polynomial-time quantum experiment, $t(n) = \text{poly}\, n$. Weaker forms of security can also be considered. An ensemble $\mathcal{E}$ is a PRU ensemble with security against any *non-adaptive* $t(n)$-time quantum adversary if it cannot be distinguished from Haar-random by any quantum experiment that runs in $t(n)$ time and queries many applications of the unitary U all at once in parallel [26, 27]. The standard (i.e. adaptive) security of PRUs is analogous to the measurable error of unitary designs, and the non-adaptive security of PRUs is analogous to the additive error of unitary designs.

The standard definitions of approximate unitary k-designs and PRUs only capture quantum experiments that perform *forward* queries to a random unitary, i.e. those that query U [16]. Experiments that perform *backward* queries, i.e. which query both U and its inverse $U^\dagger$, are not captured by these definitions [16, 47]. While forward-only access is sufficient for most applications of designs and PRUs, in some cases it can be desirable to capture queries to the inverse unitary as well. To this end, one can define *strong approximate unitary k-designs* [20] and *strong PRUs* [20, 28] in an identical manner to standard designs and PRUs, but now allowing queries to the inverse (and conjugate and transpose) as well.

III. IMPOSSIBILITY OF RANDOM UNITARIES IN CONSTANT-LOCAL HAMILTONIANS

We begin by addressing the most natural physical context: time-evolution under constant-local Hamiltonians. We consider any unitary ensemble composed of time-evolution operators under any q-local Hamiltonians for any evolution times,

$$\mathcal{E} = \{e^{-iHt} \,|\, (H,t) \sim \mathcal{D}\}, \tag{III.1}$$

where $\mathcal{D}$ is an arbitrary distribution over q-local Hamiltonians H and times t. For example, these include the temporal ensemble [75], where one fixes the Hamiltonian H and randomizes the time $t \sim [0,\infty)$. They also include examples in which the time t is fixed and the Hamiltonian itself is randomized [4], as well as examples where both H and t are jointly distributed.

When the Hamiltonian H is fixed, i.e. only the time is randomized in $\mathcal{D}$, it is obvious that the ensemble $\mathcal{E}$ cannot form a unitary 1-design or PRU. This follows because one can prepare an initial state with non-zero energy under H (assuming without loss of generality that $\text{Tr}(H) = 0$), apply a unitary drawn from $\mathcal{E}$, and then measure the final energy of the system. If the unitary were Haar-random, the energy would equilibrate to zero with high probability. In contrast, under any time-evolution by H, the energy is conserved and so remains equal to its initial value.

A more interesting setting is when the Hamiltonian H is unknown a priori (i.e. random). This foils the naive distinguishing strategy above, since one does not known which basis to perform the initial state preparation and final measurement in. Nonetheless, our main result on constant-local Hamiltonians shows that this difficulty can be surmounted. We provide a simple and efficient test to distinguish any ensemble of q-local Hamiltonian evolutions from Haar-random using only two queries, product state preparation and read-out, and minimal classical computation.

This leads immediately to our no-go theorems on unitary k-designs (for any $k \geq 2$) and PRUs:

Theorem 1 (Time-evolution under constant-local Hamiltonians cannot form unitary designs)**.** *The ensemble $\mathcal{E}$ cannot form a unitary 2-design for any additive error $\varepsilon \leq \mathcal{O}(1/12^q n)$ in one-dimensional systems, nor for any $\varepsilon \leq \mathcal{O}(1/12^q n^q)$ in all-to-all connected systems.*

Theorem 2 (Time-evolution under constant-local Hamiltonians cannot form PRUs)**.** *The ensemble $\mathcal{E}$ cannot form a PRU for any $q = \mathcal{O}(\log n)$ in one-dimensional systems, nor for any $q = \mathcal{O}(1)$ in all-to-all connected systems.*

Both no-go theorems apply to any constant-local Hamiltonian time-evolution ensemble, even those with arbitrarily long evolution times. The q-dependence of both theorems is optimal, following our results in the following section. The proof of the theorems is summarized below and provided in detail in Appendix C.

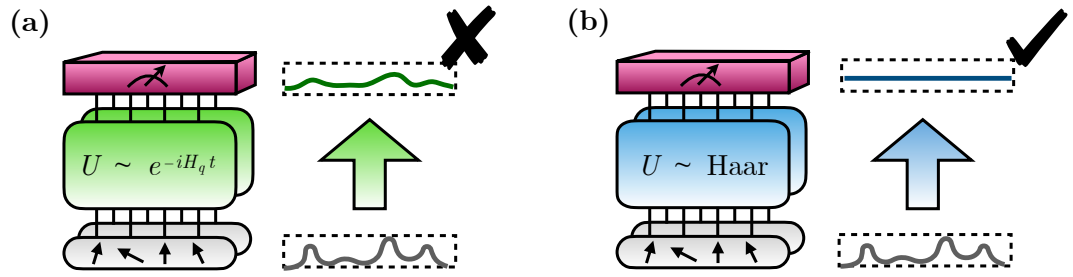

Figure 2: Illustration of our no-go result for constant-local dynamics. We show that it is possible to efficiently distinguish any ensemble $\mathcal{E}$ generated by evolving under q-local Hamiltonians up to arbitrarily long times from a Haar-random unitary by measuring random Pauli operators of weight up to q on two copies of the system, as **(a)** the output distribution of $\mathcal{E}$ retains local correlations, while **(b)** the output distribution of the Haar ensemble appears completely uniform.

Our distinguishing protocol is exceptionally simple, and bears a conceptual similarity to the distinguishing protocol discussed above when the Hamiltonian is fixed and known. We draw a random stabilizer product state $|u\rangle$ and a random Pauli operator P_i from the set of Pauli operators allowed to appear in H. That is, if H is one-dimensional, we draw P_i from the set of all q-geometrically-local Pauli operators; there are $\mathcal{O}(4^q n)$ such operators. If H is all-to-all-connected, we draw P_i from the set of all Pauli operators with weight less than or equal to q; there are $\mathcal{O}((4n)^q)$ such operators. We then prepare two copies of the product state $|u\rangle$, perform time-evolution on both copies under the same random unitary drawn from $\mathcal{E}$, and measure the Pauli operator P_i on both copies. Our main result is a proof that the expected value of the two-copy operator, $P_i \otimes P_i$—i.e. the probability that the measurements on both copies return the same value—is greater than a constant threshold value for any ensemble of constant-local Hamiltonian time-evolutions. This allows one to distinguish constant-local Hamiltonian evolutions from Haar-random, since the same expectation value is near zero under Haar-random evolution.

Intuitively, this protocol succeeds because a random product state will have a non-negligible energy under the Hamiltonian with high probability whenever H is constant-local. This follows because each term in the Hamiltonian has non-zero expectation value in a random product basis with probability $\mathcal{O}(1/3^q)$. After time-evolution, this non-negigible energy of the state must be stored in the expectation values of *some* set of Pauli operators appearing in the Hamiltonian. By selecting a random Pauli operator in the Hamiltonian, we can detect this energy with high probability, and distinguish the unitary time-evolution from Haar-random. The precise dependence on n and q follows by multiplying the probability, $\mathcal{O}(1/3^q)$, with the inverse number of Pauli operators that can appear in the Hamiltonian (Appendix C).

Finally, in the following section, we provide an additional lower bound (Proposition 1) which shows that any Hamiltonian time-evolution ensemble with polynomial evolution time requires $\mathcal{O}(nk)$ bits of randomness in the Hamiltonian. This requires Hamiltonians of locality $q = \Omega(\log k)$ in one-dimensional systems, and $q = \Omega(\log k / \log n)$ in all-to-all connected systems.

IV. FORMATION OF RANDOM UNITARIES IN NEARLY-LOCAL HAMILTONIANS

Motivated by our no-go theorems for constant-local Hamiltonian time-evolution, we will now relax our requirements, and consider Hamiltonians whose locality increases very slowly with the system size, $q = \mathrm{poly}(\log n)$. These Hamiltonians are not commonly realized in nature, where almost all systems are constant-local. Nevertheless, the study of such Hamiltonians with an increased locality has a long and fruitful history in high-energy, condensed matter, and mathematical physics [14, 76, 83–90]. In principle, such Hamiltonians might emerge as effective models for systems restricted to a low-energy subspace of their full Hilbert space. From a theoretical perspective, they will also allow us to establish that the exponential dependence on the Hamiltonian locality q in our no-go theorems is fundamental.

Our main result shows that short time-evolutions under Hamiltonians with logarithmic locality, $q = \mathcal{O}(\log n)$, are capable of forming ε-approximate unitary k-designs for any $\varepsilon = 1/\mathrm{poly}\, n$. Meanwhile, short-time evolutions under Hamiltonian with any super-logarithmic locality, $q = \omega(\log n)$, are capable of forming PRUs. This sharply contrasts with the behavior of Hamiltonians of lower locality, which are not capable of realizing designs or PRUs even after arbitrarily long evolution times, from Theorems 1 and 2. In order to rigorously establish the formation of designs and PRUs, we consider the following

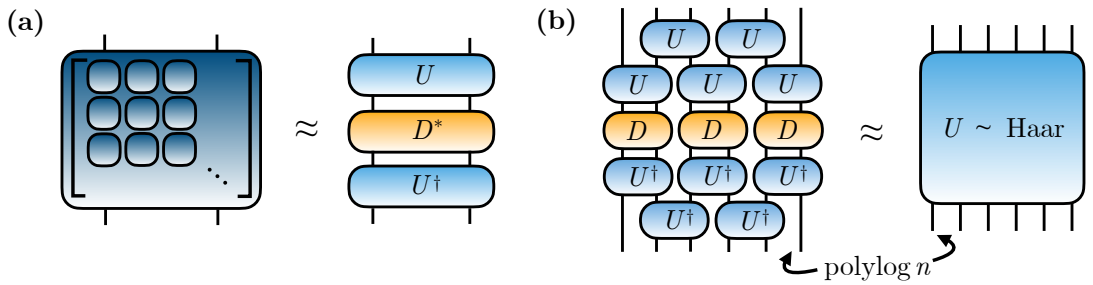

Figure 3: Graphical depiction of the asymptotic decomposition of random matrix ensembles into independent components. **(a)** Classical random matrix ensembles arising from Wigner matrices with i.i.d. elements converge to a deterministic diagonal distribution, conjugated by Haar-random eigenbasis transformations. **(b)** Our results show that Haar-random unitaries are indistinguishable from certain ensembles generated by transformations that act on subsystems of size $\mathcal{O}(\operatorname{poly}\log n)$.

random 1D Hamiltonian ensemble,

$$H = \left(\otimes_{i\in\text{even}} U_{i,i+1}\right)^\dagger \left(\otimes_{i\in\text{odd}} U_{i,i+1}\right)^\dagger \left(\sum_{i=1}^{n/\xi} \sum_{z\in\{0,1\}^\xi} J_z^i \left|z\right\rangle\!\left\langle z\right|_i\right) \left(\otimes_{i\in\text{odd}} U_{i,i+1}\right) \left(\otimes_{i\in\text{even}} U_{i,i+1}\right).$$

Here, we divide n qubits along a 1D line into n/ξ patches of ξ qubits each. We label each patch with the index $i = 1, \ldots, n/\xi$. The spectrum of the Hamiltonian is given by the central term, which is a sum of random energies $J_z^i \in [-1, 1]$ in the computational basis on each patch. The eigenbasis of the Hamiltonian is scrambled by the remaining unitary terms, which conjugate the Hamiltonian by a two-layer circuit composed of small random unitaries $U_{i,i+1}$ acting on pairs of nearest-neighbor patches [16].

We consider two instantiations of the random energies J_z^i and the small random unitaries $U_{i,i+1}$, which will allow us to realize unitary k-designs and PRUs, respectively. To realize approximate unitary k-designs, we draw each $U_{i,i+1}$ from a strong approximate unitary k-design on 2ξ qubits [20], and each J_z^i from an exact k-wise independent function on ξ bits [91, 92]. To realize PRUs, we draw each small random unitary $U_{i,i+1}$ from a strong PRU on 2ξ qubits with security against any $\operatorname{poly} n$-time quantum adversary [20, 28], and each J_z^i from a pseudorandom function (PRF) on ξ bits [91, 93]. In both cases, we then consider the unitary ensemble $\mathcal{E} = \{e^{-iHt}\}$ where H is drawn randomly as described and $t = \pi$.

Our first main result is that the first time-evolution ensemble above forms an approximate unitary k-design with measurable error ε whenever $\xi = \Omega(\log nk/\varepsilon)$.

Theorem 3 (Unitary k-designs from time-evolution under nearly-local Hamiltonians)**.** *Consider the random two-layer Hamiltonian ensemble in which each small random unitary is drawn from a strong $\frac{\varepsilon}{n}$-approximate unitary k-design and each small random phase is an exact k-wise independent function. Then the random time-evolution $U = e^{-iHt}$ for $t = \pi$ forms an ε-approximate unitary k-design for any $\xi \geq 2\log_2(nk/\varepsilon) + \mathcal{O}(1)$.*

Our second main result is that the second time-evolution ensemble above forms a PRU with security against any $\operatorname{poly} n$-time quantum adversary whenever $\xi = \omega(\log n)$.

Theorem 4 (PRUs from time-evolution under nearly-local Hamiltonians)**.** *Consider the random two-layer Hamiltonian ensemble in which each small random unitary is drawn from a strong PRU ensemble and each small random phase is drawn from a strong PRF ensemble. Then the random time-evolution $U = e^{-iHt}$ for $t = \pi$ forms a PRU, for any $\xi = \omega(\log n)$.*

Our proofs of Theorems 3 and 4 leverage the path-recording framework [28] and make several significant advancement beyond previous work. In particular, despite the appearance of the same two-layer random unitary circuit in our Hamiltonian as in [16], the gluing results of [16] strictly do not apply to our setting. This owes to the presence of the inverse unitary circuit in our Hamiltonian definition, which is necessary to ensure that the Hamiltonian is Hermitian. Instead, we prove Theorems 3 and 4 by establishing a new random unitary gluing lemma that incorporates *conjugation* by a Haar-random unitary and its inverse. Namely, for any subsystems $\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}$, we prove that the product of random unitaries, $U_{\mathsf{bc}}^\dagger (U_{\mathsf{ab}} \otimes U_{\mathsf{cd}}) U_{\mathsf{bc}}$, is indistinguishable from a random unitary on the union of the subsystems, U_{abcd}. This holds up to a measurable error that decays exponentially in the size of b and c. Despite the recent proliferation of gluing lemmas in the literature [18–23, 29], this is the first gluing lemma to our knowledge to incorporate

the commonplace phenomenon of unitary conjugation. This incorporation requires a substantially new and more intricate proof approach, owing to the presence of the inverse unitary $U_{\mathsf{bc}}^\dagger$.

To apply this gluing lemma to our ensemble of interest, we decompose each Hamiltonian time-evolution as follows,

$$e^{-iH\pi} = (\otimes_{i\in\text{even}} U_{i,i+1})^\dagger \, (\otimes_{i\in\text{odd}} U_{i,i+1})^\dagger \, (\otimes_i D_i) \, (\otimes_{i\in\text{odd}} U_{i,i+1}) \, (\otimes_{i\in\text{even}} U_{i,i+1}) \,,$$

where $D_i \equiv e^{i\pi \sum_i \sum_z J_z^i |z\rangle\langle z|_i}$ are uniformly random phases in the computational basis on each patch. We proceed in three steps. First, following earlier work [64], we show that the uniform random phases D_i, are indistinguishable from the spectrum of a Haar-random unitary on patch i. This allows us to replace each D_i—within its conjugation by the random unitary $U_{i,i+1}$—with a small Haar-random unitary U_i [64]. Second, we apply our conjugation gluing lemma $n/2\xi$ times, to replace each of the resulting $U_{i,i+1}^\dagger(U_i \otimes U_{i+1})U_{i,i+1}$ with a Haar-random unitary $U'_{i,i+1}$. In total, these two steps yield the random unitary ensemble $(\otimes_{i\in\text{even}} U_{i,i+1})^\dagger(\otimes_{i\in\text{odd}} U'_{i,i+1})(\otimes_{i\in\text{even}} U_{i,i+1})$. To complete the proof, we apply our gluing lemma $n/2\xi$ additional times, in sequence from left to right, to glue each $U'_{i,i+1}$ into a larger random unitary acting on all qubits to its left. This results in a Haar-random unitary on the entire system of n qubits, as desired. We perform a detailed analysis of the errors incurred in this approach in Appendix D 2, which yields Theorems 3 and 4.

A natural follow-up question concerns the generality of our results in Theorems 3 and 4. Does the fast formation of random unitaries hold for generic ensembles of $\mathcal{O}(\log n)$-local Hamiltonians, beyond the specific ensemble considered here? We provide some evidence towards a positive answer in the following theorem, which extends our proof of the formation of unitary designs and PRUs to a much broader range of Hamiltonian spectra and evolution times. For simplicity, we derive this extension only for additive error unitary designs and PRUs with non-adaptive security, unlike our main results which hold for measurable error unitary designs and adaptive security.

Theorem 5 (Additive error designs from generic spectra and evolution times)**.** *Consider the random two-layer Hamiltonian ensemble in Theorem 3, but in which each random diagonal term, $\sum_z J_z^i |z\rangle\langle z|_i$, is replaced with any fixed Hamiltonian H_i. The resulting time-evolution $U = e^{-iHt}$ forms an additive-error ε-approximate unitary k-design for any H_i and any time t such that $|\mathrm{Tr}(e^{-iH_i t})|^2 = o(\varepsilon/nk^2)$ for all i.*

Theorem 6 (Non-adaptive PRUs from generic spectra and evolution times)**.** *Consider the random two-layer Hamiltonian ensemble in Theorem 4, but in which each random diagonal term, $\sum_z J_z^i |z\rangle\langle z|_i$, is replaced with any fixed Hamiltonian H_i. The resulting time-evolution $U = e^{-iHt}$ forms a PRU with non-adaptive security for any H_i and any time t such that $|\mathrm{Tr}(e^{-iH_i t})|^2 = o(1/\operatorname{poly} n)$ for all i.*

Our proofs of both theorems are provided in Appendix D 1.

We conclude this section with a few remarks. First, we emphasize that the Hamiltonians we consider are efficiently described, by only a $\operatorname{poly} n$ number of random variables. They are also efficient to simulate on a quantum device for any evolution time. Both of these properties follow immediately from our use of strong unitary k-designs [20], k-wise independent functions [92], strong PRUs [20, 28], and PRFs [93], all of which have efficient descriptions and can be efficiently simulated. This is not guaranteed for general $\omega(\log n)$-local Hamiltonians, which may require $\omega(\operatorname{poly} n)$ parameters to specify.

Second, one might wonder: Is it necessary for the Hamiltonian of the system to be completely random, or might a smaller amount of randomness suffice? Indeed, a common setting for thermalization considers the scenario where the Hamiltonian is fixed, and the time is randomized instead. Unfortunately, we find that nearly all of the randomness of a unitary design composed of Hamiltonian time-evolution must come from uncertainty in the Hamiltonian itself:

Proposition 1 (Impossibility of unitary designs from efficient temporal ensembles)**.** *Consider any unitary ensemble composed of time-evolution by at most N_H many Hamiltonians for evolution times between 0 and T. Let $h \equiv \max_H \|H\|_\infty$ denote the maximum spectral norm of any Hamiltonian in the ensemble. Then the maximum evolution time T must be at least $T = \Omega(2^{nk}/(N_H h(k+1)!))$.*

The required time is exponential in the number of qubits n for any time-evolution ensemble that involves a subexponential number of Hamiltonians. The ensemble can only be efficient if there are at least $N_H = \Omega(2^{nk})$ Hamiltonians, in which case the denominator in lower bound on T cancels the numerator.

Our proof of Proposition 1 follows from a simple argument. Any approximate unitary design must contain at least $\mathcal{O}(nk)$ bits of randomness [10]. Meanwhile, randomizing the evolution time over a window $[0, T]$ can produce at most $\mathcal{O}(\log_2(\|H\|_\infty T))$ bits of randomness, since there are at most $\|H\|_\infty T$ unitaries e^{-iHt} that are distinguishable from all other such unitaries. For any normalized Hamiltonian

and polynomial evolution time, this number of bits is at most $\mathcal{O}(\log n)$, which is exponentially smaller than the required bits of randomness $\mathcal{O}(nk)$. Hence, the remaining $\mathcal{O}(nk)$ bits of randomness must come from a lack of knowledge of an extensive number of parameters of the Hamiltonian itself.

V. DISCUSSION

Our results raise several interesting questions for future work. First, while our results rule out unitary designs and PRUs from constant-local Hamiltonian dynamics, can state designs and pseudorandom states still emerge from constant-local Hamiltonian dynamics? Our no-go theorems do not extend to random states, since a random Hamiltonian ensemble could be chosen adversarially to have precisely zero energy with respect to a fixed initial state. Second, can one define an appropriate analog of unitary designs and PRUs to capture constant-local Hamiltonian time-evolutions? In particular, the Scrooge ensemble provides a promising approach for time-evolved quantum states in certain scenarios [75, 94]; however, it is unclear how to extend such notions to unitary time-evolutions. Our results also suggest that uncertainty in the parameters of the Hamiltonian itself is essential to generating enough randomness to form universal random ensembles, but it is not clear how to incorporate this insight in the context of the Scrooge ensembles. Answering these questions could yield important practical applications, for example in analog quantum experiments and simulations, and fundamental new insights on the nature of complexity and randomness in physical systems.

ACKNOWLEDGMENTS

We are grateful to Daniel Mark, John Preskill, and Adam Shaw for insightful 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 is an NSF Physics Frontiers Center.

[1] E. P. Wigner, "Random matrices in physics," *SIAM review*, vol. 9, no. 1, pp. 1–23, 1967.

[2] O. Bohigas, M.-J. Giannoni, and C. Schmit, "Characterization of chaotic quantum spectra and universality of level fluctuation laws," *Physical review letters*, vol. 52, no. 1, p. 1, 1984.

[3] S. Müller, S. Heusler, P. Braun, F. Haake, and A. Altland, "Semiclassical foundation of universality in quantum chaos," *Physical review letters*, vol. 93, no. 1, p. 014103, 2004.

[4] J. M. Deutsch, "Quantum statistical mechanics in a closed system," *Phys. Rev. A*, vol. 43, p. 2046, 1991.

[5] M. Rigol, V. Dunjko, and M. Olshanii, "Thermalization and its mechanism for generic isolated quantum systems," *Nature*, vol. 452, no. 7189, pp. 854–858, 2008.

[6] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, "Pseudo-random unitary operators for quantum information processing," *science*, vol. 302, no. 5653, pp. 2098–2100, 2003.

[7] D. Gross, K. Audenaert, and J. Eisert, "Evenly distributed unitaries: On the structure of unitary designs," *Journal of mathematical physics*, vol. 48, no. 5, 2007.

[8] C. Dankert, "Efficient simulation of random quantum states and operators," *arXiv preprint quant-ph/0512217*, 2005.

[9] C. Dankert, R. Cleve, J. Emerson, and E. Livine, "Exact and approximate unitary 2-designs and their application to fidelity estimation," *Physical Review A*, vol. 80, no. 1, p. 012304, 2009.

[10] F. G. Brandao, A. W. Harrow, and M. Horodecki, "Local random quantum circuits are approximate polynomial-designs," *Communications in Mathematical Physics*, vol. 346, pp. 397–434, 2016.

[11] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, "Efficient unitary designs with nearly time-independent hamiltonian dynamics," *arXiv preprint arXiv:1609.07021*, 2016.

[12] J. Haah, Y. Liu, and X. Tan, "Efficient approximate unitary designs from random pauli rotations," *arXiv preprint arXiv:2402.05239*, 2024.

[13] C.-F. Chen, J. Haah, J. Haferkamp, Y. Liu, T. Metger, and X. Tan, "Incompressibility and spectral gaps of random circuits," *arXiv preprint arXiv:2406.07478*, 2024.

[14] S. Guo, M. Sasieta, and B. Swingle, "Complexity is not enough for randomness," *SciPost physics*, vol. 17, no. 6, p. 151, 2024.

[15] N. LaRacuente and F. Leditzky, "Approximate unitary k-designs from shallow, low-communication circuits," *arXiv preprint arXiv:2407.07876*, 2024.

[16] T. Schuster, J. Haferkamp, and H.-Y. Huang, "Random unitaries in extremely low depth," *Science*, vol. 389, no. 6755, pp. 92–96, 2025.

[17] G. Lami, J. De Nardis, and X. Turkeshi, "Anticoncentration and state design of random tensor networks," *Physical Review Letters*, vol. 134, no. 1, p. 010401, 2025.

[18] L. Grevink, J. Haferkamp, M. Heinrich, J. Helsen, M. Hinsche, T. Schuster, and Z. Zimborás, "Will it glue? on short-depth designs beyond the unitary group," *arXiv preprint arXiv:2506.23925*, 2025.

[19] L. Cui, T. Schuster, F. Brandão, and H.-Y. Huang, "Unitary designs in nearly optimal depth," *arXiv preprint arXiv:2507.06216*, 2025.

[20] T. Schuster, F. Ma, A. Lombardi, F. Brandão, and H.-Y. Huang, "Strong random unitaries and fast scrambling," *arXiv preprint arXiv:2509.26310*, 2025.

[21] B. Foxman, N. Parham, F. Vasconcelos, and H. Yuen, "Random unitaries in constant (quantum) time," *arXiv preprint arXiv:2508.11487*, 2025.

[22] T. Schuster, D. Kufel, N. Y. Yao, and H.-Y. Huang, "Hardness of recognizing phases of matter," *Forthcoming*, 2025.

[23] Y. Zhang, S. Vijay, Y. Gu, and Y. Bao, "Designs from magic-augmented clifford circuits," *arXiv preprint arXiv:2507.02828*, 2025.

[24] Z. Ji, Y.-K. Liu, and F. Song, "Pseudorandom quantum states," in *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pp. 126–152, Springer, 2018.

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

[26] T. Metger, A. Poremba, M. Sinha, and H. Yuen, "Simple constructions of linear-depth t-designs and pseudorandom unitaries," *arXiv preprint arXiv:2404.12647*, 2024.

[27] C.-F. Chen, A. Bouland, F. G. Brandão, J. Docter, P. Hayden, and M. Xu, "Efficient unitary designs and pseudorandom unitaries from permutations," *arXiv preprint arXiv:2404.16751*, 2024.

[28] F. Ma and H.-Y. Huang, "How to construct random unitaries," in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pp. 806–809, 2025.

[29] P. Ananth, J. Bostanci, A. Gulati, and Y.-T. Lin, "Pseudorandom unitaries in the haar random oracle model," in *Annual International Cryptology Conference*, pp. 301–333, Springer, 2025.

[30] J. Emerson, R. Alicki, and K. Życzkowski, "Scalable noise estimation with random unitary operators," *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 7, no. 10, p. S347, 2005.

[31] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, "Randomized benchmarking of quantum gates," *Physical Review A*, vol. 77, no. 1, p. 012307, 2008.

[32] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, "The randomized measurement toolbox," *Nature Reviews Physics*, vol. 5, no. 1, pp. 9–24, 2023.

[33] M. Guţă, J. Kahn, R. Kueng, and J. A. Tropp, "Fast state tomography with optimal error bounds," *Journal of Physics A: Mathematical and Theoretical*, vol. 53, no. 20, p. 204001, 2020.

[34] H.-Y. Huang, R. Kueng, and J. Preskill, "Predicting many properties of a quantum system from very few measurements," *Nature Physics*, vol. 16, no. 10, pp. 1050–1057, 2020.

[35] A. Zhao, N. C. Rubin, and A. Miyake, "Fermionic partial tomography via classical shadows," *Physical Review Letters*, vol. 127, no. 11, p. 110504, 2021.

[36] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[37] A. Morvan, B. Villalonga, X. Mi, S. Mandra, A. Bengtsson, P. Klimov, Z. Chen, S. Hong, C. Erickson, I. Drozdov, *et al.*, "Phase transition in random circuit sampling," *arXiv preprint arXiv:2304.11119*, 2023.

[38] D. A. Abanin, R. Acharya, L. Aghababaie-Beni, G. Aigeldinger, A. Ajoy, R. Alcaraz, I. Aleiner, T. I. Andersen, M. Ansmann, F. Arute, *et al.*, "Constructive interference at the edge of quantum ergodic dynamics," *arXiv preprint arXiv:2506.10191*, 2025.

[39] P. Hayden and J. Preskill, "Black holes as mirrors: quantum information in random subsystems," *JHEP*, vol. 2007, no. 09, p. 120, 2007.

[40] A. Bouland, B. Fefferman, and U. Vazirani, "Computational pseudorandomness, the wormhole growth paradox, and constraints on the ads/cft duality," *arXiv preprint arXiv:1910.14646*, 2019.

[41] I. Kim, E. Tang, and J. Preskill, "The ghost in the radiation: Robust encodings of the black hole interior," *Journal of High Energy Physics*, vol. 2020, no. 6, pp. 1–65, 2020.

[42] C. Akers, N. Engelhardt, D. Harlow, G. Penington, and S. Vardhan, "The black hole interior from non-isometric codes and complexity," *arXiv preprint arXiv:2207.06536*, 2022.

[43] C. Akers, A. Bouland, L. Chen, T. Kohler, T. Metger, and U. Vazirani, "Holographic pseudoentanglement and the complexity of the ads/cft dictionary," *arXiv preprint arXiv:2411.04978*, 2024.

[44] L. Yang and N. Engelhardt, "The complexity of learning (pseudo) random dynamics of black holes and other chaotic systems," *Journal of High Energy Physics*, vol. 2025, no. 3, pp. 1–65, 2025.

[45] D. Aharonov, J. Cotler, and X.-L. Qi, "Quantum algorithmic measurement," *Nature communications*, vol. 13, no. 1, pp. 1–9, 2022.

[46] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, *et al.*, "Quantum advantage in learning from experiments," *Science*, vol. 376, no. 6598, pp. 1182–1186, 2022.

[47] J. Cotler, T. Schuster, and M. Mohseni, "Information-theoretic hardness of out-of-time-order correlators," *Physical Review A*, vol. 108, no. 6, p. 062608, 2023.

[48] W. Brown and O. Fawzi, "Decoupling with random quantum circuits," *Comm. Math. Phys.*, vol. 340, p. 867, 2015.

[49] B. Yoshida and A. Kitaev, "Efficient decoding for the hayden-preskill protocol," *arXiv preprint arXiv:1710.03363*, 2017.

[50] K. A. Landsman, C. Figgatt, T. Schuster, N. M. Linke, B. Yoshida, N. Y. Yao, and C. Monroe, "Verified quantum information scrambling," *Nature*, vol. 567, no. 7746, pp. 61–65, 2019.

[51] M. Blok, V. Ramasesh, T. Schuster, K. O'Brien, J. Kreikebaum, D. Dahlen, A. Morvan, B. Yoshida, N. Yao, and I. Siddiqi, "Quantum information scrambling on a superconducting qutrit processor," *Physical Review X*, vol. 11, no. 2, p. 021010, 2021.

[52] W. Brown and O. Fawzi, "Scrambling speed of random quantum circuits," 2012.

[53] A. Nahum, J. Ruhman, S. Vijay, and J. Haah, "Quantum Entanglement Growth Under Random Unitary Dynamics," *Phys. Rev. X*, vol. 7, p. 031016, 2017.

[54] A. Nahum, S. Vijay, and J. Haah, "Operator spreading in random unitary circuits," *Physical Review X*, vol. 8, no. 2, p. 021014, 2018.

[55] T. Schuster, B. Kobrin, P. Gao, I. Cong, E. T. Khabiboulline, N. M. Linke, M. D. Lukin, C. Monroe, B. Yoshida, and N. Y. Yao, "Many-body quantum teleportation via operator spreading in the traversable wormhole protocol," *Physical Review X*, vol. 12, no. 3, p. 031013, 2022.

[56] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, "Characterizing quantum supremacy in near-term devices," *Nature Physics*, vol. 14, no. 6, pp. 595–600, 2018.

[57] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, "On the complexity and verification of quantum random circuit sampling," *Nature Physics*, vol. 15, no. 2, p. 159, 2019.

[58] A. R. Brown and L. Susskind, "Second law of quantum complexity," *Physical Review D*, vol. 97, no. 8, p. 086015, 2018.

[59] J. Haferkamp, P. Faist, N. B. Kothakonda, J. Eisert, and N. Yunger Halpern, "Linear growth of quantum circuit complexity," *Nature Physics*, vol. 18, no. 5, pp. 528–532, 2022.

[60] J. Maldacena, S. H. Shenker, and D. Stanford, "A bound on chaos," *Journal of High Energy Physics*, vol. 2016, no. 8, pp. 1–17, 2016.

[61] D. A. Roberts and B. Yoshida, "Chaos and complexity by design," *Journal of High Energy Physics*, vol. 2017, no. 4, p. 121, 2017.

[62] J. Cotler, N. Hunter-Jones, J. Liu, and B. Yoshida, "Chaos, complexity, and random matrices," *Journal of High Energy Physics*, vol. 2017, no. 11, pp. 1–60, 2017.

[63] S. Pilatowsky-Cameo, I. Marvian, S. Choi, and W. W. Ho, "Hilbert-space ergodicity in driven quantum systems: Obstructions and designs," *Physical Review X*, vol. 14, no. 4, p. 041059, 2024.

[64] A. Gu, Y. Quek, S. Yelin, J. Eisert, and L. Leone, "Simulating quantum chaos without chaos," *arXiv preprint arXiv:2410.18196*, 2024.

[65] L. Kong and Z.-W. Liu, "Charge-conserving unitaries typically generate optimal covariant quantum error-correcting codes," *arXiv preprint arXiv:2102.11835*, 2021.

[66] L. Kong and Z.-W. Liu, "Near-optimal covariant quantum error-correcting codes from random unitaries with symmetries," *PRX Quantum*, vol. 3, no. 2, p. 020314, 2022.

[67] Z. Li, H. Zheng, and Z.-W. Liu, "Efficient quantum pseudorandomness under conservation laws," *arXiv preprint arXiv:2411.04893*, 2024.

[68] Z. Li, H. Zheng, J. Liu, L. Jiang, and Z.-W. Liu, "Designs from local random quantum circuits with su (d) symmetry," *PRX Quantum*, vol. 5, no. 4, p. 040349, 2024.

[69] H. Liu, A. Hulse, and I. Marvian, "Unitary designs from random symmetric quantum circuits," *arXiv preprint arXiv:2408.14463*, 2024.

[70] Y. Mitsuhashi, R. Suzuki, T. Soejima, and N. Yoshioka, "Unitary designs of symmetric local random circuits," *Physical Review Letters*, vol. 134, no. 18, p. 180404, 2025.

[71] J. Haah, "Short remarks on shallow unitary circuits," *arXiv preprint arXiv:2504.14005*, 2025.

[72] S. Pappalardi, L. Foini, and J. Kurchan, "Eigenstate thermalization hypothesis and free probability," *Physical Review Letters*, vol. 129, no. 17, p. 170603, 2022.

[73] M. Fava, J. Kurchan, and S. Pappalardi, "Designs via free probability," *Physical Review X*, vol. 15, no. 1, p. 011031, 2025.

[74] J. S. Cotler, D. K. Mark, H.-Y. Huang, F. Hernández, J. Choi, A. L. Shaw, M. Endres, and S. Choi, "Emergent quantum state designs from individual many-body wave functions," *PRX quantum*, vol. 4, no. 1, p. 010311, 2023.

[75] D. K. Mark, F. Surace, A. Elben, A. L. Shaw, J. Choi, G. Refael, M. Endres, and S. Choi, "Maximum entropy principle in deep thermalization and in hilbert-space ergodicity," *Physical Review X*, vol. 14, no. 4, p. 041051, 2024.

[76] E. R. Anschuetz, C.-F. Chen, B. T. Kiani, and R. King, "Strongly interacting fermions are nontrivial yet nonglassy," *Physical Review Letters*, vol. 135, no. 3, p. 030602, 2025.

[77] N. Wiebe, C. Granade, C. Ferrie, and D. G. Cory, "Hamiltonian learning and certification using quantum resources," *Physical Review Letters*, vol. 112, no. 19, p. 190501, 2014.

[78] T. J. Evans, R. Harper, and S. T. Flammia, "Scalable bayesian Hamiltonian learning," *arXiv preprint arXiv:1912.07636*, 2019.

[79] J. Haah, R. Kothari, and E. Tang, "Optimal learning of quantum Hamiltonians from high-temperature Gibbs states," *arXiv preprint arXiv:2108.04842*, 2021.

[80] H.-Y. Huang, Y. Tong, D. Fang, and Y. Su, "Learning many-body hamiltonians with heisenberg-limited scaling," *Physical Review Letters*, vol. 130, no. 20, p. 200403, 2023.

[81] A. Dutkiewicz, T. E. O'Brien, and T. Schuster, "The advantage of quantum control in many-body Hamiltonian learning," *arXiv preprint arXiv:2304.07172*, 2023.

[82] A. Bakshi, A. Liu, A. Moitra, and E. Tang, "Structure learning of hamiltonians from real-time evolution," in *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 1037–1050, IEEE, 2024.

[83] M. Mezard and A. Montanari, *Information, physics, and computation*. Oxford University Press, 2009.

[84] H. Steinacker, "Emergent geometry and gravity from matrix models: an introduction," *Classical and Quantum Gravity*, vol. 27, no. 13, p. 133001, 2010.

[85] J. Maldacena and D. Stanford, "Remarks on the Sachdev-Ye-Kitaev model," *Physical Review D*, vol. 94, no. 10, p. 106002, 2016.

[86] X.-L. Qi and A. Streicher, "Quantum epidemiology: operator growth, thermal effects, and syk," *Journal of High Energy Physics*, vol. 2019, no. 8, 2019.

[87] H. Lin and L. Susskind, "Infinite temperature's not so hot," *arXiv preprint arXiv:2206.01083*, 2022.

[88] M. Berkooz and O. Mamroud, "A cordial introduction to double scaled syk," *Reports on Progress in Physics*, vol. 88, no. 3, p. 036001, 2025.

[89] B. Swingle and M. Winer, "Bosonic model of quantum holography," *Physical Review B*, vol. 109, no. 9, p. 094206, 2024.

[90] C.-F. Chen, A. M. Dalzell, M. Berta, F. G. Brandão, and J. A. Tropp, "Sparse random hamiltonians are quantumly easy," *Physical Review X*, vol. 14, no. 1, p. 011014, 2024.

[91] To be precise, for unitary k-designs, we specify each J_z^i up to $m = \Omega(\log k/\varepsilon)$ bits and draw each bit from a k-wise independent function $f : \{0,1\}^\xi \to \{0,1\}$. For PRUs, we specify each J_z^i up to $m = \omega(\log n)$ bits and draw each bit from a pseudorandom function $f : \{0,1\}^\xi \to \{0,1\}$.

[92] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of computer and system sciences*, vol. 22, no. 3, pp. 265–279, 1981.

[93] M. Zhandry, "How to construct quantum random functions," *J. ACM*, vol. 68, aug 2021.

[94] R. Jozsa, D. Robb, and W. K. Wootters, "Lower bound for accessible information in quantum mechanics," *Physical Review A*, vol. 49, no. 2, p. 668, 1994.

[95] W. Fulton and J. Harris, *Representation theory: a first course*, vol. 129. Springer Science & Business Media, 2013.

[96] R. Goodman, N. R. Wallach, *et al.*, *Symmetry, representations, and invariants*, vol. 255. Springer, 2009.

[97] B. Collins and P. Śniady, "Integration with respect to the haar measure on unitary, orthogonal and symplectic group," *Communications in Mathematical Physics*, vol. 264, no. 3, pp. 773–795, 2006.

[98] M. Zhandry, "How to record quantum queries, and applications to quantum indifferentiability," in *Annual International Cryptology Conference*, pp. 239–268, Springer, 2019.

[99] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, "The randomized measurement toolbox," *Nature Review Physics*, 2022.

Appendices

CONTENTS

A. Review of Haar-random unitaries, unitary designs, and pseudorandom unitaries 12
1. Haar-random unitaries 12
2. Unitary designs 13
a. Additive error and parallel indistinguishability 13
b. Measurable error and adaptive indistinguishability 14
3. Pseudorandom unitaries 15

B. Review of the path-recording framework 15
1. Relation state registers 15
2. Restrictions on relation states 16
3. The path-recording oracle 17
4. The partial path-recording oracle 18
5. Approximate purification of the Haar twirl 19

C. Impossibility of random unitaries from constant-local Hamiltonian dynamics 20

D. Formation of random unitaries from nearly-local Hamiltonian dynamics 21
1. Proof of Theorems 5 and 6: Indistinguishability in non-adaptive quantum experiments 21
a. Moments of the random Hamiltonian dynamics 21
b. Gluing argument for nearly-local dynamics 24
c. Designs via local spectral distribution 26
d. A simple alternative construction and proof 27
2. Proof of Theorems 3 and 4: Indistinguishability in adaptive quantum experiments 28
a. Proof of Lemma 11: Conjugated random phases are random unitaries 29
b. Proof of Lemma 12: Gluing random unitaries via conjugation 29
3. Proof of Proposition 1: Impossibility of unitary designs from efficient temporal ensembles 31

Appendix A: Review of Haar-random unitaries, unitary designs, and pseudorandom unitaries

In this section, we provide a more detailed review of the definitions and key properties of Haar-random unitaries, unitary designs, and pseudorandom unitaries (PRUs).

1. Haar-random unitaries

We now review properties of Haar-random unitaries, which form a uniformly and maximally random distribution against which we compare other ensembles. In this context, the Haar measure is given by the unique translation-invariant measure on the unitary group $U(N)$.

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

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

where we have left out the implicit dependence on k.

This definition captures the expectation over how X transforms when we apply k copies of a Haar-random unitary U. By linearity, this is equivalent to considering an arbitrary entangled input state $|\psi\rangle$ on $nk + m$ qubits. The structure of these moments can be determined using representation theoretic properties of the unitary group. By definition, these expectation values must be invariant under any unitary change of basis applied to each individual copy. Applying Schur-Weyl duality [95, 96] yields that the moments must be of the following form:

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

$$\Phi_H(X) = \sum_{\sigma,\tau\in S_k} c_{\sigma,\tau} \operatorname{Tr}(\sigma X)\cdot\tau, \tag{A.2}$$

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

In principle, the coefficients $c_{\sigma,\tau}$ can be computed exactly using combinatorial formulas derived from the Weingarten calculus of the unitary group [97]. However, the main property of the moments that we use is their relationship to the symmetric group on k copies of the physical systems. In particular, the techniques in our work rely on the key observation that a large fraction of the moments are supported on the *distinct subspace*, which is spanned by the symmetrized vectors corresponding to elements of $[N]^k_{\text{dist}}$:

Definition 2 (Distinct subspace [26])**.** *The projector onto the* distinct subspace *is given by the operator*

$$\Pi^{\text{dist}} = \sum_{\mathbf{x}\in[N]^k_{\text{dist}}} |x\rangle\langle x|\,, \tag{A.3}$$

where $[N]^k_{\text{dist}} = \{\mathbf{x} = (x^{(1)}, x^{(2)}, ..., x^{(k)}) : x^{(i)} \neq x^{(j)} \text{ for } i \neq j\}$. The subspace has dimension $\mathfrak{D} = (2^n)!/(2^n-k)!$ which obeys $1 - k^2/2^n \leq \mathfrak{D}/2^{nk} \leq 1$.

Notably, nearly all bitstrings are distinct when $k^2 \ll 2^n$. Thus for any input state on the physical system, "most" of the moments are also supported on this subspace. This fact was originally applied to analyze state designs in [25], and since then has been extended to various frameworks for analyzing unitary ensembles [19, 26, 28].

In addition, is often useful to apply these restrictions to a *locally* distinct subspace corresponding to some subsystems of subextensive size, similar to the techniques of [19]. In particular, for subsystems of size ξ, the corresponding local distinct subspace is given as the space spanned by the symmetrized vectors corresponding to elements of $[2^\xi]^k_{\text{dist}}$ on each subsystem:

Definition 3 (Local distinct subspace [19])**.** *For any system of n qubits divided into patches of ξ qubits each, let* loc-dist $= \{\mathbf{x} : x_a^{(i)} \neq x_a^{(j)} \text{ for all } a \text{ and } i \neq j\}$ *denote the set of locally distinct* $\mathbf{x}$*. The* local distinct subspace *corresponding to S is defined by the projector*

$$\Pi^{\text{dist}}_{\text{loc}} = \sum_{x\in\text{loc-dist}} |x\rangle\langle x|\,. \tag{A.4}$$

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

In the following sections, we discuss how the properties of the k-wise twirls over different ensembles relate to notions of indistinguishability from Haar-random.

2. Unitary designs

a. Additive error and parallel indistinguishability

The most well-studied notion of statistical distance for unitary ensembles is additive error, which is given by the difference between the moments in diamond norm:

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

$$\|\Phi_{\mathcal{E}} - \Phi_H\|_\diamond \leq \varepsilon, \tag{A.5}$$

where we have used the abbreviated notation

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

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

Recall that the diamond norm is defined via $\|\Phi - \Phi'\|_\diamond = \max_\rho \|\Phi(\rho) - \Phi'(\rho)\|_1$, where the maximization is over all input states ρ on $nk + m$ qubits, including an arbitrarily large ancillary system of size m. This norm thus measures the maximum distinguishability of $\Phi_\mathcal{E}$ and Φ_H, which apply k copies of a random unitary U in parallel. It follows that the additive error definition is equivalent to the maximum distinguishability of $\mathcal{E}$ from the Haar ensemble in any quantum experiment that queries k copies of the unitary U in parallel.

Fact 2 (Additive error is equivalent to parallel indistinguishability)**.** *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.*

b. Measurable error and adaptive indistinguishability

Certain settings in quantum complexity theory and cryptography demand indistinguishability under more general quantum experiments that can query k copies of U. It is known that this condition is strictly stronger than indistinguishability under queries to $U^{\otimes k}$, i.e., k parallel queries to U [26, 28].

In particular, we consider quantum experiments making k queries to U which can apply the unitary in sequence and with arbitrary quantum operations in between each query. This is much more powerful as it enables the quantum experiment to learn some properties about U, then adaptively probe the unitary U based on the properties it has learned. The formulation of a general quantum experiment that makes k queries to U is given as follows.

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

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

To capture indistinguishability under the most powerful quantum experiments that make up to k queries to a unitary U, we require a corresponding stronger notion of approximation error, the measurable error [19]. This quantity is given by the maximum distinguishability between a random unitary ensemble and the Haar ensemble over all possible k-query quantum experiments. Moreover, whenever this error is large, there exists a quantum experiment that can distinguish the two ensembles.

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

$$\sup_{T_1 \cdots T_{k+1}} \|\rho_\mathcal{E} - \rho_H\|_1 \leq \varepsilon, \tag{A.7}$$

where we have used the notation

$$\rho_\mathcal{E} = \mathop{\mathbb{E}}_{U \sim \mathcal{E}} \left[T_{k+1}[U \otimes \mathbb{1}_m] T_k \cdots T_2 [U \otimes \mathbb{1}_m] T_1 |0^{n+m}\rangle\langle 0^{n+m}| T_1^\dagger [U^\dagger \otimes \mathbb{1}_m] T_2^\dagger \cdots T_k^\dagger [U^\dagger \otimes \mathbb{1}_m] T_{k+1}^\dagger \right] \tag{A.8}$$

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

In addition, it is shown in [19] that these experiments are equivalent to ones which use only k parallel queries, followed by a postselection on a Bell state on nk qubits. We refer to Section IV.B of the Supplementary Material [19] for more details.

3. Pseudorandom unitaries

In the context of quantum cryptography, pseudorandom unitary (PRU) ensembles are families of unitaries which can be efficiently constructed but are *computationally* indistinguishable from Haar-random [24] by any adversary with only polynomial resources:

Definition 7 (Pseudorandom unitary ensemble)**.** *A family of unitaries defined via* $\mathcal{U}_n = \{U_\alpha \in U(2^n)\}_\alpha$ *is pseudorandom with* non-adaptive *security if it satisfies the following:*

1. *(Efficient implementation) There exists an efficient algorithm* Q *such that for any* $U_\alpha \in \mathcal{U}_n$ *and* $|\psi\rangle \in \mathbb{C}^{2^n}$, $Q(\alpha, |\psi\rangle) = U_\alpha |\psi\rangle$.
2. *(Computational indistinguishability) For* $U_\alpha \sim \mathcal{U}_n$ *and* $k \in \mathrm{poly}(n)$, U_α *is computationally indistinguishable from* k *copies of a Haar-random unitary operator. More precisely, for any efficient quantum algorithm* $\mathcal{T}$ *which uses at most* k *copies of* U_α,

$$\left| \mathop{\mathbb{E}}_{\alpha} [\mathcal{T}[U_\alpha](|0\rangle^k) = 1] - \mathop{\mathbb{E}}_{U \sim \mathsf{Haar}} [\mathcal{T}[U](|0\rangle^k) = 1] \right| = \mathrm{negl}(n). \tag{A.9}$$

Here $\mathrm{negl}(n)$ denotes an inverse superpolynomial scaling $1/\omega(\mathrm{poly}\, n)$. While the efficient implementation condition is straightforward to check given a description of $\mathcal{U}_n$ and a protocol to implement U_α, it is more difficult to directly bound the computational distinguishability of $\mathcal{U}_n$ from the Haar ensemble. However, it is sufficient to show that it is indistinguishable from a Haar-random unitary transformation even with access to arbitrary generalized measurements:

Fact 3 (Sufficient condition for computational indistinguishability)**.** *Suppose for any* $k = O(\mathrm{poly}\, n)$, $\mathcal{U}_n$ *forms an approximate unitary* k*-design up to* $\epsilon = 1/\omega(\mathrm{poly}\, n)$. *Then* $U_\alpha \sim \mathcal{U}_n$ *is also* computationally *indistinguishable from a Haar-random unitary.*

It is common to consider settings which allow either at most k parallel or k sequential queries, corresponding to closeness in additive or measurable error, respectively [26]. The existence of PRUs in the adaptive setting remained an open question until very recently, when it was resolved in [28] assuming the existence of quantum-secure pseudorandom functions on bitstrings. In the following section, we provide an overview of techniques introduced in [28] in order to analyze queries to, or applications of, random unitary transformations.

Appendix B: Review of the path-recording framework

In this section we summarize the path-recording framework, which was introduced in [28] as a framework for analyzing the security of PRUs, including the usual adaptive setting as well as a stronger version where the adversary has access to both U and $U^\dagger$.

1. Relation state registers

In order to analyze the ensembles of interest, it is often useful to consider additional working registers which can be used to approximately reconstruct the twirling operation. In particular, we introduce *relation state* registers to record how the basis states are shuffled by the Haar twirl. Here we define a relation R as a multiset of ordered pairs $\{(x_1, y_1), \ldots, (x_k, y_k)\}$, where $(x_i, y_i) \in [N]^2$. The *size* $|R|$ equals the number of pairs counting multiplicities.

Definition 8 (Sets of relations)**.** *Let* $\mathcal{R}$ *denote the set of all relations and* $\mathcal{R}_k$ *the set of all length-*k *relations. Then define*

$$\mathrm{Dom}(R) = \{x \in [N] : \exists y \text{ such that } (x, y) \in R\}, \tag{B.1}$$

$$\mathrm{Im}(R) = \{y \in [N] : \exists x \text{ such that } (x, y) \in R\}, \tag{B.2}$$

$$\mathrm{Dom}_J(R) = \{x_J \in [2^{|J|}] : \exists x, y \text{ such that } (x, y) \in R \text{ and } \forall j \in J, x^{(j)} = x_J^{(j)}\}, \tag{B.3}$$

$$\mathrm{Im}_J(R) = \{y_J \in [2^{|J|}] : \exists x, y \text{ such that } (x, y) \in R \text{ and } \forall j \in J, y^{(j)} = y_J^{(j)}\}, \tag{B.4}$$

where $J \subseteq [n]$ *corresponds to a subset of the physical registers.*

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

Definition 9 (Relation states)**.** *For relation $R = \{(x_1, y_1), \ldots, (x_k, y_k)\}$, define*

$$|R\rangle = \frac{\sum_{\pi \in S_k} |x_{\pi(1)}, y_{\pi(1)}, \ldots, x_{\pi(k)}, y_{\pi(k)}\rangle}{\sqrt{k! \cdot \prod_{(x,y)\in[N]^2} \mathsf{num}(R,(x,y))!}}, \tag{B.5}$$

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

The relation states form an orthonormal basis for the symmetric subspace of $(\mathbb{C}^{N^2})^{\otimes k}$. When all pairs in R are distinct, the normalization simplifies to $1/\sqrt{k!}$. In addition, we often consider relation state registers which may be of *variable* length:

Definition 10 (Variable-length registers)**.** *For $k \geq 0$, let $\mathsf{R}^{(k)}$ be a register with Hilbert space $\mathcal{H}_{\mathsf{R}^{(k)}} = (\mathbb{C}^N \otimes \mathbb{C}^N)^{\otimes k}$. Define the variable-length register R with infinite-dimensional Hilbert space*

$$\mathcal{H}_{\mathsf{R}} = \bigoplus_{t=0}^{\infty} \mathcal{H}_{\mathsf{R}^{(k)}} = \bigoplus_{t=0}^{\infty} (\mathbb{C}^N \otimes \mathbb{C}^N)^{\otimes k}. \tag{B.6}$$

Moreover, we can decompose $\mathsf{R}^{(k)} = (\mathsf{R}_{\mathsf{X}}^{(k)}, \mathsf{R}_{\mathsf{Y}}^{(k)})$ where $\mathsf{R}_{\mathsf{X}}^{(k)} = |x_1, \ldots, x_k\rangle$ and $\mathsf{R}_{\mathsf{Y}}^{(k)} = |y_1, \ldots, y_k\rangle$. Due to the direct sum structure, relation states of different lengths are orthogonal.

2. Restrictions on relation states

We now discuss restricted sets of relation states. These play an analogous role in our analysis of the path-recording oracle to that of the distinct subspace projection described in Definition 2 for the analysis of the Haar twirl in previous work [19, 25, 26].

Definition 11 (Restricted relation sets)**.** *We define variants of restricted relation sets as follows.*

- $\mathcal{R}_k^{inj}$*: injective relations where $(y_1, \ldots, y_k) \in [N]_{dist}^k$*
- $\mathcal{R}_k^{bij}$*: bijective relations where $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in [N]_{dist}^k$*

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

We now introduce projection operators which act on the space of relation states.

Definition 12 (Projectors and extensions)**.** *Define the projector onto relation states of length k:*

$$\Pi_k^{\mathcal{R}} = \sum_{R \in \mathcal{R}_k} |R\rangle\langle R| = \Pi_{\mathsf{sym}}^{N^2,k}, \tag{B.7}$$

where $\Pi_{\mathsf{sym}}^{N^2,k}$ projects onto the symmetric subspace of $(\mathbb{C}^{N^2})^{\otimes k}$.

We introduce additional notation for constructions involving two variable-length registers such as L and R which correspond to forward and inverse applications of the same unitary.

Definition 13 (Length projectors)**.** *For integers $\ell, r \geq 0$, let $\Pi_{\ell,r}$ project onto $\mathcal{H}_{\mathsf{L}^{(\ell)}} \otimes \mathcal{H}_{\mathsf{R}^{(r)}}$. For integer $t \geq 0$, let $\Pi_{\leq k}$ project onto $\bigoplus_{\ell,r\geq 0:\ell+r\leq k} \mathcal{H}_{\mathsf{L}^{(\ell)}} \otimes \mathcal{H}_{\mathsf{R}^{(r)}}$.*

Definition 14 (Length-restricted operators)**.** *For operator B acting on registers L and R, define*

$$B_{\ell,r} = B \cdot \Pi_{\ell,r}, \tag{B.8}$$

$$B_{\leq k} = B \cdot \Pi_{\leq k}. \tag{B.9}$$

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

Definition 15 (Restricted order pairs of relation sets)**.** *Let $\mathcal{R}^{2,\mathrm{dist}}$ be the set of all ordered pairs of relations $(L,R) \in \mathcal{R}^2$ where $L \cup R = \{(x_1, y_1), \ldots, (x_t, y_t))\}$ is a bijective relation, i.e., $x_1, \ldots, x_t$ are distinct and $y_1, \ldots, y_t$ are distinct.*

Definition 16 (Bijective-relation projectors)**.** *Define the projectors*

$$\Pi^{\mathsf{bij}}_{\mathsf{LR}} \coloneqq \sum_{(L,R)\in\mathcal{R}^{2,\mathrm{dist}}} |L\rangle\langle L|_{\mathsf{L}} \otimes |R\rangle\langle R|_{\mathsf{R}}\,, \qquad \Pi^{\mathsf{bij}}_{\leq k,\mathsf{LR}} \coloneqq \Pi^{\mathsf{bij}}_{\mathsf{LR}} \cdot \Pi_{\leq k,\mathsf{LR}} = \Pi_{\leq k,\mathsf{LR}} \cdot \Pi^{\mathsf{bij}}_{\mathsf{LR}}, \tag{B.10}$$

where the projector $\Pi_{\leq k,\mathsf{LR}}$ is the maximum-length projector given by Definition 13.

In addition, we state the following properties, which are often useful for bounding statistical distances between quantum states.

Fact 4. *For any pure states $|u\rangle, |v\rangle$ with $\langle u|u\rangle, \langle v|v\rangle \leq 1$,*

$$\big\| |u\rangle\langle u| - |v\rangle\langle v| \big\|_1 \leq 2 \big\| |u\rangle - |v\rangle \big\|_2, \tag{B.11}$$

where the $\|\cdot\|_2$ on the RHS denotes the vector 2-norm.

Lemma 1 (Gentle measurement lemma)**.**

$$\big\|\Pi\rho\Pi - \rho\big\|_1 \leq 2\sqrt{1 - \mathrm{Tr}(\Pi\rho)}. \tag{B.12}$$

Lemma 2 (Sequential gentle measurement (Lemma 2.3 of [28]))**.** *Let $|\psi\rangle$ be a normalized state, $P_1, \ldots, P_k$ be projectors, and $U_1, \ldots, U_k$ be unitaries.*

$$\|U_k \ldots U_1 |\psi\rangle - P_k U_k \ldots P_1 U_1 |\psi\rangle\|_2 \leq k\sqrt{1 - \|P_k U_k \ldots P_1 U_1 |\psi\rangle\|_2^2}. \tag{B.13}$$

3. The path-recording oracle

We now present definitions and useful technical results for the path-recording oracle framework introduced in [28]. This construction builds upon a line of work [98] from the cryptography literature on using purification oracles to analyze notions of computational security against quantum adversaries.

Definition 17 (Oracle adversaries)**.** *A k-query oracle adversary $\mathcal{T}$ is parameterized by a sequence of $(n+m)$-qubit unitaries $(T_1, \ldots, T_{k+1})$ acting on registers (A, B), where A is the n-qubit query register and B is an m-qubit ancilla, and a sequence of oracle queries $U_1, \ldots, U_k$ where each $U_i \in \{U, U^\dagger\}$. The state after k queries is*

$$|\mathcal{T}_k^U\rangle_{\mathsf{AB}} = T_{k+1}[U_k \otimes \mathbb{1}_m] \cdots T_2[U_1 \otimes \mathbb{1}_m] T_1 |0^{n+m}\rangle_{\mathsf{AB}}\,. \tag{B.14}$$

The path-recording oracle V proposed in [28] efficiently simulates a Haar-random unitary U under both queries to U and $U^\dagger$. Informally, V can be understood as a unitary oracle which constructs an approximate purification for the Haar twirl, such that tracing out over the auxiliary working registers results in a state which indistinguishable from the output of the Haar twirl. To define the path-recording oracle V, we separately construct the left and right parts, or V^L and V^R, respectively.

Definition 18 (Left and right parts of V)**.** *Let V^L be the linear operator that acts as follows. For $x \in [N]$ and $(L, R) \in \mathcal{R}^{2,\leq N-1}$,*

$$V^L \cdot |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \sum_{\substack{y\in[N]:\\ y\notin \mathrm{Im}(L\cup R)}} \frac{1}{\sqrt{N - |\mathrm{Im}(L\cup R)|}} |y\rangle_{\mathsf{A}} |L\cup\{(x,y)\}\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}}\,. \tag{B.15}$$

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

$$V^R \cdot |y\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \sum_{\substack{x\in[N]:\\ x\notin \mathrm{Dom}(L\cup R)}} \frac{1}{\sqrt{N - |\mathrm{Dom}(L\cup R)|}} |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\cup\{(x,y)\}\rangle_{\mathsf{R}}\,. \tag{B.16}$$

By construction, V^L and V^R take states in $\mathbb{1}_{\mathsf{A}} \otimes \Pi^{\mathcal{R}^2}_{\leq i,\mathsf{LR}}$ to $\mathbb{1}_{\mathsf{A}} \otimes \Pi^{\mathcal{R}^2}_{\leq i+1,\mathsf{LR}}$.

Fact 5 (Claim 14 [28])**.** *V^L and V^R are partial isometries.*

Definition 19 (Path-recording oracle V)**.** *The path-recording oracle is the operator V defined as*

$$V = V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger}) + (\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}. \tag{B.17}$$

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

Fact 6 (Claim 15 in [28])**.** *V is a partial isometry.*

4. The partial path-recording oracle

Another useful construction from [28] is the partial path-recording oracle W, which is a restricted version of the full 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 $\mathcal{R}^{2,\mathrm{dist}}$. Similar to V, the partial path-recording oracle W contains a left part W^L and a right part W^R.

Definition 20 (W^L and W^R)**.** *Define W^L to be the linear map such that for any $(L,R) \in \mathcal{R}^{2,\mathrm{dist}}$ and $x \in [N]$ such that $x \notin \mathrm{Dom}(L \cup R)$,*

$$W^L \cdot |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{y \in [N]: \\ y \notin \mathrm{Im}(L \cup R)}} |y\rangle_{\mathsf{A}} |L \cup \{(x,y)\}\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}}. \tag{B.18}$$

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

$$W^R \cdot |y\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{x \in [N]: \\ x \notin \mathrm{Dom}(L \cup R)}} |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R \cup \{(x,y)\}\rangle_{\mathsf{R}}. \tag{B.19}$$

Definition 21. *The partial path-recording oracle is the operator W defined as*

$$W = W^L + W^{R,\dagger}. \tag{B.20}$$

Lemma 3 (Fact 5 in [28])**.** *For any integer $i \geq 0$, W^L, W^R map states in the subspace associated to the projector $\mathbb{1}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\leq i,\mathsf{LR}}$ into the subspace associated with the projector $\mathbb{1}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\leq i+1,\mathsf{LR}}$.*

Fact 7 (Claims 9 and 11 in [28])**.** *W^L, W^R, W are partial isometries.*

It is useful to introduce projectors of the following form, which we use restrict to valid relation states corresponding to the action of V or W:

Definition 22. *For a partial isometry G, let $\mathrm{Dom}(G)$ and $\mathrm{Im}(G)$ denote its domain and image. Let $\Pi^{\mathrm{Dom}(G)} = G^\dagger \cdot G$ and $\Pi^{\mathrm{Im}(G)} = G \cdot G^\dagger$ denote the orthogonal projectors onto $\mathrm{Dom}(G)$ and $\mathrm{Im}(G)$.*

Lemma 4 (Fact 8 in [28])**.** *The domain and image of the partial isometry W are given by*

$$\Pi^{\mathrm{Dom}(W)} = \Pi^{\mathrm{Dom}(W^L)} + \Pi^{\mathrm{Im}(W^R)}, \tag{B.21}$$

$$\Pi^{\mathrm{Im}(W)} = \Pi^{\mathrm{Dom}(W^R)} + \Pi^{\mathrm{Im}(W^L)}. \tag{B.22}$$

Lemma 5 (W is a restriction of V (Claim 17 of [28]))**.** *We have*

$$W = V \cdot \Pi^{\mathrm{Dom}(W)}, \tag{B.23}$$

$$W^\dagger = V^\dagger \cdot \Pi^{\mathrm{Im}(W)}. \tag{B.24}$$

We now present a key property of W which enables us to analyze approximate purifications on a distinct subspace, after twirling by exact unitary 2-designs.

Lemma 6 (Twirling by unitary 2-design (Lemma 9.2 in [28]))**.** *For any unitary 2-design $\mathfrak{C}$, and any integer $0 \leq t \leq N-1$, we have*

$$\left\| \mathop{\mathbb{E}}_{C,D \sim \mathfrak{C}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathsf{bij}}_{\leq t,\mathsf{LR}} - \Pi^{\mathrm{Dom}(W)}_{\leq t,\mathsf{ALR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_\infty \leq 6t\sqrt{\frac{t}{N}}, \tag{B.25}$$

$$\left\| \mathop{\mathbb{E}}_{C,D\sim\mathfrak{C}} (D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathsf{bij}}_{\leq t,\mathsf{LR}} - \Pi^{\mathrm{Im}(W)}_{\leq t,\mathsf{ALR}}\right) \cdot (D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}}) \right\|_\infty \leq 6t\sqrt{\frac{t}{N}}. \tag{B.26}$$

5. Approximate purification of the Haar twirl

We proceed to describe the action of the path-recording oracle on the system.

Definition 23 (Global state after queries to $V, V^\dagger$)**.** *For a k-query oracle adversary $\mathcal{T}$ that can perform queries to $U, U^\dagger$, where $b_i \in \{0,1\}$ correspond to $U, U^\dagger$, respectively, and any $0 \leq i \leq k$, let*

$$|\mathcal{T}_i^V\rangle_{\mathsf{ABLR}} = \prod_{i=1}^{k} \left(\left((1-b_i)\cdot V_{\mathsf{ALR}} + b_i \cdot V_{\mathsf{ALR}}^\dagger \right) \cdot A_{i,\mathsf{AB}} \right) |0^{n+m}\rangle_{\mathsf{AB}} \otimes |\varnothing\rangle_{\mathsf{L}} |\varnothing\rangle_{\mathsf{R}} \tag{B.27}$$

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

We will also consider the global purified state after queries to $W, W^\dagger$, where we twirl the input and the output states by two independent random unitaries sampled from a unitary 2-design. For this purpose, it is convenient to define the purification of two random unitaries C, D which modify the basis of the input and output to the (partial) path-recording oracle.

Definition 24. *For any distribution $\mathfrak{C}$ over n-qubit unitaries, define the state*

$$|\mathsf{init}(\mathfrak{C})\rangle_{\mathsf{CD}} \coloneqq \int_{C,D} \sqrt{d\mu_{\mathfrak{C}}(C) d\mu_{\mathfrak{C}}(D)}\, |C\rangle_{\mathsf{C}} \otimes |D\rangle_{\mathsf{D}}\,, \tag{B.28}$$

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

Definition 25 (Controlled C, D and Q)**.** *Define the following operators*

$$\mathsf{cC} \coloneqq \int_C C_{\mathsf{A}} \otimes |C\rangle\langle C|_{\mathsf{C}}\,, \quad \mathsf{cD} \coloneqq \int_D D_{\mathsf{A}} \otimes |D\rangle\langle D|_{\mathsf{D}}\,, \tag{B.29}$$

$$\mathsf{cQ} \coloneqq \int_{C,D} Q[C,D]_{\mathsf{L,R}} \otimes |C\rangle\langle C|_{\mathsf{C}} \otimes |D\rangle\langle D|_{\mathsf{D}}\,. \tag{B.30}$$

Definition 26 (Global state after queries to twirled $W, W^\dagger$)**.** *For a k-query adversary $\mathcal{T}$ that can perform queries to $U, U^\dagger$, where $b_i \in \{0,1\}$ correspond to $U, U^\dagger$, let*

$$|\mathcal{T}_0^{W,\mathfrak{C}}\rangle = |0^n\rangle_{\mathsf{A}} |0^m\rangle_{\mathsf{B}} |\varnothing\rangle_{\mathsf{L}} |\varnothing\rangle_{\mathsf{R}} |\mathsf{init}(\mathfrak{C})\rangle_{\mathsf{CD}}\,. \tag{B.31}$$

For i from 1 to t, let

$$|\mathcal{T}_i^{W,\mathfrak{C}}\rangle = \left((1-b_i)\cdot(\mathsf{cD}\cdot W\cdot \mathsf{cC}) + b_i \cdot (\mathsf{cD}\cdot W\cdot \mathsf{cC})^\dagger \right) \cdot A_i \cdot |\mathcal{T}_{i-1}^{W,\mathfrak{C}}\rangle\,. \tag{B.32}$$

Finally, we present key properties of the path-recording oracle V which enable them to be used to simulate the action of Haar-random unitaries.

Lemma 7 (W is indistinguishable from V after twirling (Lemma 9.3 in [28]))**.** *Let $\mathfrak{C}$ be any exact unitary 2-design. For any k-query oracle adversary $\mathcal{T}$ that can query $\mathcal{O}, \mathcal{O}^\dagger$,*

$$\left\| \mathrm{Tr}_{-\mathsf{AB}}\, |\mathcal{T}_k^{W,\mathfrak{C}}\rangle\langle\mathcal{T}_k^{W,\mathfrak{C}}|_{\mathsf{ABLRCD}}\,, \mathrm{Tr}_{-\mathsf{AB}}\, |\mathcal{T}_k^{V}\rangle\langle\mathcal{T}_k^{V}|_{\mathsf{ABLR}} \right\|_1 \leq \frac{18k}{N^{1/8}}. \tag{B.33}$$

Lemma 8 (Two-sided unitary invariance (Claim 16 in [28]))**.** *For any integer $0 \leq k \leq N-1$ and any pair of n-qubit unitaries C, D,*

$$\| D_{\mathsf{A}} \cdot V_{\leq k} \cdot C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq k} \|_\infty \leq 16\sqrt{\frac{2k(k+1)}{N}}, \tag{B.34}$$

$$\left\| C_{\mathsf{A}}^\dagger \cdot (V^\dagger)_{\leq k} \cdot D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot (V^\dagger)_{\leq k} \right\|_\infty \leq 16\sqrt{\frac{2k(k+1)}{N}}. \tag{B.35}$$

Theorem 7 (V is indistinguishable from a Haar-random unitary (Theorem 8 in [28])). *For any k-query oracle adversary $\mathcal{T}$ that can can query $\mathcal{O}, \mathcal{O}^\dagger$,*

$$\left\| \mathop{\mathbb{E}}_{\mathcal{O}\sim\mu_{\mathsf{Haar}}} |\mathcal{T}_k^{\mathcal{O}}\rangle\langle\mathcal{T}_k^{\mathcal{O}}|_{\mathsf{AB}}\,,\ \mathrm{Tr}_{\mathsf{LR}}\left(|\mathcal{T}_k^{V}\rangle\langle\mathcal{T}_k^{V}|_{\mathsf{ABLR}}\right) \right\|_1 \leq \frac{18k(k+1)}{N^{1/8}}. \tag{B.36}$$

Appendix C: Impossibility of random unitaries from constant-local Hamiltonian dynamics

In this section, we provide the proof of Theorems 1 and 2, which show that ensembles generated by time-evolution under any constant-local Hamiltonians for any lengths of time cannot form approximate unitary 2-designs nor PRUs.

Proof of Theorems 1 and 2. Let q denote the maximum locality of a term in any Hamiltonian H in our ensemble, i.e. $q = \max_i w[P_i]$ when we decompose H as a sum of Pauli operators, $H = \sum_i h_i P_i$. We describe a protocol which distinguishes a random constant-local Hamiltonian time evolution from a Haar-random unitary transformation as follows.

First, we select a random stabilizer product state $|u\rangle$ and a random Pauli P_i in H with weight less than q. We then consider the mean square expectation value of P_i when a random product state $|u\rangle$ is time-evolved under e^{-iHt},

$$E_{\mathcal{E}^{(q)}} \equiv \mathop{\mathbb{E}}_{U\sim\mathcal{E}^{(q)}} \mathop{\mathbb{E}}_i \mathop{\mathbb{E}}_u \langle u| e^{iHt} P_i e^{-iHt} |u\rangle^2 \tag{C.1}$$

This is equivalent to computing the expectation value of $P_i \otimes P_i$ on two copies of $e^{-iHt}|u\rangle$. In a unitary 2-design with additive error ε, we must have $E_{\mathcal{E}} \leq 2\varepsilon + \mathcal{O}(1/2^n)$. In a pseudorandom unitary with security against any $\mathrm{poly}(n)$-time adversary, we must have $E_{\mathcal{E}} \leq 1/\omega(\mathrm{poly}\, n)$.

We lower bound $E_{\mathcal{E}}$ above these values as follows. We first apply a standard formula for the twirl over two copies of a random stabilizer product state [99], which yields

$$\mathop{\mathbb{E}}_u \langle u| e^{iHt} P_i e^{-iHt} |u\rangle^2 = \frac{1}{2^n} \mathrm{Tr}\big(e^{iHt} P_i e^{-iHt} \cdot \mathcal{W}(e^{iHt} P_i e^{-iHt})\big), \tag{C.2}$$

where $\mathcal{W}(Q) = (1/3)^{w[Q]}Q$ is a quantum channel that multiplies each Pauli operator Q by a factor that decays exponentially in its weight $w[Q]$. Intuitively, this factor corresponds to the probability that the Pauli operator commutes with a random stabilizer product measurement basis. We therefore obtain the lower bound

$$\frac{1}{2^n} \mathrm{Tr}\big(e^{iHt} P_i e^{-iHt} \cdot \mathcal{W}(e^{iHt} P_i e^{-iHt})\big) \geq (1/3)^q \cdot \frac{1}{2^n} \mathrm{Tr}\big(e^{iHt} P_i e^{-iHt} \cdot \mathcal{P}_{\leq q}(e^{iHt} P_i e^{-iHt})\big), \tag{C.3}$$

where $\mathcal{P}_{\leq q}(Q) = \delta_{w[Q]\leq q} Q$ denotes the superoperator that projects onto Pauli strings of weight less than q. In addition, we further have the lower bound

$$\frac{1}{2^n} \mathrm{Tr}\big(e^{iHt} P_i e^{-iHt} \cdot \mathcal{P}_{\leq q}(e^{iHt} P_i e^{-iHt})\big) \geq \frac{\mathrm{Tr}\big(e^{iHt} P_i e^{-iHt} H\big)^2}{\mathrm{Tr}(H^2)}, \tag{C.4}$$

which follows from applying the superoperator $\mathcal{P}_H(Q) = \mathrm{Tr}(QH)H/\mathrm{tr}(H^2)$, which projects a Pauli string onto its overlap with the Hamiltonian H, onto the first copy of $e^{iHt}P_i e^{-iHt}$, and then using the fact that $\mathrm{Tr}(H\mathcal{P}_{\leq q}(\cdot)) = \mathrm{Tr}(H(\cdot))$ to simplify the resulting trace since each term of H has weight at most q. We now observe that the numerator is time-independent, so that we can simplify it via

$$\frac{\mathrm{Tr}\big(e^{iHt} P_i e^{-iHt} H\big)^2}{\mathrm{Tr}(H^2)} = \frac{\mathrm{Tr}(P_i H)^2}{\mathrm{Tr}(H^2)} = \frac{h_i^2}{\sum_j h_j^2}. \tag{C.5}$$

Taking the expectation over valid Pauli operators P_i with weight less than or equal to q replaces $h_i^2 \to \frac{1}{M_q}\sum_{j:w[P_j]\leq q} h_j^2$, where M_q is the number of such Paulis. In total, this yields

$$\mathop{\mathbb{E}}_{U\sim\mathcal{E}} \mathop{\mathbb{E}}_i \mathop{\mathbb{E}}_u \langle u| e^{iHt} P_i e^{-iHt} |u\rangle^2 \geq (1/3)^q \cdot \frac{1}{M_q}. \tag{C.6}$$

We have $M_q \leq 4^q n$ in one-dimensional systems and $M_q \leq (4n)^q$ in all-to-all connected systems. Hence, we

have $\varepsilon \geq \mathcal{O}(1/(12^q n))$ in one-dimensional systems and $\varepsilon \geq \mathcal{O}(1/(12^q n^q))$ for all-to-all connected systems, which completes our proof for unitary designs. To achieve $\varepsilon = 1/\omega(\mathrm{poly}\, n)$, we require $q = \omega(\log n)$ in one-dimensional systems and $q = \omega(1)$ in all-to-all connected systems, which completes our proof for pseudorandom unitaries. □

Appendix D: Formation of random unitaries from nearly-local Hamiltonian dynamics

In this section, we present the proofs of our main results on the formation of unitary designs and PRUs in nearly-local Hamiltonians. We begin by discussing the non-adaptive setting and presenting the proofs of Theorems 5 and 6 in the main text. We then turn to the adaptive setting and present the proof of Theorems 3 and 4.

1. Proof of Theorems 5 and 6: Indistinguishability in non-adaptive quantum experiments

Our analysis of the non-adaptive setting is organized as follows. We first prove that in any non-adaptive quantum experiment making k queries, a unitary $U^\dagger D U$ where U is Haar-random and D is any unitary operation, is indistinguishable from a Haar-random unitary up to measurable error $\mathcal{O}(k^2|\mathrm{Tr}(D)|^2)$. This allows us to replace $U_{i,i+1}^\dagger (H_i \otimes H_{i+1}) U_{i,i+1}$ for each odd i with a Haar-random unitary on $i, i+1$ in Theorems 5 and 6. We then prove a gluing lemma for conjugated random unitaries with non-adaptive security. Our gluing lemma is strictly weaker than the gluing lemma for adaptive security that we prove in the following section (Appendix D 2), but has the advantage of possessing a more explicit proof. Finally, we introduce an alternative random Hamiltonian time-evolution ensemble for which the proof of non-adaptive security is especially succinct.

a. *Moments of the random Hamiltonian dynamics*

We define a model with a Haar-random eigenbasis which is invariant under any unitary transformation, and represents the dynamics on a connected subsystem. We will then show that in the limit of large system size, the polynomial-order moments of these dynamics are close to those of Haar-random transformations.

Definition 27 (Randomized Hamiltonian dynamics)**.** *Consider a family of Hamiltonians on systems of n qubits which is given by*

$$\mathcal{O}_{\mathsf{inv}} = \{H = U \Lambda U^\dagger \,|\, U \sim \mathsf{Haar},\, \Lambda \sim \mathcal{S}\}, \tag{D.1}$$

where $\mathcal{S}$ is the N-variate spectral distribution of the eigenvalues of $\mathcal{O}_{\mathsf{inv}}$. We then define unitary ensembles given by randomized Hamiltonian dynamics *as those generated by evolving under a Hamiltonian H sampled uniformly from $\mathcal{O}$ for a time distributed according to $t \sim P_H$:*

$$\mathcal{E}_{\mathsf{inv}} = \left\{ e^{-iHt} \,\middle|\, H \sim \mathcal{O}_{\mathsf{inv}}, t \sim P_H \right\}. \tag{D.2}$$

In addition, we denote the distribution of the diagonalization of $\mathcal{E}_{\mathsf{inv}}$ by

$$\mathcal{D} = \left\{ e^{-i\Lambda t} \,\middle|\, \Lambda \sim \mathcal{S}, t \sim P_H \right\}. \tag{D.3}$$

Since the eigenbasis and spectral distribution of the ensemble are independent of one another, we can average over each of them separately. Our strategy for proving the statistical closeness of the dynamics of this ensemble to the Haar moments is to first consider the average over the eigenbasis transformation using the path-recording framework of [28].

It is convenient to introduce a modified version of the path-recording oracle which provides an approximate purification in experiments that only query k copies of a unitary in parallel. This setup is equivalent to an adaptive experiment with input state $|\psi\rangle$ on registers $(\otimes_i^k \mathsf{A}_i) \otimes \mathsf{B}$, in which each step consists of applying U to A_i, then applying a postprocessing step T which is simply the permutation operator which shifts the A_i registers by one.

Definition 28 (Parallel path-recording oracle)**.** *The k-query* parallel *path recording oracle $V^{(k)}$ is defined via its left and right components*

$$\begin{aligned} V_L^{(k)} \cdot \left[\bigotimes_{i=1}^{k} |x_i\rangle\right] |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} &= \sum_{\substack{\mathbf{y}\in[N]^k_{\mathrm{dist}}:\\ y_i\notin \mathrm{Im}(L\cup R)}} \frac{1}{Z_L} |y\rangle_{\mathsf{A}} |L\cup\{(x,y_i)\}_i\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}}, \\ V_R^{(k)} \cdot \left[\bigotimes_{i=1}^{k} |y_i\rangle\right] |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} &= \sum_{\substack{\mathbf{x}\in[N]^k_{\mathrm{dist}}:\\ x_i\notin \mathrm{Dom}(L\cup R)}} \frac{1}{Z_R} |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\cup\{(x_i,y)\}_i\rangle_{\mathsf{R}}, \end{aligned} \tag{D.4}$$

where the normalization factors Z_L, Z_R are given by

$$\begin{aligned} Z_L &= \frac{1}{\sqrt{(N-|\mathrm{Im}(L\cup R)|)(N-|\mathrm{Im}(L\cup R)|-1)\cdots(N-|\mathrm{Im}(L\cup R)|-k+1)}}, \\ Z_R &= \frac{1}{\sqrt{(N-|\mathrm{Dom}(L\cup R)|)(N-|\mathrm{Dom}(L\cup R)|-1)\cdots(N-|\mathrm{Dom}(L\cup R)|-k+1)}}. \end{aligned} \tag{D.5}$$

Definition 29 (Parallel partial path-recording oracle)**.** *Similar to the adaptive case, the k-query* parallel *partial path-recording oracle $W^{(k)}$ is defined via an additional restriction on the domain of the left and right components:*

$$\begin{aligned} W_L^{(k)} &= V_L^{(k)} \cdot \prod_{i=1}^{k} \Pi^{\mathrm{Dom}(W_{L_i})}, \\ W_R^{(k)} &= V_R^{(k)} \cdot \prod_{i=1}^{k} \Pi^{\mathrm{Dom}(W_{R_i})}, \end{aligned} \tag{D.6}$$

where W_{R_i} denotes the partial path-recording oracle applied to the i-th copy of the system, and the projectors act on the shared path-recording register as well as the i-th copy of the physical system.

In the remainder of this section, we use "path-recording oracle" to refer to the parallel version, unless otherwise specified. In addition, we will use the following property to simplify our analysis:

Lemma 9 ($\widetilde{W}^{(k)}$ is indistinguishable from a Haar-random unitary)**.** *Let $\mathfrak{C}$ be any exact unitary 2-design. For any k-query oracle adversary $\mathcal{T}$ that can query $\mathcal{O}, \mathcal{O}^\dagger$,*

$$\left\| \mathop{\mathbb{E}}_{\mathcal{O}\sim\mathsf{Haar}} |\mathcal{T}_k^{\mathcal{O}}\rangle\langle\mathcal{T}_k^{\mathcal{O}}|_{\mathsf{AB}} - \mathrm{Tr}_{\mathsf{LRCD}}\, |\mathcal{T}_k^{W,\mathfrak{C}}\rangle\langle\mathcal{T}_k^{W,\mathfrak{C}}|_{\mathsf{ABLRCD}} \right\|_1 \leq \frac{36k(k+1)}{N^{1/8}}. \tag{D.7}$$

Proof. This follows from Lemma 7 and Theorem 7 via an application of the triangle inequality. □

We can therefore substitute all instances of the random eigenbasis transformation with applications of $W^{(k)}$, sandwiched by C, C' which are drawn from an exact 2-design, to obtain an approximate purification of the moment. We proceed to the main technical result of this section, which is bounding the statistical distance between this purification and the output of $\widetilde{V}^{(k)}$, i.e. the action of $V^{(k)}$ after conjugating by some C drawn from a 2-design.

Proposition 2 (Statistics of random eigenbasis dynamics are close to $\widetilde{V}^{(k)}$)**.** *Suppose D is sampled from an arbitrary distribution $\mathcal{D}$. For any k and input state $|\psi\rangle$ on $nk+m$ qubits, the trace distance between the twirl over the random eigenbasis Hamiltonian dynamics and the action of $\widetilde{V}^{(k)}$ is bounded by*

$$\left\| \mathop{\mathbb{E}}_{U\sim\mathcal{E}_{\mathsf{inv}}} \left[(U)^{\otimes k} |\psi\rangle\langle\psi| \left(U^\dagger\right)^{\otimes k} \right] - \mathrm{Tr}_{\mathsf{L}} |\mathcal{T}_k^{\widetilde{V}}\rangle\langle\mathcal{T}_k^{\widetilde{V}}| \right\|_1 \leq \frac{144k(k+1)}{N^{1/8}} + \frac{12k^2}{N} + \mathop{\mathbb{E}}_{D\sim\mathcal{D}} \left[\frac{8k^2}{2^{2n}} |\mathrm{Tr}\, D|^2 \right], \tag{D.8}$$

up to subleading corrections $O(k^2/N^2)$.

Proof. We first apply Lemma 9 to explicitly compute an approximate purification of the average over

the random eigenbasis transformation. For any instance of D, we obtain a state of the form

$$|\mathcal{T}_k^{\mathsf{inv}}\rangle = \frac{1}{Z}\mathop{\mathbb{E}}_{C}\left[C^{\otimes k}W^{(k)}\sum_{\mathbf{x},\mathbf{y}\in[N]^k_{\mathrm{dist}}}|\varnothing\rangle_{\mathsf{L}}\,|\{(x_i,y_i)\}_{i\in[k]}\rangle_{\mathsf{R}}\left[\bigotimes_{j=1}^{k}\widetilde{D}\,|x_j\rangle\langle y_j|\right](C^\dagger)^{\otimes k}\right]|\psi\rangle\,, \tag{D.9}$$

where $\widetilde{D}$ is the twirl of $C'D(C')^\dagger$ over C', Z is the normalization factor $(N!/(N-k)!)^{-1/2}$, and we have expanded the action of the inverse direction $(W^{(k)})^\dagger$ acting in the inverse direction. Since this includes a total of $2k$ copies of U or $U^\dagger$, we incur an error which is upper bounded by

$$\left\|\mathrm{Tr}_{\mathsf{LR}}\,|\mathcal{T}_k^{\mathsf{inv}}\rangle\langle\mathcal{T}_k^{\mathsf{inv}}| - \mathop{\mathbb{E}}_{U\sim\mathsf{Haar}}\left[\left(UDU^\dagger\right)^{\otimes k}|\psi\rangle\langle\psi|\left(UD^\dagger U^\dagger\right)^{\otimes k}\right]\right\|_1 \leq \frac{144k(k+1)}{2^{n/8}}. \tag{D.10}$$

Rather than constructing a purification and change of basis corresponding to the twirl over C, C', we directly impose a restriction on the support of $|\mathcal{T}_k^{\mathsf{inv}}\rangle$. In particular, we insert the projector

$$\Pi^{\notin\mathrm{Im}(W^R)} = \mathbb{1} - \Pi^{\mathrm{Im}(W^R)} \tag{D.11}$$

before the action of $W^{(k)}$ to obtain

$$|\widetilde{\mathcal{T}_k^{\mathsf{inv}}}\rangle = \mathop{\mathbb{E}}_{C}\left[C^{\otimes k}W^{(k)}\Pi^{\notin\mathrm{Im}(W^R)}\widetilde{D}(W^\dagger)^{(k)}(C^\dagger)^{\otimes k}\right]|\psi\rangle\,. \tag{D.12}$$

The error from applying this restriction is given by

$$\left\|\mathrm{Tr}_{\mathsf{LR}}\,|\mathcal{T}_k^{\mathsf{inv}}\rangle\langle\mathcal{T}_k^{\mathsf{inv}}| - \mathrm{Tr}_{\mathsf{LR}}\,|\widetilde{\mathcal{T}_k^{\mathsf{inv}}}\rangle\langle\widetilde{\mathcal{T}_k^{\mathsf{inv}}}|\right\|_1 \leq 2\left\|\mathop{\mathbb{E}}_{C}\left[C^{\otimes k}W^{(k)}\Pi^{\mathrm{Im}(W^R)}\widetilde{D}(W^\dagger)^{(k)}(C^\dagger)^{\otimes k}\right]|\psi\rangle\right\|_2, \tag{D.13}$$

where we have used the property that the trace distance is monotonic under quantum operations, in addition to Fact 4. The expression on the RHS is upper bounded by summing over all overlap terms in the computational basis from the k applications of the partial path-recording oracle corresponding to the forward direction, and the k in the inverse direction with a coincidence of the form $\langle x|\widetilde{D}|x\rangle$, which enables us to derive a condition in terms of D:

$$\begin{aligned}
\frac{1}{2}\,\mathrm{RHS} &\leq \sum_{i,i'\in[k]}\left|\left\langle\Pi_{i,i'}^{\mathrm{eq}}\right\rangle\right|^2 = \left|\mathop{\mathbb{E}}_{C}\left[C^{\otimes k}W^{(k)}\left[\sum_{i,i'\in[k]}\Pi_{i,i'}^{\mathrm{eq}}\right]\widetilde{D}(W^\dagger)^{(k)}(C^\dagger)^{\otimes k}\right]|\psi\rangle\right|^2 \\
&\leq \frac{1}{2^n}\sum_{i,i'\in[k]}\sum_{x_i,x_{i'}\in[N]}\left|\langle x_{i'}|\widetilde{D}|x_i\rangle\right|^2\delta(x_i,x_{i'}) \\
&\leq \frac{k^2}{2^n}\sum_{x\in[N]}\langle xx|\mathop{\mathbb{E}}_{C'}\left[(C')^{\otimes 2}(D\otimes D^\dagger)(C'^\dagger)^{\otimes 2}\right]|xx\rangle \\
&\leq \frac{k^2}{2^n}\sum_{x\in[N]}\frac{1}{2^{2n}-1}\left[|\mathrm{Tr}\,D|^2 + \mathrm{Tr}\,|D|^2 - \frac{1}{2^n}\,\mathrm{Tr}\,|D|^2 - \frac{1}{2^n}|\mathrm{Tr}\,D|^2\right] \\
&\leq \frac{2k^2}{2^{2n}}|\mathrm{Tr}\,D|^2 + \frac{2k^2}{2^n},
\end{aligned} \tag{D.14}$$

where in the last step we have used the fact that $\mathrm{Tr}\,|D|^2 = 2^n$. Plugging this back into Equation D.13 yields

$$\left\|\mathrm{Tr}_{\mathsf{LR}}\,|\mathcal{T}_k^{\mathsf{inv}}\rangle\langle\mathcal{T}_k^{\mathsf{inv}}| - \mathrm{Tr}_{\mathsf{LR}}\,|\widetilde{\mathcal{T}_k^{\mathsf{inv}}}\rangle\langle\widetilde{\mathcal{T}_k^{\mathsf{inv}}}|\right\|_1 \leq \frac{4k^2}{2^{2n}}|\mathrm{Tr}\,D|^2 + \frac{4k^2}{2^n}. \tag{D.15}$$

Expanding the action of the W^k corresponding to the forward direction in $|\widetilde{\mathcal{T}_k^{\mathsf{inv}}}\rangle$ yields

$$\frac{1}{Z'}\sum_{(L,R)\in\mathcal{R}^2_{\mathrm{dist}}}|\{(x'_{i'},y'_{i'})\}_{i'\in[k]}\rangle_{\mathsf{L}}\,|\{(x_i,y_i)\}_{i\in[k]}\rangle_{\mathsf{R}}\bigotimes_{j=1}^{k}\langle x'_j|\,\widetilde{D}\,|x_j\rangle\cdot\mathop{\mathbb{E}}_{C}\left[C\,|y'_j\rangle\langle y_j|\,C^\dagger\right]|\psi\rangle\,, \tag{D.16}$$

where we have included the normalization factor $Z' = (N!/(N-2k)!)^{-1/2}$. In addition, we have that

$$|\mathcal{T}_k^{\widetilde{V}}\rangle = \frac{1}{Z} \sum_{\mathbf{y}' \in [N]^k_{\text{dist}}} |\{(y_i', y_i)\}_{i\in[k]}\rangle_{\mathsf{L}} \, |\varnothing\rangle_{\mathsf{R}} \bigotimes_{j=1}^{k} \mathop{\mathbb{E}}_{C} \left[C \left|y_j'\right\rangle\!\left\langle y_j\right| C^\dagger\right] |\psi\rangle \,. \tag{D.17}$$

Computing the partial trace over the relation state registers and expanding up to leading order yields that the outputs of the two are indistinguishable up to

$$\left\| \mathrm{Tr}_{\mathsf{LR}} |\mathcal{T}_k^{\widetilde{\mathsf{inv}}}\rangle\langle\mathcal{T}_k^{\widetilde{\mathsf{inv}}}| - \mathrm{Tr}_{\mathsf{L}} |\mathcal{T}_k^{\widetilde{V}}\rangle\langle\mathcal{T}_k^{\widetilde{V}}| \right\|_1 \leq 2\left[\left(\frac{2k^2}{2^{2n}}|\mathrm{Tr}\, D|^2 + \frac{2k^2}{2^n}\right) + \left(\frac{2k^2}{2^n}\right)\right] + O\left(\frac{k^2}{2^{2n}}\right), \tag{D.18}$$

where we have again applied the triangle inequality to to bound the contributions to the norm from the $\left|\langle x_i'|\widetilde{D}|x_i\rangle\right|^2$ and $\left|\mathbb{E}_C \left[C \left|y_j'\right\rangle\!\left\langle y_j\right| C^\dagger\right] |\psi\rangle\right|^2$ terms. Finally, applying triangle inequality to Equations D.10, D.15, D.18 gives

$$\begin{aligned}
&\left\| \mathop{\mathbb{E}}_{D\sim\mathcal{D}} \mathop{\mathbb{E}}_{U\sim\mathsf{Haar}} \left[\left(UDU^\dagger\right)^{\otimes k} |\psi\rangle\langle\psi| \left(UD^\dagger U^\dagger\right)^{\otimes k}\right] - \mathrm{Tr}_{\mathsf{L}} |\mathcal{T}_k^{\widetilde{V}}\rangle\langle\mathcal{T}_k^{\widetilde{V}}| \right\|_1 \\
&\quad \leq \frac{144k(k+1)}{2^{n/8}} + \mathop{\mathbb{E}}_{D\sim\mathcal{D}} \left[\frac{8k^2}{2^{2n}}|\mathrm{Tr}\, D|^2 + \frac{12k^2}{2^n} + O\left(\frac{k^2}{N^2}\right)\right] \\
&\quad = \frac{144k(k+1)}{N^{1/8}} + \frac{12k^2}{N} + \mathop{\mathbb{E}}_{D\sim\mathcal{D}} \left[\frac{8k^2}{2^{2n}}|\mathrm{Tr}\, D|^2\right] + O\left(\frac{k^2}{N^2}\right),
\end{aligned} \tag{D.19}$$

which yields the stated bound up to leading order in k/N. □

b. Gluing argument for nearly-local dynamics

In order to prove Theorems 5 and 6, we now present a gluing-style argument for neighboring patches of the form given in Definition 27. It is convenient to introduce a new isometry which *expands* relation states of a given length, when restricted to a particular subspace.

Definition 30 (Expansion map)**.** *We construct a map which acts nontrivially on relation states in a single register* L *of length* k *whose output is distinct on* $S_1 \cup S_2$*, so that* $|\mathrm{Im}_{S_1\cup S_2}(\mathsf{L})| = k$ *for disjoint physical subsystems* S_1, S_2 *of size* ξ *each.*

On this subspace, the map "expands" the original relation state into superpositions over relation states on two intermediate registers which correspond to non-overlapping regions $S_1' \supseteq S_1, S_2' \supseteq S_2$*, sandwiched by a pair of relation states* $\mathsf{L}_0, \mathsf{R}_0$ *corresponding to the original physical system:*

$$\begin{aligned}
\mathsf{Expand}^k_{\mathsf{L}\to\mathsf{L}_0\mathsf{R}_0\mathsf{L}_1\mathsf{L}_2} = \sum_{\mathbf{w^1},\mathbf{w^2},\mathbf{z^1},\mathbf{z^2}\in[2^\xi]^k_{\text{dist}}} \frac{1}{Z} \Big[&|\{(x_i^1 x_i^2, w_i^1 w_i^2)\}_{i\in[k]}\rangle_{\mathsf{L}_0} |\{(z_i^1 z_i^2, y_i^1 y_i^2)\}_{i\in[k]}\rangle_{\mathsf{R}_0} \\
&|\{(w_i^1 x_i^{\overline{1}}, z_i^1 y_i^{\overline{1}})\}_{i\in[k]}\rangle_{\mathsf{L}_1} |\{(w_i^2 x_i^{\overline{2}}, z_i^2 y_i^{\overline{2}})\}_{i\in[k]}\rangle_{\mathsf{L}_2}\Big] \\
&\cdot \langle\{(x_i, y_i)\}_{i\in[k]}|_{\mathsf{L}} \cdot \Pi^{\text{dist}}_{S_1S_2},
\end{aligned} \tag{D.20}$$

where Z *is the normalization factor* $\left[(2^\xi)!/(2^\xi - k)!\right]^{-2}$*, and we have used the shorthand* x_i^1 *to denote the substring of* x *on* S_1*. This map acts as an isometry on the image of* $\Pi^{\text{dist}}_{S_1S_2}$*.*

We now present the formal statement of our bound for the "glued" dynamics:

Lemma 10 (Gluing through conjugation)**.** *Consider the ensemble*

$$\mathcal{E}' = \{U_{AA'}(U_{A\overline{A}} \otimes U_{A'\overline{A'}})U_{AA'}^\dagger\}, \tag{D.21}$$

where $U_{A\overline{A}}, U_{A'\overline{A'}}$ *are drawn from from* ϵ_A*- and* $\epsilon_{A'}$*-approximate* k*-designs, respectively, on the regions* $A\overline{A}$ *and* $A'\overline{A'}$*, and* $U_{AA'}$ *is a Haar-random transformation on the overlapping region* AA'*. In addition, suppose that* A *and* A' *consist of* ξ *qubits each. Then* $\mathcal{E}'$ *is an approximate* k*-design up to additive error*

$$\|\Phi_{\mathcal{E}'} - \Phi_H\|_\diamond \leq \varepsilon_A + \varepsilon_{A'} + \frac{108k(k+1)}{2^{\xi/8}} + \frac{18k(k+1)}{2^{\xi/4}} + \frac{2k\sqrt{2}}{2^{\xi/2}} + \frac{k\sqrt{2}}{2^\xi}. \tag{D.22}$$

Proof. Consider the ensemble given by

$$\mathcal{E}'_0 = \{ U_{AA'}(U_{A\overline{A}} \otimes U_{A'\overline{A'}})U^\dagger_{AA'} \;\Big|\; U_{A\overline{A}}, U_{A'\overline{A'}} \sim \mathsf{Haar}\}, \tag{D.23}$$

where the unitaries $U_{A\overline{A}}, U_{A'\overline{A'}}$ are still conjugated by a random overlapping unitary, but we have instead drawn them from the Haar measure on $A\overline{A}$ and $A'\overline{A'}$ rather than from an approximate k-design. By assumption, we have that

$$\left\|\Phi_{\mathcal{E}'} - \Phi_{\mathcal{E}'_0}\right\|_\diamond \leq \varepsilon_A + \varepsilon_{A'}. \tag{D.24}$$

We now apply Theorem 7 in order to construct an approximate purification of the moments of $\mathcal{E}'_0$. For any input state $|\psi\rangle$ on $nk+m$ qubits, the output is approximated by tracing over the relation state registers of

$$|\mathcal{T}_k^{\mathsf{conj}}\rangle = V^{(k)}_{AA'} \left(V_{A\overline{A}} \otimes V_{A'\overline{A'}}\right)^{(k)} \left(V^\dagger_{AA'}\right)^{(k)} |\psi\rangle\,, \tag{D.25}$$

where we have instantiated multiple path-recording oracles V_S with separate relation state registers corresponding to subsystem S. We obtain an exponentially small error in trace distance:

$$\left\| \mathrm{Tr}_{\mathsf{L}_{A\overline{A}}\mathsf{L}_{A'\overline{A'}}\mathsf{L}_{\overline{A}\overline{A'}}\mathsf{R}_{\overline{A}\overline{A'}}} |\mathcal{T}_k^{\mathsf{conj}}\rangle\langle\mathcal{T}_k^{\mathsf{conj}}| - \mathop{\mathbb{E}}_{U\sim\mathcal{E}'_0} U^{\otimes k} |\psi\rangle\langle\psi| \left(U^\dagger\right)^{\otimes k} \right\|_1 \leq \frac{108k(k+1)}{2^{\xi/8}}. \tag{D.26}$$

We will consider an intermediate comparison to the approximate purification of the Haar moment $|\mathcal{T}_k^V\rangle$. To do so, we examine the restriction of $|\mathcal{T}_k^{\mathsf{conj}}\rangle$ to a particular subspace for which we can construct a partial isometry mapping to the image of $V^{(k)}$. In particular, we insert a *doubly* distinct projection before and after the applications of $V_{A\overline{A}} \otimes V_{A\overline{A'}}$:

$$|\widetilde{\mathcal{T}_k^{\mathsf{conj}}}\rangle = V^{(k)}_{AA'} \left[\Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left(V_{A\overline{A}} \otimes V_{A'\overline{A'}}\right)^{(k)} \left[\Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left(V^\dagger_{AA'}\right)^{(k)} |\psi\rangle\,, \tag{D.27}$$

Since these projectors are all diagonal in the computational basis, it is clear that the support of $|\widetilde{\mathcal{T}_k^{\mathsf{conj}}}\rangle$ is contained in the support of $|\mathcal{T}_k^{\mathsf{conj}}\rangle$. The error incurred by enforcing this restriction is therefore given by the magnitude of the remaining portion not contained in the support of $|\widetilde{\mathcal{T}_k^{\mathsf{conj}}}\rangle$.

$$\begin{aligned}
&\left\| \mathrm{Tr}_{\mathsf{L}_{A\overline{A}}\mathsf{L}_{A'\overline{A'}}\mathsf{L}_{\overline{A}\overline{A'}}\mathsf{R}_{\overline{A}\overline{A'}}} |\mathcal{T}_k^{\mathsf{conj}}\rangle\langle\mathcal{T}_k^{\mathsf{conj}}| - \mathrm{Tr}_{\mathsf{L}_{A\overline{A}}\mathsf{L}_{A'\overline{A'}}\mathsf{L}_{\overline{A}\overline{A'}}\mathsf{R}_{\overline{A}\overline{A'}}} |\widetilde{\mathcal{T}_k^{\mathsf{conj}}}\rangle\langle\widetilde{\mathcal{T}_k^{\mathsf{conj}}}| \right\|_1 \\
\leq &\left\| V^{(k)}_{AA'} \left[\mathbb{1} - \Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left(V_{A\overline{A}} \otimes V_{A'\overline{A'}}\right)^{(k)} \left[\Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left(V^\dagger_{AA'}\right)^{(k)} |\psi\rangle \right\|_2 \\
&+ \left\| V^{(k)}_{AA'} \left[\Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left(V_{A\overline{A}} \otimes V_{A'\overline{A'}}\right)^{(k)} \left[\mathbb{1} - \Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left(V^\dagger_{AA'}\right)^{(k)} |\psi\rangle \right\|_2 \\
= &\left\| V^{(k)}_{AA'} \left[\mathbb{1} - \Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left[\Pi^{\mathrm{dist}}_{A\overline{A}} \otimes \Pi^{\mathrm{dist}}_{A'\overline{A'}}\right] \left(V_{A\overline{A}} \otimes V_{A'\overline{A'}}\right)^{(k)} \left[\Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left(V^\dagger_{AA'}\right)^{(k)} |\psi\rangle \right\|_2 \\
&+ \left\| V^{(k)}_{AA'} \left[\Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\right] \left(V_{A\overline{A}} \otimes V_{A'\overline{A'}}\right)^{(k)} \left[\mathbb{1} - \Pi^{\mathrm{dist}}_A \otimes \Pi^{\mathrm{dist}}_{A'}\Pi^{\mathrm{dist}}_{AA'}\right] \left(V^\dagger_{AA'}\right)^{(k)} |\psi\rangle \right\|_2 \leq \frac{2k\sqrt{2}}{2^{\xi/2}},
\end{aligned} \tag{D.28}$$

where in the second step we have used the fact that the output of each $V_S^{(k)}$ corresponding to the physical subsystem S is distinct on S, then applied a standard counting argument for the portion of the distinct subspace which is contained on a local distinct subspace as given in Definition 3. In addition, we consider the corresponding restriction $\Pi^{\mathrm{dist}}_{AA'}$ on the output of $V^{(k)}_{A\overline{A}A'\overline{A'}}$, and similarly bound its distance from the full output of $|\mathcal{T}_k^V\rangle$:

$$\left\|\mathrm{Tr}_{\mathsf{L}} |\mathcal{T}_k^V\rangle\langle\mathcal{T}_k^V| - \mathrm{Tr}_{\mathsf{L}} \left[\Pi^{\mathrm{dist}}_{AA'} |\mathcal{T}_k^V\rangle\langle\mathcal{T}_k^V|\right]\right\|_1 \leq \frac{k\sqrt{2}}{2^\xi}. \tag{D.29}$$

By inspection, we have that the Expand isometry maps the restriction $\Pi^{\mathrm{dist}}_{AA'} |\mathcal{T}_k^V\rangle$ to the output of $|\widetilde{\mathcal{T}_k^{\mathsf{conj}}}\rangle$:

$$\mathsf{Expand}^k_{\mathsf{L}\to\mathsf{L}_{A\overline{A}}\mathsf{L}_{A'\overline{A'}}\mathsf{L}_{\overline{A}\overline{A'}}\mathsf{R}_{\overline{A}\overline{A'}}} \left[\Pi^{\mathrm{dist}}_{AA'} |\mathcal{T}_k^V\rangle\langle\mathcal{T}_k^V|\right] = |\widetilde{\mathcal{T}_k^{\mathsf{conj}}}\rangle\,. \tag{D.30}$$

Since this map is isometric and acts as a change of basis on the relation state registers, we have

$$\mathrm{Tr}_{\mathsf{L}}\left[\Pi^{\mathrm{dist}}_{AA'}\left|\mathcal{T}^V_k\right\rangle\right] = \mathrm{Tr}_{\mathsf{L}_{A\overline{A}}\mathsf{L}_{A'\overline{A'}}\mathsf{L}_{\overline{A}\overline{A'}}\mathsf{R}_{\overline{A}\overline{A'}}}\left|\widetilde{\mathcal{T}^{\mathsf{conj}}_k}\right\rangle\!\left\langle\widetilde{\mathcal{T}^{\mathsf{conj}}_k}\right| . \tag{D.31}$$

Finally, we apply Theorem 7 to obtain

$$\left\|\mathrm{Tr}_{\mathsf{L}}\left|\mathcal{T}^V_k\right\rangle\!\left\langle\mathcal{T}^V_k\right| - \mathop{\mathbb{E}}_{U\sim\mathsf{Haar}} U^{\otimes k}\left|\psi\right\rangle\!\left\langle\psi\right|(U^\dagger)^{\otimes k}\right\|_1 \leq \frac{18k(k+1)}{2^{\xi/4}}. \tag{D.32}$$

We complete the proof by applying the triangle inequality to the results of Equations D.24, D.26, D.28, D.31, D.29, and D.32, which yields the stated bound. □

We now restate the main results of this section, which states that the moments of the nearly-local dynamics are close to those of the Haar ensemble, up to any polynomial order.

Theorem 8 (Theorem 5 in main text)**.** *Suppose H is drawn from a variant of the random two-layer Hamiltonian ensemble in Theorem 3 in which each random diagonal term, $\sum_z J^i_z \left|z\right\rangle\!\left\langle z\right|_i$, is replaced with any fixed Hamiltonian H_i. The resulting time-evolution $U = e^{-iHt}$ forms an additive-error ε-approximate unitary k-design for any H_i and any time t such that $|\mathrm{Tr}\big(e^{-iH_i t}\big)|^2 = o(\varepsilon/nk^2)$ for all i.*

Theorem 9 (Theorem 6 in main text)**.** *Suppose H is drawn from a variant of the random two-layer Hamiltonian ensemble in Theorem 3 in which $\sum_z J^i_z \left|z\right\rangle\!\left\langle z\right|_i$ is replaced with any fixed Hamiltonian H_i. The resulting time-evolution $U = e^{-iHt}$ forms a PRU with non-adaptive security for any H_i and any time t such that $|\mathrm{Tr}\big(e^{-iH_i t}\big)|^2 = o(1/\operatorname{poly} n)$ for all i.*

Proof of Theorems 8 and 9. We first observe that H_i admits a fixed diagonalization $H_i = U_0 D_0 U_0^\dagger$. By assumption, the Hamiltonian ensemble is invariant under change of basis on each patch. Both statements then follow immediately from substituting the result of Proposition 2 into each patch for the ensemble of interest, then applying the result of Lemma 10 to each instance of conjugation by overlapping unitaries, up to n/ξ. Setting $\xi = \operatorname{poly}\log(n)$ yields the stated result. □

c. *Designs via local spectral distribution*

While our bound above holds for D sampled from arbitrary spectral distributions, we are often interested in systems whose distributions have particular properties, such as being generated by an extensive number of local degrees of freedom. We remark that it is possible to obtain superpolynomial-order designs up to superpolynomially small order even for distributions that are generated by single-qubit operators.

Fact 8. *Suppose D is sampled from a distribution which is constructed by taking a product of an extensive number of i.i.d. local random phases $D_i \sim \mathcal{D}_0$. Then*

$$\mathop{\mathbb{E}}_{D\sim\mathcal{D}}\left[|\mathrm{Tr}\, D|^2\right] = \left(\mathop{\mathbb{E}}_{D'\sim\mathcal{D}_0}|\mathrm{Tr}\, D'|^2\right)^{n/n_0}, \tag{D.33}$$

where n_0 is the size of the physical subsystem corresponding to $\mathcal{D}_0$.

In particular, this implies that the bound of Proposition 2 is exponentially small in n for models in which the energy spectrum is generated by single-qubit operators with eigenvalues E_0 and E_1, and the evolution time is concentrated around

$$t_0 = \pi\hbar/\Delta E = \pi\hbar/|E_0 - E_1|. \tag{D.34}$$

Corollary 1 (Statistics of random eigenbasis dynamics are close to Haar-random)**.** *For any $k = 2^{o(n)}$, the random eigenbasis Hamiltonian dynamics with phases generated by single-qubit operators with constant energy gap ΔE forms an approximate k-design at constant time scales $t \sim G(t_0, t_0/8)$, up to additive error*

$$\left\|\Phi_{\mathcal{E}_{\mathsf{inv}}} - \Phi_H\right\|_\diamond \leq \frac{162k(k+1)}{N^{1/8}} + \frac{12k^2}{N} + \frac{8k^2}{c^n} + O\left(\frac{k^2}{N^2}\right), \tag{D.35}$$

where t_0 is given by Equation D.34, $G(\mu, \sigma)$ denotes the normal distribution, and c is a positive constant greater than one.

Proof. We bound the trace moments via Fact 8

$$\mathop{\mathbb{E}}_{D\sim\mathcal{D}}\left[|\mathrm{Tr}\, D|^2\right] = \left[\int_0^{2\pi} d\theta \left[(\cos(x)+1)^2 + \sin^2(\theta)\right]\left[\frac{1}{\sqrt{2\pi(\pi/8)^2}} e^{-(\theta-\pi)^2/2(\pi/8)^2}\right]\right]^n < 1. \tag{D.36}$$

The result then follows immediately from an application of the triangle inequality to the statements of Proposition 2 and Theorem 7, and using the fact that V satisfies an approximate two-sided unitary invariance property, as described in Claim 8. □

Proposition 3 (Statistics of nearly-local dynamics with local spectrum are close to Haar-random)**.** *When $\mathcal{D}$ is generated by single-qubit operators with constant energy gap ΔE and the time scale is taken to be $t \sim G(t_0, t_0/8)$, the ensemble of nearly-local Hamiltonians is an approximate k-design up to additive error*

$$\epsilon = \frac{270nk(k+1)}{2^{\xi/8}\xi} + \frac{8nk^2}{c^\xi \xi} + O\left(\frac{k^2}{2^{\xi/4}\xi}\right), \tag{D.37}$$

where c is a positive constant greater than one, and we have left out subleading terms in $k/2^\xi$. In particular, when $\xi = O(\mathrm{poly}\log n)$, this ensemble forms an approximate design for all $k = \mathrm{poly}(n)$.

Proof. This follows from substituting the result of Corollary 1 into each patch for the ensemble of interest, then applying the result of Lemma 10 to each instance of conjugation by overlapping unitaries, up to n/ξ. Setting $\xi = \mathrm{poly}\log(n)$ yields the stated result. □

d. A simple alternative construction and proof

We conclude our discussion of the non-adaptive setting by introducing an alternative random Hamiltonian time-evolution ensemble and providing an especially short proof of its indistinguishability from Haar-random in any non-adaptive quantum experiment. We consider the random unitary ensemble,

$$\mathcal{E}_{\mathbf{F}} = \left(\otimes_{i\in\mathrm{even}} U_{i,i+1}\right)^\dagger \cdot \left(\otimes_{i\in\mathrm{odd}} F_{i,i+1}\right) \cdot \left(\otimes_{i\in\mathrm{even}} U_{i,i+1}\right), \tag{D.38}$$

where each $U_{i,i+1}$ is a strong PRU on $2\xi = \omega(\log n)$ qubits with security against any poly n-time quantum adversary, and each $F_{i,i+1}$ is a PRF on $2\xi = \omega(\log n)$ qubits with security against any poly n-time quantum adversary. While the ensemble of Hamiltonians and evolution time scale is not made explicit in the definition of $\mathcal{E}_{\mathbf{F}}$, for any distribution over evolution time which can be efficiently specified, it is also possible to extract the corresponding ensemble of Hamiltonians. Moreover, fixing the time scale to be concentrated around some constant $t_0 = O(1)$ yields a well-defined ensemble of Hamiltonians whose time dynamics can be efficiently computed at any time scale.

We remark that in this ensemble, the basis transformation is itself non-entangling across several cuts of the system. However, it is still possible to obtain approximate designs up to superpolynomial order and error due to the action of the pseudorandom phases:

Theorem 10. *The time evolution of the ensemble of Hamiltonians described via $\mathcal{E}_{\mathbf{F}}$ with non-entangling basis transformations and spectral distribution which generates pseudorandom phases on nearly-local patches forms an approximate k-design up to additive error*

$$\epsilon = \frac{36nk(k+1)}{2^{\xi/8}\xi} + \frac{4nk}{2^{\xi/2}\xi} + O\left(\frac{k^2}{N^{1/8}}\right). \tag{D.39}$$

Proof. Consider any input state $|\psi\rangle$ over $nk+m$ qubits. For simplicity, we will assume that $n = n'\xi$, where $\xi = \omega(\log n)$. Recall the path-recording oracle V_i for simulating Haar-random unitaries U_i under both forward and inverse queries and the purification $O_{F_{i,i+1}}$ of Haar-random diagonal unitaries $F_{i,i+1}$ as in [28]. As with the construction of $V^{(k)}$ given in Definition 28, we can consider a parallel version of the random phase oracle $O^{(k)}_{F_{i,i+1}}$ which acts equivalently to the original oracle in a restricted experiment

where each of the k queries do not use any adaptive postprocessing on the previous queries. We define the following pure states:

$$|\mathcal{T}_k^{\mathbf{VFV}^\dagger}\rangle = \left[\bigotimes_{i=1}^{n'} V_i^{(k)} \bigotimes_{i\in\text{even}} O_{F_{i,i+1}}^{(k)} \bigotimes_{i\in\text{odd}} O_{F_{i,i+1}}^{(k)} \bigotimes_{i=1}^{n'} (V_i^\dagger)^{(k)}\right] |\psi\rangle_{\mathsf{A}} |\varnothing^{n'}\rangle_{\mathsf{L}} |\varnothing^{n'}\rangle_{\mathsf{R}} |0^{n'}\rangle_{\mathsf{E}}, \tag{D.40}$$

$$|\mathcal{T}_k^{VFV^\dagger}\rangle = \left[V^{(k)} O_F^{(k)} (V^\dagger)^{(k)}\right] |\psi\rangle_{\mathsf{A}} |\varnothing^{n'}\rangle_{\mathsf{L}} |\varnothing^{n'}\rangle_{\mathsf{R}} |0^{n'}\rangle_{\mathsf{E}}. \tag{D.41}$$

Applying Theorem 7 to each patch and using triangle inequality yields

$$\left\| \mathop{\mathbb{E}}_{U\sim\mathcal{E}_{\mathbf{F}}} \left[U^{\otimes k} |\psi\rangle\langle\psi| (U^\dagger)^{\otimes k}\right] - \text{Tr}_{\mathsf{LRE}} |\mathcal{T}_k^{\mathbf{VFV}^\dagger}\rangle\langle\mathcal{T}_k^{\mathbf{VFV}^\dagger}| \right\|_1 \leq \frac{36nk(k+1)}{2^{\xi/8}\xi}. \tag{D.42}$$

Substituting in the definitions of V_i and $O^{F_{i,i+1}}$ from [28], then using a similar argument as [19] enables us to compare $|\mathcal{T}_k^{\mathbf{VFV}^\dagger}\rangle$ to an ensemble constructed via random unitary and phase transformations on the entire system. In particular, we observe that the action of the $\otimes_{i\in[n']} V_i^{(k)}$ and $\otimes_{i\in\text{even}} O_{F_{i,i+1}}^{(k)} \otimes_{i\in\text{odd}} O_{F_{i,i+1}}^{(k)}$ is equivalent to that of $V^{(k)}\cdot\Pi_{\text{loc}}^{\text{dist}}$, and $O_F^{(k)}\cdot\Pi_{\text{loc}}^{\text{dist}}$, respectively, after tracing over the purifying register, where the projector onto the local distinct subspace is given via Definition 3 and F is drawn from a family of PRFs on n bits. An application of the gentle measurement lemma then yields

$$\left\| \text{Tr}_{\mathsf{LRE}} |\mathcal{T}_k^{\mathbf{VFV}^\dagger}\rangle\langle\mathcal{T}_k^{\mathbf{VFV}^\dagger}| - \text{Tr}_{\mathsf{LRE}} |\mathcal{T}_k^{VFV^\dagger}\rangle\langle\mathcal{T}_k^{VFV^\dagger}| \right\|_1 \leq \frac{4nk}{2^{\xi/2}\xi}, \tag{D.43}$$

where we have used the fact that the restrictions can be applied after all oracle queries. Applying triangle inequality and collecting error terms yields

$$\left\| \mathop{\mathbb{E}}_{U\sim\mathcal{E}_{\mathbf{F}}} \left[(U)^{\otimes k} |\psi\rangle\langle\psi| \left(U^\dagger\right)^{\otimes k}\right] - \text{Tr}_{\mathsf{L}} |\mathcal{T}_k^{VFV^\dagger}\rangle\langle\mathcal{T}_k^{VFV^\dagger}| \right\|_1 \leq \frac{36nk(k+1)}{2^{\xi/8}\xi} + \frac{4nk}{2^{\xi/2}\xi}. \tag{D.44}$$

We can now analyze $|\mathcal{T}_k^{VFV^\dagger}\rangle$ following the approach of Proposition 2. We observe that by assumption, the value of the trace moments are bounded via

$$\left| \mathop{\mathbb{E}}_{F} \left[\frac{1}{N}|\text{Tr}\, F|^2\right] - \mathop{\mathbb{E}}_{U\sim\mathsf{Haar}} \left[\frac{1}{N}|\text{Tr}\, U|^2\right] \right| \leq \frac{1}{\omega(\text{poly}\, n)}, \tag{D.45}$$

since the normalized moments correspond to physical measurements. We therefore have that substituting the intermediate bounds from Proposition 2 and Theorem 7 yields

$$\left\| \text{Tr}_{\mathsf{L}} |\mathcal{T}_k^{VFV^\dagger}\rangle\langle\mathcal{T}_k^{VFV^\dagger}| - \text{Tr}_{\mathsf{L}} |\mathcal{T}_k^{\widetilde{V}}\rangle\langle\mathcal{T}_k^{\widetilde{V}}| \right\|_1 \leq \frac{36k(k+1)}{N^{1/8}} + \frac{12k^2}{N} + \frac{8k^2}{N}. \tag{D.46}$$

As a result, by a final triangle inequality, we have that

$$\left\| \mathop{\mathbb{E}}_{U\sim\mathcal{E}_{\mathbf{F}}} \left[U^{\otimes k} |\psi\rangle\langle\psi| (U^\dagger)^{\otimes k}\right] - \mathop{\mathbb{E}}_{U\sim\mathsf{Haar}} \left[U^{\otimes k} |\psi\rangle\langle\psi| (U^\dagger)^{\otimes k}\right] \right\|_1 \leq \frac{36nk(k+1)}{2^{\xi/8}\xi} + \frac{4nk}{2^{\xi/2}\xi} + O\left(\frac{k^2}{N^{1/8}}\right), \tag{D.47}$$

where we have again used the bound from Theorem 7 to compare $|\mathcal{T}_k^{\widetilde{V}}\rangle$ when traced over the purifying register, to the action of a Haar-random unitary. This yields the stated result. □

2. Proof of Theorems 3 and 4: Indistinguishability in adaptive quantum experiments

Having demonstrated our simpler proofs in the non-adaptive setting, we now turn to the adaptive setting and provide the complete proof of Theorems 3 and 4. We consider the following random unitary ensemble, which is generated by evolving the random Hamiltonian ensemble described in the main text for an evolution time $t = \pi$,

$$U = \left(\bigotimes_{i\in\text{even}} U_{i,i+1}^\dagger\right)\left(\bigotimes_{i\in\text{odd}} U_{i,i+1}^\dagger\right)\left(\bigotimes_{i\in\text{odd}} F_{i,i+1}\right)\left(\bigotimes_{i\in\text{odd}} U_{i,i+1}\right)\left(\bigotimes_{i\in\text{even}} U_{i,i+1}\right). \tag{D.48}$$

In Theorem 3, each small random unitary $U_{i,i+1}$ and each small PRF $F_{i,i+1}$ are chosen to be indistinguishable from a Haar-random unitary and a truly random function by any k-query quantum experiment. In Theorem 4, the are chosen to be indistinguishable by any polynomial-time quantum experiment.

As described in the main text, our proof of Theorems 3 and 4 follows from a "gluing" argument. To this end, we have the following two lemmas, which we prove in the subsequent subsections.

Lemma 11 (Conjugated random phases are random unitaries [64])**.** *Let $\mathcal{E}$ be equal to the product $U^\dagger F U$, where U is Haar-random and F is a random continuous phase gate. Then $\mathcal{E}$ is indistinguishable from a Haar-random unitary up to measurable error $\mathcal{O}(k/N^{1/4})$.*

The lemma is not stated explicitly in [64], but is derived in several steps spread between different proofs of their work. We provide a concise step-by-step summary of the proof in Section D 2 a below.

Lemma 12 (Gluing via conjugation)**.** *Let a, b, c, d be four subsystems. Consider the ensemble $\mathcal{E}$ on abcd given by the product of Haar-random unitaries, $U_{\mathsf{bc}}^\dagger(U_{\mathsf{ab}} \otimes U_{\mathsf{cd}})U_{\mathsf{bc}}$. The ensemble $\mathcal{E}$ is indistinguishable from a Haar-random unitary U_{abcd} up to measurable error $\mathcal{O}(t^2/N_{\mathsf{b}}^{1/2}) + \mathcal{O}(t^2/N_{\mathsf{c}}^{1/2}) + \mathcal{O}(t^2/N_{\mathsf{bc}}^{1/8})$.*

The proof of this lemma is significantly more involved and is completed via the path-recording framework in Section D 2 b.

Our proof of Theorems 3 and 4 follows simply from Lemma 11 and Lemma 12.

Proof of Theorems 3 and 4. By definition, each strong PRU is indistinguishable from a Haar-random unitary by any poly n-time quantum experiments, and each PRF is indistinguishable from a uniform continuous random phase by any poly n-time quantum experiment. Hence, we will assume $U_{i,i+1}$ and $F_{i,i+1}$ are truly random from hereon.

From Lemma 11, each product $U_{i,i+1}^\dagger F_{i,i+1} U_{i,i+1}$ for i odd is indistinguishable from a Haar-random unitary $U'_{i,i+1}$ up to measurable error $\mathcal{O}(k/2^{\xi/2})$ in any k-query quantum experiment. There are $n/2\xi$ such i, which leads to a total measurable error $\mathcal{O}((n/2\xi)k/2^{\xi/2})$. Then, applying Lemma 12 $n/2\xi$ times sequentially from left to right, we find that the entire product, $(\otimes_{i\in\text{even}} U_{i,i+1})^\dagger(\otimes_{i\in\text{even}} F_{i,i+1})(\otimes_{i\in\text{even}} U_{i,i+1})$, is indistinguishable from a Haar-random unitary on all n qubits up to measurable error $\mathcal{O}(k^2/2^{\xi/4})$ in any k-query quantum experiment. Hence, the random nearly-local Hamiltonian time-evolution ensemble is indistinguishable from a Haar-random unitary up to measurable error $\mathcal{O}(k^2/2^{\xi/4})$. For any $\xi = \omega(\log n)$, the measurable error is super-polynomially small in n for any $k = \text{poly}\, n$, and hence the ensemble forms a PRU with security against any poly n-time quantum adversary. □

a. *Proof of Lemma 11: Conjugated random phases are random unitaries*

We provide a concise summary of the proof in [64], and refer to [64] for further details. We can diagonalize a Haar-random unitary U' as $U' = U^\dagger F_{CUE} U$, where U is Haar-random and F_{CUE} is randomly drawn from the CUE spectral distribution [64]. Note that both the probability distribution p of N uniform random phases and the probability distribution p_{CUE} of N CUE-distributed random phases are invariant under any permutation of the N bitstrings. From this property, Eq. (B.34) of [64] shows that the measurable error of any quantum experiment that queries F versus F_{CUE} up to k times, is bounded above by the total variation distance between the $2k$-body marginal $p^{(2k)}$ of p and the $2k$-body marginal $p_{CUE}^{(2k)}$ of p_{CUE}. From Lemma 23 of [64], the $2k$-body marginals of the uniform and CUE distributions are close up to total variation distance $\mathcal{O}(k/N^{1/4})$. Hence, the measurable error between F and F_{CUE} is at most $\mathcal{O}(k/N^{1/4})$. This immediately implies that the measurable error between $U^\dagger F U$ and $U' = U^\dagger F_{CUE} U$ is at most $\mathcal{O}(k/N^{1/4})$ as well. □

b. *Proof of Lemma 12: Gluing random unitaries via conjugation*

Let $U \equiv U_{\mathsf{bc}}^\dagger(U_{\mathsf{ab}} \otimes U_{\mathsf{cd}})U_{\mathsf{bc}}$ be the unitary of interest, and $U' \equiv U_{\mathsf{bc}}^\dagger(U_{\mathsf{abcd}})U_{\mathsf{bc}} = U_{\mathsf{abcd}}$ a Haar-random unitary. In the latter expression, we have used the invariance of the Haar measure under any unitary rotation to eliminate $U_{\mathsf{bc}}, U_{\mathsf{bc}}^\dagger$.

From [28], we can replace each query to U with the product of path-recording oracles, $V \equiv V_{\mathsf{bc}}^\dagger(V_{\mathsf{ab}} \otimes V_{\mathsf{cd}})V_{\mathsf{bc}}$, acting on auxiliary spaces L_{ab}, L_{cd}, L_{bc}, R_{bc}. In particular, we take V_{bc}, $V_{\mathsf{bc}}^\dagger$ identical to [28]. From [28], this incurs a measurable error $\mathcal{O}(t^2/N_{\mathsf{bc}}^{1/8})$. On the other hand, we make two modifications to the path-recording oracle V_{ab}. First, following Appendix B of [28], we take V_{ab} to output bitstrings y_{ab}

that are locally distinct on b, and V_{cd} to output bitstrings y_{cd} that are locally distinct on c. This incurs a measurable error $\mathcal{O}(t^2/N_{\mathsf{b}}) + \mathcal{O}(t^2/N_{\mathsf{c}})$ following Appendix B of [28]. Second, we further enforce that the output bitstrings are locally distinct on b from all previous *inputs* to V_{ab}, and similar for c and V_{cd}. Inserting such a projector reduces the normalization of the state by at most $\mathcal{O}(t/N_{\mathsf{b}})$ per application, and hence by at most $\mathcal{O}(t^2/N_{\mathsf{b}})$ after t applications (and similar for c). From the sequential gentle measurement lemma [28], this incurs a total measurable error of at most $\mathcal{O}(t^2/N_{\mathsf{b}}^{1/2}) + \mathcal{O}(t^2/N_{\mathsf{c}}^{1/2})$.

We proceed in a similar manner for U'. We replace each query to U' with the product, $V' \equiv V_{\mathsf{bc}}^\dagger(V_{\mathsf{abcd}})V_{\mathsf{bc}}$, acting on auxiliary spaces $\mathsf{L}_{\mathsf{abcd}}$, L_{bc}, R_{bc}. We take V_{bc}, $V_{\mathsf{bc}}^\dagger$ as in [28] as before. We then take V_{abcd} as in the previous paragraph, to output bitstrings y_{abcd} that are locally distinct on both b and c, and which are also subsequently projected to also be locally distinct from all previous inputs to V_{abcd} on b and c. In total, these replacements accrue a measurable error $\mathcal{O}(t^2/N_{\mathsf{bc}}^{1/8}) + \mathcal{O}(t^2/N_{\mathsf{b}}^{1/2}) + \mathcal{O}(t^2/N_{\mathsf{c}}^{1/2})$, which has the same scaling as measurable error accrued in the previous paragraph.

From these definitions, for both V and V', the input to $V_{\mathsf{bc}}^\dagger$ is always distinct from all previous outputs of V_{bc}. This follows from our projection on the output of $V_{\mathsf{ab}} \otimes V_{\mathsf{cd}}$ (or V_{abcd}) onto bitstrings that are locally distinct from all previous inputs; every output of V_{bc} is an input to the proceeding $V_{\mathsf{ab}} \otimes V_{\mathsf{cd}}$ (or V_{abcd}). The input to $V_{\mathsf{bc}}^\dagger$ is also always distinct from all previous inputs to $V_{\mathsf{bc}}^\dagger$, since the output of $V_{\mathsf{ab}} \otimes V_{\mathsf{cd}}$ (or V_{abcd}) is locally distinct from all previous such outputs. Hence, we can replace $V_{\mathsf{bc}}^\dagger$ with its restriction on the distinct subspace, $W_{\mathsf{bc},R}$ [28]. This guarantees that $V_{\mathsf{bc}}^\dagger$ always creates a new entry in the R_{bc} register whenever it is queried.

From this property, it follows that the states on the auxiliary registers when we apply U correspond to "chains" of the form,

$$\begin{aligned}
&|\cup_{i=1}^m \{(x_{\mathsf{b}}^i x_{\mathsf{c}}^i, y_{\mathsf{b}}^{i,0} y_{\mathsf{c}}^{i,0})\}\rangle_{\mathsf{L}_{\mathsf{bc}}} \\
&|\cup_{i=1}^m \{(x_{\mathsf{a}}^{i,1} y_{\mathsf{b}}^{i,0}, z_{\mathsf{a}}^{i,1} y_{\mathsf{b}}^{i,1}), \ldots, (x_{\mathsf{a}}^{i,t_i} y_{\mathsf{b}}^{i,t_i-1}, z_{\mathsf{a}}^{i,t_i} y_{\mathsf{b}}^{i,t_i})\}\rangle_{\mathsf{L}_{\mathsf{ab}}} \\
&|\cup_{i=1}^m \{(y_{\mathsf{c}}^{i,0} x_{\mathsf{d}}^{i,1}, y_{\mathsf{c}}^{i,1} z_{\mathsf{d}}^{i,1}), \ldots, (y_{\mathsf{c}}^{i,t_i-1} x_{\mathsf{d}}^{i,t_i}, y_{\mathsf{c}}^{i,t_i} z_{\mathsf{d}}^{i,t_i})\}\rangle_{\mathsf{L}_{\mathsf{cd}}} \\
&|\cup_{i=1}^m \{(y_{\mathsf{b}}^{i,t_i} y_{\mathsf{c}}^{i,t_i}, z_{\mathsf{b}}^i z_{\mathsf{c}}^i)\}\rangle_{\mathsf{R}_{\mathsf{bc}}} .
\end{aligned} \tag{D.49}$$

Each chain $i = 1, \ldots, m$ of length t_i involves $t_i - 1$ applications of the annihilation branch of V_{bc}. Each annihilation undoes the action of a previous creation by $W_{\mathsf{bc},R}$, and thereby "chains" together the output of the $V_{\mathsf{ab}} \otimes V_{\mathsf{cd}}$ that preceded that $W_{\mathsf{bc},R}$ with the input of the $V_{\mathsf{ab}} \otimes V_{\mathsf{cd}}$ that proceeded the V_{bc}. That is, the output of the earlier $V_{\mathsf{ab}} \otimes V_{\mathsf{cd}}$ is stored in pairs with the input of the later $V_{\mathsf{ab}} \otimes V_{\mathsf{cd}}$ in the L_{ab} and L_{cd} relation registers. We have $\sum_i t_i = t$, the total number of applications of the unitary. From our definitions, all of the $y_{\mathsf{b}}^{i,\tau_i}$ for any i and any $0 \leq \tau_i \leq t_i$ are distinct, and similar for the $y_{\mathsf{c}}^{i,\tau_i}$.

Meanwhile, the the states on the auxiliary registers when we apply U' correspond to chains of the very similar form,

$$\begin{aligned}
&|\cup_{i=1}^m \{(x_{\mathsf{b}}^i x_{\mathsf{c}}^i, y_{\mathsf{b}}^{i,0} y_{\mathsf{c}}^{i,0})\}\rangle_{\mathsf{L}_{\mathsf{bc}}} \\
&|\cup_{i=1}^m \{(x_{\mathsf{a}}^{i,1} y_{\mathsf{b}}^{i,0} y_{\mathsf{c}}^{i,0} x_{\mathsf{d}}^{i,1}, z_{\mathsf{a}}^{i,1} y_{\mathsf{b}}^{i,1} y_{\mathsf{c}}^{i,1} z_{\mathsf{d}}^{i,1}), \ldots, (x_{\mathsf{a}}^{i,t_i} y_{\mathsf{b}}^{i,t_i-1} y_{\mathsf{c}}^{i,t_i-1} x_{\mathsf{d}}^{i,t_i}, z_{\mathsf{a}}^{i,t_i} y_{\mathsf{b}}^{i,t_i} y_{\mathsf{c}}^{i,t_i} z_{\mathsf{d}}^{i,t_i})\}\rangle_{\mathsf{L}_{\mathsf{abcd}}} \\
&|\cup_{i=1}^m \{(y_{\mathsf{b}}^{i,t_i} y_{\mathsf{c}}^{i,t_i}, z_{\mathsf{b}}^i z_{\mathsf{c}}^i)\}\rangle_{\mathsf{R}_{\mathsf{bc}}} ,
\end{aligned} \tag{D.50}$$

where similar to before all of the $y_{\mathsf{b}}^{i,\tau_i}$ are distinct and all of the $y_{\mathsf{c}}^{i,\tau_i}$ are distinct. Moreover, the coefficients of each auxiliary register as above are identical to those of the auxiliary registers for U. That is, the only difference between the path-recording state in the experiment involving U and that in the experiment involving U' is the replacement of each auxiliary state in Eq. (D.49) with the corresponding auxiliary state in Eq. (D.50).

It remains only to show that there is a one-to-one isometry between the auxiliary states in Eq. (D.49) and those in Eq. (D.50). Note that this is not a priori guaranteed, owing to the symmetrization of each set of pairs in each register. To show that there exists an isometry, we must show that for every state in Eq. (D.50) there is a unique associated state in Eq. (D.49). The reverse direction follows trivially, since there is less symmetrization in Eq. (D.49) than in Eq. (D.50). This claim follows immediately from the fact that all $y_{\mathsf{b}}^{i,\tau_i}$ are distinct and all $y_{\mathsf{c}}^{i,\tau_i}$ are distinct. Hence, for each value of $z_{\mathsf{b}}^i z_{\mathsf{c}}^i$ on the R_{bc} register, there are a unique two values of y_{b}^{i,t_i} and y_{c}^{i,t_i}, and in turn a unique two values of y_{b}^{i,t_i-1} and y_{c}^{i,t_i-1}, and so on to $y_{\mathsf{b}}^{i,0}$ and $y_{\mathsf{c}}^{i,0}$, on the L_{ab} and L_{cd} registers, and thus a unique value of $y_{\mathsf{b}}^{i,0} y_{\mathsf{c}}^{i,0}$ and $x_{\mathsf{b}}^i x_{\mathsf{c}}^i$ on the L_{bc} register. The local distinctness of $y_{\mathsf{b}}^{i,\tau_i}$ and $y_{\mathsf{c}}^{i,\tau_i}$ guarantees that for each $y_{\mathsf{b}}^{i,\tau_i+1}$ and $y_{\mathsf{c}}^{i,\tau_i+1}$ there is a unique $y_{\mathsf{b}}^{i,\tau_i}$ and $y_{\mathsf{c}}^{i,\tau_i}$ on L_{ab} and L_{cd}. The distinctness of $y_{\mathsf{b}}^{i,\tau_i} y_{\mathsf{c}}^{i,\tau_i}$ from $y_{\mathsf{b}}^{i,0} y_{\mathsf{c}}^{i,0}$ guarantees that the step

in process above where one jumps from the L_{ab}, L_{cd} registers to the L_{bc} register is uniquely determined. This completes our proof. □

3. Proof of Proposition 1: Impossibility of unitary designs from efficient temporal ensembles

We consider the state $\Phi_{\mathcal{E}}(|0^n\rangle\langle 0^n|^{\otimes k})$, in which the twirl over k copies of a unitary drawn from $\mathcal{E}$ is applied to k copies of the zero state on n qubits. For a Haar-random unitary, the state $\Phi_H(|0^n\rangle\langle 0^n|^{\otimes k})$ has a flat spectrum across the symmetric subspace, which contains $\binom{2^n+k-1}{k}$ elements [16]. For any approximate unitary k-design with additive error ε, $\Phi_{\mathcal{E}}(|0^n\rangle\langle 0^n|^{\otimes k})$ must be ε-close in trace distance to this state.

Let us now analyze the rank of the state $\Phi_{\mathcal{E}}(|0^n\rangle\langle 0^n|^{\otimes k})$. We begin by considering the case of a single fixed Hamiltonian; our results will trivially extend to a bounded number L of random Hamiltonians. Let us discretize the time interval $[0,T]$ into steps $\tau, 2\tau, \ldots, (T/\tau)\tau$ of a small fixed size τ. For any probability distribution $\mathcal{D}$ over the evolution time $t \in [0,T]$, we can decompose the state $\Phi_{\mathcal{E}}(|0^n\rangle\langle 0^n|^{\otimes k})$ into a mixture of contributions from nearby each time step,

$$\Phi_{\mathcal{E}}(|0^n\rangle\langle 0^n|^{\otimes k}) = \sum_{\ell=1}^{T/\tau} \mathcal{D}(\ell) \int_{(\ell-1)\tau}^{\ell\tau} dt \mathcal{D}(t|\ell) \left(e^{-iHt}|0^n\rangle\langle 0^n| e^{iHt}\right)^{\otimes k}, \tag{D.51}$$

where $\mathcal{D}(\ell)$ is the total probability to select a time in the ℓ-th step, and $\mathcal{D}(t|\ell) = \mathcal{D}(t)/\mathcal{D}(\ell)$ is the conditional probability to select a time t within the step ℓ. We can then apply the general bound,

$$\begin{aligned}&\left\|e^{-iHt}|0^n\rangle\langle 0^n| e^{iHt} - e^{-iH\ell\tau}|0^n\rangle\langle 0^n| e^{iH\ell\tau}\right\|_1 \\ &\quad\leq 2\left\|(e^{-iHt} - e^{-iH\ell\tau})|0^n\rangle\right\|_2 \leq 2\left\|(e^{-iH(t-\ell\tau)} - 1)|0^n\rangle\right\|_2 \leq 2\|H\|_\infty |t-\ell\tau|.\end{aligned}$$

where the first inequality follows from the inequality $\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \leq 2\||u\rangle - |v\rangle\|_2$ [28]. In fact, we will need instead an identical version of this bound for the k-th power of both states,

$$\begin{aligned}&\left\|\left(e^{-iHt}|0^n\rangle\langle 0^n| e^{iHt}\right)^{\otimes k} - \left(e^{-iH\ell\tau}|0^n\rangle\langle 0^n| e^{iH\ell\tau}\right)^{\otimes k}\right\|_1 \\ &\qquad\leq 2\left\|((e^{-iHt})^{\otimes k} - (e^{-iH\ell\tau})^{\otimes k})|0^n\rangle^{\otimes k}\right\|_2 \leq 2k\|H\|_\infty |t-\ell\tau|.\end{aligned}$$

Inserting this bound into Eq. (D.51) and applying the triangle inequality to the integral over t, we find

$$\left\|\Phi_{\mathcal{E}}(|0^n\rangle\langle 0^n|^{\otimes k}) - \sum_{\ell=1}^{T/\tau} \mathcal{D}(\ell)\cdot\left(e^{-iH\ell\tau}|0^n\rangle\langle 0^n| e^{iH\ell\tau}\right)^{\otimes k}\right\|_1 \leq 2k\|H\|_\infty \tau. \tag{D.52}$$

This shows $\Phi_{\mathcal{E}}(|0^n\rangle\langle 0^n|^{\otimes k})$ can be approximated by a state with rank T/τ up to a small trace-norm error $2k\|H\|_\infty\tau$.

The proof is now complete. The state $\Phi_{\mathcal{E}}(|0^n\rangle\langle 0^n|^{\otimes k})$ is $2k\|H\|_\infty\tau$-close to a state with rank T/τ. The state $\Phi_H(|0^n\rangle\langle 0^n|^{\otimes k})$ has a flat spectrum with rank $\binom{2^n+k-1}{k}$. A simple computation shows that any rank r quantum state can be at most $2(1-r/r_0)$-close to a state with a flat spectrum of rank $r_0 > r$. Hence, for the two states of interest to be ε-close, we must have

$$2\left(1 - \frac{T}{\tau}\binom{2^n+k-1}{k}^{-1}\right) - 2k\|H\|_\infty\tau \leq \varepsilon. \tag{D.53}$$

Let $\varepsilon = 1/4$ and set τ such that $2k\|H\|_\infty\tau = 1/4$ as well. Hence, we require

$$1 - \frac{T}{\tau}\binom{2^n+k-1}{k}^{-1} \leq \frac{1}{4}, \tag{D.54}$$

which requires

$$T \geq \frac{3}{4}\tau \binom{2^n + k - 1}{k} = \frac{3}{32k\|H\|_\infty}\binom{2^n + k - 1}{k} \geq \frac{3}{32k\|H\|_\infty}\frac{2^{nk}}{k!}. \tag{D.55}$$

If the ensemble involves N_H Hamiltonians, the lower bound decreases by a factor of N_H. This completes the proof. □