Exact Emergent Quantum State Designs from Quantum Chaotic Dynamics

Wen Wei Ho[1] and Soonwon Choi[2]
[1]*Department of Physics, Stanford University, Stanford, California 94305, USA*
[2]*Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Received 12 November 2021; accepted 18 January 2022; published 11 February 2022)

We present exact results on a novel kind of emergent random matrix universality that quantum many-body systems at infinite temperature can exhibit. Specifically, we consider an ensemble of pure states supported on a small subsystem, generated from projective measurements of the remainder of the system in a local basis. We rigorously show that the ensemble, derived for a class of quantum chaotic systems undergoing quench dynamics, approaches a universal form completely independent of system details: it becomes uniformly distributed in Hilbert space. This goes beyond the standard paradigm of quantum thermalization, which dictates that the subsystem relaxes to an ensemble of quantum states that reproduces the expectation values of local observables in a thermal mixed state. Our results imply more generally that the *distribution* of quantum states themselves becomes indistinguishable from those of uniformly random ones, i.e., the ensemble forms a quantum state design in the parlance of quantum information theory. Our work establishes bridges between quantum many-body physics, quantum information and random matrix theory, by showing that pseudorandom states can arise from isolated quantum dynamics, opening up new ways to design applications for quantum state tomography and benchmarking.

DOI: 10.1103/PhysRevLett.128.060601

Introduction.—Universality, the emergence of features independent of precise microscopic details, allows us to simplify the analysis of complex systems and to establish important general principles. Quantum thermalization prescribes a scenario where such universal behavior arises from generic dynamics of isolated quantum many-body systems. It is widely accepted that quantum chaotic many-body systems—that is, systems with spectral correlations described by random matrix theory (RMT) [1,2]—will locally relax to maximally entropic thermal states constrained only by global conservation laws [3]. Physically, this arises because of the extensive amounts of entanglement generated between a local subsystem and its complement, which acts like a bath. Ignoring the state of the bath, the subsystem acquires a universal, mixed form, described by a generalized Gibbs state. Understanding this universality has led to the development of the eigenstate thermalization hypothesis (ETH) [4,5], and has also spurred intense research into mechanisms for its breakdown such as many-body localization [3,6] and quantum many-body scarring [7,8].

Here we take a perspective different from the standard treatment of quantum thermalization and ask: what happens if (some) information about the bath is explicitly kept track of instead of discarded—how then does one describe properties of a local subsystem? Will there be any kind of universality in this setting? Such a consideration is of fundamental interest, as it would illuminate the role of the bath in quantum thermalization beyond the conventional paradigm. It is also natural given the capability of present-day quantum simulators, which allow access to correlations not only within a subsystem, but also between the subsystem and its complement.

To this end we consider here the projected ensemble, introduced in Refs. [9,10]. This is a collection of pure states supported on a local subsystem A, each of which is associated with the outcome of a projective measurement of the complementary subsystem B in a fixed local basis. Such an ensemble contains strictly more information than the conventionally studied reduced density matrix ρ_A, which is recovered from the first moment of the ensemble's distribution; higher moments further characterize statistical properties of the ensemble in increasingly refined fashions, such as the spread of projected states over Hilbert space.

In this Letter, we present exact results on universal properties exhibited by the projected ensemble, obtained from a class of quantum chaotic many-body dynamics without global conservation laws: we rigorously show that its statistics becomes completely independent of microscopic details over time. Concretely, we focus on the nonintegrable, periodically kicked Ising model and prove in the thermodynamic limit (TDL) that the projected ensemble evolves toward a maximally entropic distribution, i.e., all its moments agree exactly with those of the uniform ensemble over Hilbert space. In the parlance of quantum information theory (QIT), such an ensemble is said to form a quantum state design [11–14]. Intriguingly, this happens in finite time in quench dynamics.

Our results demonstrate a new kind of emergent random matrix universality exhibited by quantum chaotic many-body systems at infinite temperature: at late times, a local subsystem A is characterized by an ensemble of states indistinguishable from random ones not only within expectation values of observables (*á la* standard quantum thermalization [3]), but also within any statistical properties of the states themselves. In other words, there is no protocol performable on A which can information-theoretically differentiate the projected states from uniformly random ones. Theoretical and experimental evidence have been given conjecturing the appearance of such universality across wide classes of physical systems and states [9,10]; our results complement these by furnishing an exactly solvable model where this conjecture can be proven.

We note that the kicked Ising model we study exhibits RMT spectral statistics for all times, as proven in Ref. [15]; the result involved a necessary averaging over a small but nonvanishing amount of disorder. In contrast, our work demonstrates how universal randomness can also arise naturally within the dynamics of a single instance of a clean Hamiltonian and wave function, induced by measurements.

Projected ensembles and quantum state designs.—The projected ensemble is defined as follows [9,10]. Consider a single generator state $|\Psi\rangle$ of a large system of N qubits (generalization to a qudit system is immediate), and a bipartition into subsystems A and B with N_A and N_B qubits, respectively. We assume the state of B is projectively measured in the local computational basis, so that one obtains a bit-string outcome $z_B = (z_{B,1}, z_{B,2}, \cdots, z_{B,N_B}) \in \{0,1\}^{N_B}$ and its associated pure quantum state on A,

$$|\psi(z_B)\rangle = (\mathbb{I}_A \otimes \langle z_B|)|\Psi\rangle/\sqrt{p(z_B)}, \qquad (1)$$

with probability $p(z_B) = \langle\Psi|\mathbb{I}_A \otimes |z_B\rangle\langle z_B|\Psi\rangle$; see Fig. 1(a). The set of (generally nonorthogonal) projected states over all 2^{N_B} outcomes with respective probabilities, forms the *projected ensemble* $\mathcal{E} \coloneqq \{p(z_B), |\psi(z_B)\rangle\}$.

The statistical properties of $\mathcal{E}$ are characterized by moments of its distribution. Concretely, the kth moment is captured by a density matrix

$$\rho_{\mathcal{E}}^{(k)} = \sum_{z_B} p(z_B)(|\psi(z_B)\rangle\langle\psi(z_B)|)^{\otimes k} \qquad (2)$$

acting on the k-fold tensor product space $\mathcal{H}_A^{\otimes k}$, where $\mathcal{H}_A$ is the Hilbert space of A. The first moment $k=1$ (mean) contains information about the expectation value of any physical observable in A, as $\rho_{\mathcal{E}}^{(1)}$ equals ρ_A. Higher moments $k \geq 2$ capture properties beyond, in particular, quantifying the variance, skewness, etc. of the distribution of projected states over $\mathcal{H}_A$. We note that understanding statistical properties of ensembles of quantum states or unitaries (specifically quantifying the degree of randomness) forms the basis of many applications in quantum

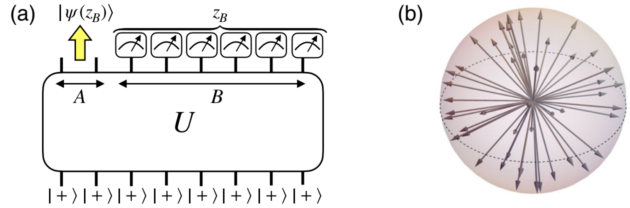


FIG. 1. (a) Projected state $|\psi(z_B)\rangle$ on A arises from a projective measurement of subsystem B in the local z basis, with measurement outcome z_B. Here the generator state is an initial product state $|+\rangle^{\otimes N}$ evolved by unitary U. (b) Distribution over Hilbert space of projected states $|\psi(z_B)\rangle$, each occurring with probability $p(z_B)$, illustrated for $N_A = 1$. The projected ensemble $\mathcal{E}$ forming a quantum state design in the TDL implies the states cover the Bloch sphere uniformly.

information science such as cryptography, tomography, or machine learning, as well as sampling-based computational-advantage tests for near-term quantum devices [16–29]. Equation (2) probes analogous information for the projected states of a small subsystem, where now the ensemble is of states correlated to measurement outcomes of the bath. We emphasize such higher moments have begun to be experimentally probed in quantum simulators [9], highlighting the need to better understand their universal properties.

We focus in this Letter on generator states arising from quench dynamics of systems without explicit conservation laws. As quantum thermalization dictates that the first moment should acquire a universal form $\rho_{\mathcal{E}}^{(1)} \propto \mathbb{I}_A$ over time, it is natural to conjecture that higher moments become similarly "maximally mixed" [9,10]. To quantify this, we appeal to the notion of *quantum state designs* in QIT [11–14], which measures the similarity of $\mathcal{E}$ to an ensemble of uniformly (i.e., Haar)-random states on A [30], whose kth moment is given by

$$\rho_{\text{Haar}}^{(k)} = \int_{\psi\sim\text{Haar}(2^{N_A})} d\psi(|\psi\rangle\langle\psi|)^{\otimes k}. \qquad (3)$$

The agreement of moments is captured by the trace distance $\Delta^{(k)} = \frac{1}{2}\|\rho_{\mathcal{E}}^{(k)} - \rho_{\text{Haar}}^{(k)}\|_1$; if $\Delta^{(k)}$ vanishes (is ϵ small), then $\mathcal{E}$ is said to form an exact (ϵ approximate) quantum state k-design. Below, we study a local, quantum chaotic model where the projected ensemble from quench dynamics can be exactly calculated, and analyze the degree to which state k-designs are formed, with time and number of qubits measured.

Model and results.—We consider a 1D chain of N spin-1/2 particles (or qubits) evolving under dynamics generated by the Floquet unitary

$$U_F = U_h\, e^{-iH_{\text{Ising}}\tau}. \qquad (4)$$

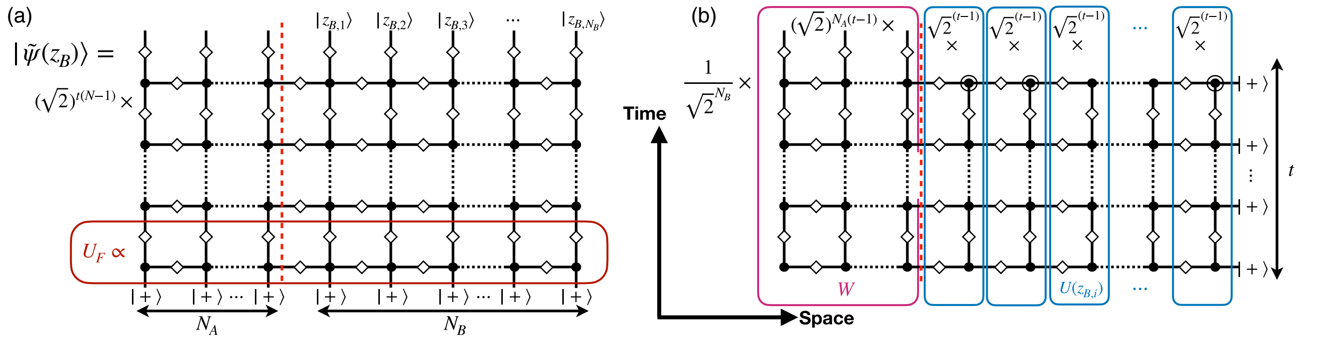


FIG. 2. (a) Tensor-network representation of an (unnormalized) projected state $|\tilde{\psi}(z_B)\rangle$ for the kicked Ising model, given measurement outcome z_B. Each black node carries factor g, see Eq. (5). The red box is proportional to the Floquet unitary U_F, which acts on the spin chain with initial state $|+\rangle^{\otimes N}$. There are t applications of U_F. (b) The same state can be obtained from evolution in the spatial direction (right to left) of the initial state $|+\rangle^{\otimes t}$ on the "dual chain," by products of unitaries $U(z_{B,i})$ (blue box), where $z_{B,i} \in \{0,1\}$, illustrated here as the particular product $U(1)U(1)U(0)\cdots U(1)$. $U(z_{B,i})$ is generated also by a kicked Ising model; however, the strength of the longitudinal field at temporal site t depends on $z_{B,i}$ (see main text). There is a final linear map W (pink box) sending the resulting t qubit state to a state supported on A.

Here $U_h = \exp(-ih\sum_{i=1}^N \sigma_i^y)$ is a global y rotation, while $H_{\text{Ising}} = J\sum_{i=1}^{N-1}\sigma_i^z\sigma_{i+1}^z + g\sum_{i=1}^N \sigma_i^z + (b_1\sigma_1^z + b_N\sigma_N^z)$ is the Ising model with nearest-neighbor interaction strength J and longitudinal field g, applied for time $\tau = 1$. $\sigma_i^x, \sigma_i^y, \sigma_i^z$ are standard Pauli matrices at site i. The last term in H_{Ising} are boundary terms with strengths we fix to $b_1 = b_N = \pi/4$, introduced solely for technical simplifications. See Ref. [30] for discussions of the case with periodic boundary conditions.

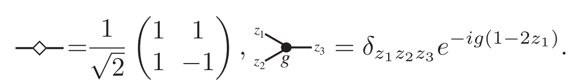
Equation (4) describes unitary evolution by a 1D periodically kicked Ising model, which is known to be nonintegrable for generic values of (J, h, g), and possesses no global conservation laws. We fix $J, h = \pi/4$ and allow arbitrary g excluding exceptional points $g \notin \mathbb{Z}\pi/8$. We calculate the projected ensemble $\mathcal{E}$ on subsystem A comprised of the first N_A contiguous qubits, measuring the remaining N_B qubits in the computational z basis from the generator state $|\Psi(t)\rangle = U_F^t|+\rangle^{\otimes N}$, where $|+\rangle$ is the x polarized state (see Supplemental Material [30] for a discussion on other initial states). Here $t \in \mathbb{Z}$ is the number of applications of U_F.

Our central result is that for a fixed subsystem A, evolution under the kicked Ising model for a sufficiently long but finite time followed by measurements on an infinitely-large complementary subsystem B, essentially effects random rotations on A, so that the projected states are statistically indistinguishable from Haar-random ones, see Fig. 1(b). Precisely, we have:

Theorem 1: For $t \geq N_A$ and $g \notin \mathbb{Z}\pi/8$, the projected ensemble $\mathcal{E}$ forms an exact quantum state design in the thermodynamic limit: for any k, $\lim_{N_B\to\infty}\rho_{\mathcal{E}}^{(k)} = \rho_{\text{Haar}}^{(k)}$.

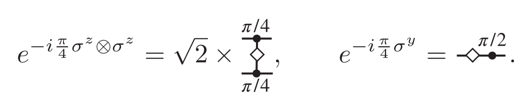
The proof of our claim combines several tools used in quantum chaos and QIT, outlined here. First, we leverage a so-called *dual-unitary* property of U_F enjoyed at the special values of J, h picked [15,36]: the unitary represented as a tensor-network can be interpreted as unitary evolution not only along the temporal, but also the *spatial* direction (Fig. 2). In the dual picture, measuring N_B qubits induces an ensemble of quantum circuits enumerated by measurement outcomes, which act on t fictitious qubits. Each projected state (1) arises from a particular circuit evolution, followed by a map to the space of N_A qubits [discussed in Eq. (8)]. We show the ensemble of circuits, when infinitely deep (corresponding to the TDL), is statistically indistinguishable from Haar-random unitaries—i.e., it forms a *unitary design* [11–14], allowing us to establish that the projected states are correspondingly uniformly distributed over Hilbert space.

We now flesh out the above steps. We first introduce the following elementary diagrams:



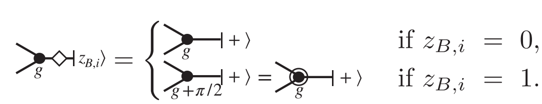
$$= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad = \delta_{z_1 z_2 z_3} e^{-ig(1-2z_1)}. \tag{5}$$

The former represents the Hadamard gate, while the latter is a tensor evaluating to nonzero values, $e^{\mp ig}$, if and only if all three indices $z_i \in \{0,1\}$ agree, $z_1, z_2, z_3 = 0(1)$, respectively. These tensors can be contracted with one another, or with quantum states (see Ref. [30] for details). Using this notation, evolution by Ising interactions and transverse fields can be cast (up to irrelevant global phases) as



$$e^{-i\frac{\pi}{4}\sigma^z\otimes\sigma^z} = \sqrt{2}\times \quad , \qquad e^{-i\frac{\pi}{4}\sigma^y} = \quad . \tag{6}$$

Additionally, a measurement at site i is represented by a contraction with an outcome state $|z_{B,i}\rangle$, yielding two possibilities



$$= \begin{cases} \quad\quad & \text{if } z_{B,i} = 0, \\ \quad = \quad & \text{if } z_{B,i} = 1. \end{cases} \tag{7}$$

Combined together, our diagrams allow a particularly compact tensor-network representation of the (unnormalized) projected state $|\tilde{\psi}(z_B)\rangle = (\mathbb{I}_A \otimes \langle z_B|)U_F^t|+\rangle^{\otimes N}$ [Fig. 2(a)]. We note this tensor-network state is closely related to the one representing the 2D cluster state that forms a universal resource for measurement-based quantum computation [30,31].

Figure 2(a) demonstrates the dual-unitary property of U_F evidently: there is a self-similarity of the diagram read bottom-up (temporally) or right-left (spatially). Precisely, Fig. 2(b) illustrates $|\tilde{\psi}(z_B)\rangle$ can be equivalently interpreted as evolution of an initial state $|+\rangle^{\otimes t}$ on t qubits ("dual chain") by quantum circuits $\mathcal{U}(z_B) \coloneqq U(z_{B,1})U(z_{B,2})\cdots U(z_{B,N_B})$, followed by a linear map W transforming the resulting state to one on N_A qubits:

$$|\tilde{\psi}(z_B)\rangle = \frac{1}{\sqrt{2^{N_B}}} W\mathcal{U}(z_B)|+\rangle^{\otimes t}. \tag{8}$$

Here, $U(z_{B,i})$ takes two forms: $U(0)$, $U(1)$, depending on the measurement outcome $z_{B,i} \in \{0,1\}$. Both are identical in form and have parameters J, h, g, b_1 similar to the Floquet unitary (4), upon interpreting the site index i to run along the t-site dual chain, except with differing boundary fields $b_t = \pi/4(3\pi/4)$ if $z_{B,i} = 0(1)$. Equation (2) can thus be rewritten as a sum over all circuit evolutions:

$$\rho_{\mathcal{E}}^{(k)} = \sum_{z_B} \frac{1}{2^{N_B}} \frac{[W\mathcal{U}(z_B)(|+\rangle\langle+|)^{\otimes t}\mathcal{U}(z_B)^\dagger W^\dagger]^{\otimes k}}{[\langle+|^{\otimes t}\mathcal{U}(z_B)^\dagger W^\dagger W\mathcal{U}(z_B)|+\rangle^{\otimes t}]^{k-1}}. \tag{9}$$

We now observe that for $t \geq N_A$, W is expressible as $W = \sqrt{2}^{(t-N_A)}\langle+|^{\otimes(t-N_A)}V$ [37], where V is a unitary on $\mathbb{C}^{2^t}$ whose particular form is unimportant as we will argue below. This assertion can be straightforwardly verified diagrammatically [30]. We further observe that Eq. (9) can be thought of as the average behavior of a function taking as input a circuit $\mathcal{U}(z_B)$, with output $[(\cdots)^{\otimes k}/(\cdots)^{k-1}]$, sampled uniformly over all 2^{N_B} possible circuits indexed by z_B. Our task therefore falls to examining the statistics of the (uniform) ensemble of unitaries $\mathcal{E}_{\mathcal{U}} \coloneqq \{\mathcal{U}(z_B)\}$. We show that this discrete set $\mathcal{E}_U$ in fact samples the (continuous) space of unitaries on $\mathbb{C}^{2^t}$ uniformly in the TDL $N_B \to \infty$, stated in Theorem 2.

We can thus in Eq. (9) replace in the TDL the sum over states $\mathcal{U}(z_B)|+\rangle^{\otimes t}$, which by virtue of Theorem 2 become uniformly distributed over Hilbert space, with an integral over Haar-random states. This step is justified more rigorously in the Supplemental Material [30]. The unitary V entering in the decomposition of W can then be absorbed in the integral via invariance of the Haar measure, leading to

$$\lim_{N_B\to\infty} \rho_{\mathcal{E}}^{(k)} = \int_{\Psi\sim\mathrm{Haar}(2^t)} d\Psi \frac{(|\Psi_+\rangle\langle\Psi_+|)^{\otimes k}}{\langle\Psi_+|\Psi_+\rangle^k} \times 2^{t-N_A}\langle\Psi_+|\Psi_+\rangle,$$

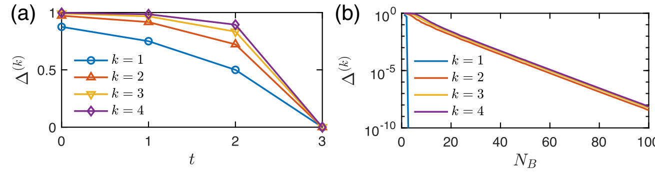


FIG. 3. Trace distance $\Delta^{(k)}$ of kth moment of projected ensemble to a Haar random ensemble versus (a) time and (b) projected subsystem size N_B, for $g = \pi/9$ and $N_A = 3$. For (a), $N_B = 100$. For (b), $t = N_A = 3$.

where $|\Psi_+\rangle = \langle+|^{\otimes(t-N_A)}|\Psi\rangle$. Finally, Lemma 4 of Ref. [10] specifies that random variables $[(|\Psi_k\rangle\langle\Psi_k|)^{\otimes k}/\langle\Psi_k|\Psi_k\rangle^k]$ and $2^{t-N_A}\langle\Psi_+|\Psi_+\rangle$ are independent, allowing us to distribute the integral: the former equals (3) while the latter evaluates to 1, giving our claimed result. ■

Figure 3 numerically illustrates the emergence of quantum state designs for various Floquet times and projected subsystem size N_B. We find that $\mathcal{E}$ forms an exact state k-design for $k = 1$ when $N_B \geq N_A = t$ (i.e., reduced density matrix is maximally mixed), as expected from the results of Ref. [32], while it converges exponentially fast with N_B for higher k's.

Statistics of unitary ensemble $\mathcal{E}_U$.—In Theorem 1, we used the following nontrivial result describing the distribution of unitaries $\mathcal{U}(z_B)$ in the TDL:

Theorem 2: For $g \notin \mathbb{Z}\pi/8$, all moments k of $\mathcal{E}_U$ and the Haar-random unitary ensemble agree in the TDL: $\lim_{N_B\to\infty}\sum_{z_B}(1/2^{N_B})\mathcal{U}(z_B)^{\otimes k}\otimes\mathcal{U}(z_B)^{*\otimes k} = \int_{U\sim\mathrm{Haar}(2^t)} dU U^{\otimes k}\otimes U^{*\otimes k}$. That is, $\mathcal{E}_{\mathcal{U}}$ in the TDL forms an exact unitary design.

Recall an element of $\mathcal{E}_U$ is a quantum circuit, e.g., $U(1)U(0)U(0)U(1)\cdots$, which is interpretable as an instance of evolution by a randomly kicked Ising model on t qubits, where the randomness arises only from the boundary longitudinal field at site t taking two possible values g and $g+\pi/2$ with equal probability, between every kick. Thus, Theorem 2 amounts to saying that unitaries generated by a kicked Ising model with time dependent but ultralocalized randomness, suffice to form arbitrarily good approximations of Haar-random unitaries after long enough times. In contrast, many previous works concerning the emergence of such unitary designs in dynamics assume *global* (i.e., an extensive number of) system parameters that are random in time [18,38,39], and so the randomly kicked Ising model constitutes an example where the degree of randomness required is arguably minimal. The proof of Theorem 2, presented in the Supplemental Material [30], is technical, but essentially amounts to showing that basic unitaries $U(0)$, $U(1)$ (and their inverses) form a universal gate set, such that any unitary on $\mathbb{C}^{2^t}$ can be reached from their products [40].

Discussion.—Our main result, Theorem 1, establishes the first provable example of a new kind of emergent random matrix universality exhibited by quantum chaotic many-body systems, conjectured by Refs. [9,10]. It represents a deep form of quantum thermalization characterized by a maximally entropic distribution of pure states of a subsystem induced by the bath, suggesting a generalization of the ETH to account for such features. An open question is how such universality is modified in the presence of globally conserved quantities, like energy. For $k = 1$, quantum thermalization already specifies a universal form at late times: a Gibbs ensemble at a definite temperature. What are the universal ensembles, if any, that $\rho_{\mathcal{E}}^{(k)}$ for $k \geq 2$ tend toward? From a technical standpoint, our work asserts the projected ensemble forms a quantum state design in the limit when infinitely many qubits are measured; understanding the rate of convergence with large but finite system sizes would be very interesting (see Supplemental Material [30] for a preliminary discussion).

The appearance of quantum state designs in a physical system has also quantum information science applications, in particular for tasks like state tomography, benchmarking, or cryptography, which employ ensembles of random unitaries or states [16–29,42]. For example, by applying random unitaries, projectively measuring, and processing the classical data, one can in certain cases reconstruct an approximate description of a system's state in a protocol called classical shadow tomography [26]. Our results suggest that one can replace the direct application of a random unitary, which requires fine control, with simple projective measurements following quantum chaotic dynamics to effectively realize random rotations on a subsystem, potentially amounting to a hardware-efficient method to implement the tomographic protocol.

We thank N. Hunter-Jones, H. Pichler, and X.-L. Qi for useful discussions. We also thank J. Cotler and N. Maskara for a careful read of the manuscript. W. W. H. is supported in part by the Stanford Institute of Theoretical Physics.

[1] M. L. Mehta, *Random Matrices and the Statistical Theory of Energy Levels* (Academic Press, New York, 1967).
[2] F. Haake, *Quantum Signatures of Chaos* (Springer, New York, 2001).
[3] R. Nandkishore and D. A. Huse, Many-body localization and thermalization in quantum statistical mechanics, Annu. Rev. Condens. Matter Phys. **6**, 15 (2015).
[4] J. M. Deutsch, Quantum statistical mechanics in a closed system, Phys. Rev. A **43**, 2046 (1991).
[5] M. Srednicki, Chaos and quantum thermalization, Phys. Rev. E **50**, 888 (1994).
[6] D. A. Abanin, E. Altman, I. Bloch, and M. Serbyn, Colloquium: Many-body localization, thermalization, and entanglement, Rev. Mod. Phys. **91**, 021001 (2019).
[7] M. Serbyn, D. A. Abanin, and Z. Papić, Quantum many-body scars and weak breaking of ergodicity, Nat. Phys. **17**, 675 (2021).
[8] S. Moudgalya, B. A. Bernevig, and N. Regnault, Quantum many-body scars and Hilbert space fragmentation: a review of exact results, arXiv:2109.00548.
[9] J. Choi, A. L. Shaw, I. S. Madjarov, X. Xie, J. P. Covey, J. S. Cotler, D. K. Mark, H.-Y. Huang, A. Kale, H. Pichler, F. G. S. L. Brandão, S. Choi, and M. Endres, Emergent randomness and benchmarking from many-body quantum chaos, arXiv:2103.03535.
[10] J. S. Cotler, D. K. Mark, H.-Y. Huang, F. Hernandez, J. Choi, A. L. Shaw, M. Endres, and S. Choi, Emergent quantum state designs from individual many-body wave functions, arXiv:2103.03536.
[11] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, Quantum data hiding, IEEE Trans. Inf. Theory **48**, 580 (2002).
[12] A. Ambainis and J. Emerson, Quantum t-designs: t-wise independence in the quantum world, in *2007 22nd Annual IEEE Conference on Computational Complexity* (IEEE Computer Society, Los Alamitos, CA, USA, 2007), pp. 129–140.
[13] D. Gross, K. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, J. Math. Phys. (N.Y.) **48**, 052104 (2007).
[14] D. A. Roberts and B. Yoshida, Chaos and complexity by design, J. High Energy Phys. 04 (2017) 121.
[15] B. Bertini, P. Kos, and T. Prosen, Exact Spectral form Factor in a Minimal Model of Many-Body Quantum Chaos, Phys. Rev. Lett. **121**, 264101 (2018).
[16] 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, Phys. Rev. A **77**, 012307 (2008).
[17] E. Magesan, J. M. Gambetta, and J. Emerson, Scalable and Robust Randomized Benchmarking of Quantum Processes, Phys. Rev. Lett. **106**, 180504 (2011).
[18] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Efficient Quantum Pseudorandomness, Phys. Rev. Lett. **116**, 170502 (2016).
[19] G. Alagic, T. Gagliardoni, and C. Majenz, Unforgeable quantum encryption, in *Advances in Cryptology—EUROCRYPT 2018*, edited by J. B. Nielsen and V. Rijmen (Springer International Publishing, Cham, 2018), pp. 489–519.
[20] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling, Nat. Phys. **15**, 159 (2019).
[21] J. Haferkamp, D. Hangleiter, A. Bouland, B. Fefferman, J. Eisert, and J. Bermejo-Vega, Closing Gaps of a Quantum Advantage with Short-Time Hamiltonian Dynamics, Phys. Rev. Lett. **125**, 250501 (2020).
[22] J. Radhakrishnan, M. Rötteler, and P. Sen, Random measurement bases, quantum state distinction and applications to the hidden subgroup problem, Algorithmica **55**, 490 (2009).
[23] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Randomizing quantum states: Constructions and applications, Commun. Math. Phys. **250**, 371 (2004).
[24] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acín, and M. Lewenstein, Random Bosonic States for Robust Quantum Metrology, Phys. Rev. X **6**, 041044 (2016).
[25] S. Kimmel and Y.-K. Liu, Phase retrieval using unitary 2-designs, *2017 International Conference on Sampling*

Theory and Applications (SampTA) (IEEE, New York, 2017), 10.1109/SAMPTA.2017.8024414.

[26] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, Nat. Phys. **16**, 1050 (2020).

[27] Y. Nakata, D. Zhao, T. Okuda, E. Bannai, Y. Suzuki, S. Tamiya, K. Heya, Z. Yan, K. Zuo, S. Tamate, Y. Tabuchi, and Y. Nakamura, Quantum circuits for exact unitary t-designs and applications to higher-order randomized benchmarking, PRX Quantum **2**, 030339 (2021).

[28] D. Aharonov, J. Cotler, and X.-L. Qi, Quantum algorithmic measurement, arXiv:2101.04634.

[29] H.-Y. Huang, R. Kueng, and J. Preskill, Information-Theoretic Bounds on Quantum Advantage in Machine Learning, Phys. Rev. Lett. **126**, 190505 (2021).

[30] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.128.060601 for details of statements and proofs presented in the main text, which includes Refs. [10,14,15,31–35].

[31] R. Raussendorf and Hans J. Briegel, A One-Way Quantum Computer, Phys. Rev. Lett. **86**, 5188 (2001).

[32] B. Bertini, P. Kos, and T. Prosen, Entanglement Spreading in a Minimal Model of Maximal Many-Body Quantum Chaos, Phys. Rev. X **9**, 021033 (2019).

[33] R. Goodman and N. R. Wallach, *Representations and Invariants of the Classical Groups* (Cambridge University Press, Cambridge, England, 1998).

[34] I. Marvian and R. W. Spekkens, A generalization of schur-weyl duality with applications in quantum estimation, Commun. Math. Phys. **331**, 431 (2014).

[35] J. Preskill, Caltech lecture notes for physics 219/computer science 219 quantum computation course (2020), http://theory.caltech.edu/~preskill/ph229/notes/chap6.pdf.

[36] M. Akila, D. Waltner, B. Gutkin, and T. Guhr, Particle-time duality in the kicked ising spin chain, J. Phys. A **49**, 375101 (2016).

[37] I.e., W is proportional to an isometry, $WW^\dagger \propto \mathbb{I}_{2^{N_A}}$.

[38] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, Commun. Math. Phys. **346**, 397 (2016).

[39] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics, Phys. Rev. X **7**, 021006 (2017).

[40] A result by Ref. [41] further guarantees such products when infinitely long become uniformly distributed over the unitary group, though we do not use this in our proof.

[41] J. Emerson, E. Livine, and S. Lloyd, Convergence conditions for random quantum circuits, Phys. Rev. A **72**, 060302(R) (2005).

[42] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell *et al.*, Quantum supremacy using a programmable superconducting processor, Nature (London) **574**, 505 (2019).