

RECEIVED: November 10, 2016

REVISED: January 28, 2017

ACCEPTED: March 28, 2017

PUBLISHED: April 20, 2017

Chaos and complexity by design

Daniel A. Roberts^{a,b} and Beni Yoshida^c

^aCenter for Theoretical Physics and Department of Physics,
Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, U.S.A.

^bSchool of Natural Sciences, Institute for Advanced Study,
Princeton, NJ 08540, U.S.A.

^cPerimeter Institute for Theoretical Physics,
Waterloo, Ontario N2L 2Y5, Canada

E-mail: roberts@ias.edu, byoshida@perimeterinstitute.ca

ABSTRACT: We study the relationship between quantum chaos and pseudorandomness by developing probes of unitary design. A natural probe of randomness is the “frame potential,” which is minimized by unitary k -designs and measures the 2-norm distance between the Haar random unitary ensemble and another ensemble. A natural probe of quantum chaos is out-of-time-order (OTO) four-point correlation functions. We show that the norm squared of a generalization of out-of-time-order $2k$ -point correlators is proportional to the k th frame potential, providing a quantitative connection between chaos and pseudorandomness. Additionally, we prove that these $2k$ -point correlators for Pauli operators completely determine the k -fold channel of an ensemble of unitary operators. Finally, we use a counting argument to obtain a lower bound on the quantum circuit complexity in terms of the frame potential. This provides a direct link between chaos, complexity, and randomness.

KEYWORDS: AdS-CFT Correspondence, Gauge-gravity correspondence, Random Systems, Holography and condensed matter physics (AdS/CMT)

ARXIV EPRINT: [1610.04903](https://arxiv.org/abs/1610.04903)

Contents

1	Introduction	2
2	Measures of Haar	9
3	Measures of chaos and design	15
3.1	Chaos and k -designs	16
3.2	Frame potentials	18
3.3	Ensemble vs. time averages	20
4	Measures of complexity	22
4.1	Discrete ensembles	23
4.2	Continuous ensembles	25
5	Measures of correlators	27
5.1	Haar random averages	27
5.2	Dissipation vs. scrambling	31
6	Discussion	33
6.1	Generalized frame potentials and designs	35
A	More proofs	39
A.1	Proof of theorem 2	39
A.2	Proof of eq. (5.33)	40
B	More orthogonal states	41
C	More complexity bounds	42
C.1	Circuit depth	42
C.2	Early times	43
D	More Haar random averages	43
D.1	8-point functions	44
D.2	Higher-point functions	47
E	More (general) frame potentials	49
F	More chaos in quantum channels	54
F.1	OTO correlators and black holes as mirrors	54
F.2	Operational interpretation	56
F.3	Rényi- k entropy	58

1 Introduction

Random unitary operators have often been used to approximate chaotic dynamics. Notably, in the context of black holes Hayden and Preskill used a model of random dynamics to show such systems can be efficient information scramblers; initially localized information will quickly thermalize and become thoroughly mixed across the entire system [1]. It was later conjectured [2] and then proven [3, 4] that black holes are the fastest scramblers in nature, suggesting their dynamics must have much in common with random unitary evolution. Such “scrambling” is a byproduct of strongly-coupled chaotic dynamics [5–7], and so the work of [1] suggests there should be strong quantitative connection between such chaos and pseudorandomness.¹

The connection between pseudorandomness and chaotic dynamics can also be understood at the level of operators. For example, consider W a local operator of low weight (e.g. a Pauli operator acting on a single spin). With a chaotic Hamiltonian H , the operator $W(t) = e^{iHt} W e^{-iHt}$ will be a complicated nonlocal operator that has an expansion as a sum of products of many local operators with an exponential number of terms each with a pseudorandom coefficient [13]. We can gain intuition for this by considering the Baker-Campbell-Hausdorff expansion of $W(t)$

$$W(t) = \sum_{j=0}^{\infty} \frac{(it)^j}{j!} \underbrace{[H, \dots [H, W]}_j \dots \underbrace{]}_j. \tag{1.1}$$

If H is q -local and sufficiently “generic” to contain all possible q -local interactions, then the j th term will consist of a sum of roughly $\sim (n/q)^{qj}$ terms each of weight ranging from 1 to $\sim j(q-1)$, where we assume the system consists of n spins so that the Hilbert space is of dimension $d = 2^n$:

- At roughly $j \sim n/(q-1)$, there will be many terms in the sum of weight n . These terms are delocalized over the entire system. For a system without spatial locality, the relationship between time t and when the j th term becomes $O(1)$ is roughly $t \sim \log j$. The timescale $t \sim O(\log n)$ for the operator to cover the entire system is indicative of fast-scrambling behavior.
- At around $j \sim 2n/q \log(n/q)$, the total number of terms will reach 2^{2n} , equal to the total number of orthogonal linear operators acting on the Hilbert space.² Even after the operator covers the entire system, it continues to spread over the unitary group (though possibly only until a time roughly $O(\log n) + \text{a constant}$).

¹Scrambling has a close connection to the decoupling theorem, see e.g. [8, 9]. Also, see [10–12] for studies connecting randomness to entanglement.

²The number of terms is actually not a well defined quantity, since it can change under local rotations of spin, and should possibly instead consider the minimum number of terms under all local changes of basis. For chaotic systems, the distinction should not be important, since there will not exist a local change of basis where the number of terms drastically simplifies. We thank Douglas Stanford who thanks Juan Maldacena for raising this point.

Furthermore, the coefficient of any given term will be incredibly complicated, depending on the details of the path through the interaction graph and the time. Over time, $W(t)$ should cover the entire unitary group (possibly quotiented by a group set by the symmetries of the Hamiltonian). At sufficiently large t , one might even suspect that for many purposes $W(t)$ can be approximated by a random operator $\tilde{W} \equiv U^\dagger W U$, with U sampled randomly from the unitary group.³ If this is true, then we would say that $W(t)$ behaves pseudorandomly.

Chaos

This pattern of growth of $W(t)$ can be measured by a second local operator V . For example, the group commutator of $W(t)$ with V , given by $W(t)^\dagger V^\dagger W(t) V$, measures the effect of the small perturbation V on a later measurement of W . In other words, it is a measure of the butterfly effect and the strength of chaos:

- If $W(t)$ is of low weight and few terms, then $W(t)$ and V approximately commute $[W(t), V] \approx 0$, and the operator $W(t)^\dagger V^\dagger W(t) V$ is close to the identity.
- If instead the dynamics are strongly chaotic, $W(t)$ will grow to eventually have a large commutator with all other local operators in the system (in fact, just about all other operators), and so $W(t)^\dagger V^\dagger W(t) V$ will be nearly random and have a small expectation in most states.

Thus, the decay of out-of-time-order (OTO) four-point functions of the form

$$\langle W(t)^\dagger V^\dagger W(t) V \rangle = \langle U(t)^\dagger W^\dagger U(t) V^\dagger U(t)^\dagger W U(t) V \rangle, \tag{1.2}$$

can act as a simple diagnostic of quantum chaos, where $U(t) = e^{-iHt}$ is the unitary time evolution operator, and the correlator is usually evaluated on the thermal state $\langle \cdot \rangle \equiv \text{tr} \{ e^{-\beta H} \cdot \} / \text{tr} e^{-\beta H}$ [3, 4, 6, 14, 15].⁴ For further discussion, please see a selection (but by all means not a complete set) of recent work on out-of-time-order four-point functions and chaos [3, 4, 7, 13, 15–31].

For sufficiently chaotic systems and sufficiently large times, the correlators eq. (1.2) will reach a floor value equivalent to the substitution, $W(t) \rightarrow U^\dagger W U$ with U chosen randomly. Furthermore, it can be shown [7] that the decay of correlators eq. (1.2) implies the sort of information-theoretic scrambling studied by Hayden and Preskill in [1]. This explains why the random dynamics model of [1] was such a good approximation for strongly-chaotic systems, such as black holes. However, are out-of-time-order four-point functions eq. (1.2) actually a sufficient diagnostic of chaos?

In [1] the authors did not actually require the dynamics to be a uniformly random unitary operator sampled from the Haar measure on the unitary group. Instead, it would have been sufficient to sample from a simpler ensemble of operators that could reproduce

³Of course, for a less generic and sparser Hamiltonian e.g. a free system, the expansion of $W(t)$ will organize itself in a way such that the commutator in eq. (1.1) does not produce an exponential number of terms. Said another way, the terms in the expansion of $W(t)$ will only cover a small subset of the unitary group, and the assumption of uniform randomness will not hold.

⁴Usually W, V are taken to be Hermitian, but here we will more generally allow them to be unitary.

only a few moments of the larger Haar ensemble.⁵ Of course, there may be other finer-grained information theoretic properties of a system that are dependent on higher moments and would require a larger ensemble to replicate the statistics of the Haar random dynamics. If random dynamics is a valid approximation for computing some, but not all, of these finer-grained quantities then they can represent a measure of the degree of pseudorandomness of the underlying dynamics. In this paper, we will make some progress in developing some of these finer-grained quantities and therefore connect measures of chaos to measures of randomness.

Unitary design

The extent to which an ensemble of operators behaves like the uniform distribution can be quantified by the notion of unitary k -designs [32–36].⁶ A unitary k -design is a subset of the unitary group that replicates the statistics of at least k moments of the distribution. Consider a finite-dimensional Hilbert space $\mathcal{H}^{\otimes k} = (\mathbb{C}^d)^{\otimes k}$ consisting of k copies of $\mathcal{H} = \mathbb{C}^d$. Given an ensemble of unitary operators $\mathcal{E} = \{p_j, U_j\}$ acting on \mathcal{H} with probability distribution p_j , the ensemble \mathcal{E} is a unitary k -design if and only if

$$\sum_j p_j \underbrace{(U_j \otimes \cdots \otimes U_j)}_k \rho \underbrace{(U_j^\dagger \otimes \cdots \otimes U_j^\dagger)}_k = \int_{\text{Haar}} dU \underbrace{(U \otimes \cdots \otimes U)}_k \rho \underbrace{(U^\dagger \otimes \cdots \otimes U^\dagger)}_k, \quad (1.3)$$

for all quantum states ρ in $\mathcal{H}^{\otimes k}$. Therefore, whether or not a given ensemble \mathcal{E} forms at most a k -design is a fine-grained notion of the randomness of the ensemble.⁷

Inspection of eq. (1.2) suggests that a 2-design is sufficient for OTO four-point functions to decay. This was also the requirement for a system to appear scrambled [1, 2, 49]. However, the four-point functions eq. (1.2) are not the only observables related to chaos and the butterfly effect. In an attempt to understand the geometry and interior of a typical microstate of a holographic black hole, Shenker and Stanford constructed a series of black hole geometries by making multiple perturbations of an essentially maximally entangled state [16]. While they were unfortunately unsuccessful at constructing a generic microstate, studying correlation functions in these geometries leads one to a family of $2k$ -point out-of-time-order correlation functions of the form

$$\langle \mathcal{W}^\dagger V(0)^\dagger \mathcal{W} V(0) \rangle = \langle W_1(t_1)^\dagger \cdots W_{k-1}(t_{k-1})^\dagger V(0)^\dagger W_{k-1}(t_{k-1}) \cdots W_1(t_1) V(0) \rangle, \quad (1.4)$$

where $V(0)$ and the $W_j(0)$ are local operators, and $\mathcal{W} \equiv W_{k-1}(t_{k-1}) \cdots W_1(t_1)$ is a composite operator that lets us understand how the correlator is organized. The existence of these correlators begs the question: do these contain any additional information about the system or are they redundant with the four-point functions? The fact that the correlators eq. (1.4) involve many more copies of unitary time evolution, suggests a relationship between higher-point functions and unitary design. In fact, we will show that a generalization of the OTO higher-point correlators eq. (1.4) are probes of unitary design.

⁵Inspection of eq. (1.2) suggests that only two moments are required since there are only two copies of U and two copies of U^\dagger in the correlator. We will explain this more carefully in the rest of the paper.

⁶N.B. in the literature, these are often referred to as unitary t -designs. Here, we will reserve t for time. For recent work on unitary designs, see [1, 9, 33, 37–48].

⁷With this definition, a $k + 1$ -design is automatically a k -design.

Complexity

Probes of chaos and unitary design can only indirectly address a sharp question of recent interest in holography: the existence and growth of the black hole interior via the time evolution of the state. To be precise, one cannot make use of unitary designs since evolution by a time-independent Hamiltonian does not define any ensemble. However, even in this setting we still expect that higher-point OTO should be able to see fine-grained properties of time evolved states that are not captured by four-point OTO correlators.

One fine-grained quantity is the quantum circuit complexity of a quantum state $|\psi(t)\rangle = U(t)|\psi(0)\rangle$. Consider a simple initial state, such as the product state $|\psi(0)\rangle = |0\rangle^{\otimes n}$, undergoing chaotic time evolution. After a short time thermalization time of $O(1)$, the system will evolve to an equilibrium in which local quantities will reach their thermodynamic values. Next, after the scrambling time of $O(\log n)$, the initial state $|\psi(0)\rangle$ will be forgotten: the information will be distributed in such a way that measurements of even a large number of collections of local quantities of $|\psi(t)\rangle$ will not reveal the initial state. However, even after the scrambling time, the quantum circuit complexity of the time-evolved state $|\psi(t)\rangle$, as quantified by the number of elementary quantum gates necessary to reach it from the initial product state, will continue to evolve. In fact, it is expected to keep growing linearly in time until it saturates at a time exponential in the system size $e^{O(n)}$ [50, 51].

We hope this presents an intuitive picture that chaos, pseudorandomness, and quantum circuit complexity should be related. To that end, having first established a connection between higher-point out-of-time-order correlators and pseudorandomness, we will next connect the randomness of an ensemble to computational complexity. Finally, we will use correlation functions to probe pseudorandomness by comparing different random averages to expectations from time evolution.

Below, we will summarize our main results, deferring the technical statements to the body and appendices.

Main results

We will focus on a particular form of $2k$ -point correlation functions evaluated on the maximally mixed state $\rho = \frac{1}{d}I$

$$\langle A_1 U^\dagger B_1 U \cdots A_k U^\dagger B_k U \rangle := \frac{1}{2^n} \text{tr} \{ A_1 U^\dagger B_1 U \cdots A_k U^\dagger B_k U \}, \quad (1.5)$$

where any of the A_j, B_j may be a product Pauli operators that act on a single spin.⁸ Note that each of the B_j is conjugated by the same unitary U (which is similar to picking all the time arguments in eq. (1.4) to be either 0 or t). Furthermore, U will not necessarily represent Hamiltonian time evolution, and instead we will let U be sampled from some ensemble.⁹ From this point forward, we will use the notation

$$\tilde{B} \equiv U^\dagger B U, \quad (1.6)$$

⁸To be clear, this means that the operators we are correlating are not necessarily simple or local.

⁹As a result, these correlators are not really out-of-time-order, since there may not be a notion of time. Instead, they are probably more accurately called *out-of-complexity-order* (OCO) since we might generalize

to simplify expressions involving unitary conjugation. Therefore, we can represent the ensemble average of OTO $2k$ -point correlation functions as

$$\langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle_{\mathcal{E}} := \int_{\mathcal{E}} dU \langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle, \quad (1.7)$$

where the integral is with respect to the probability distribution in an ensemble of unitary operators $\mathcal{E} = \{p_j, U_j\}$. Finally, the k -fold channel over the ensemble \mathcal{E} is

$$\Phi_{\mathcal{E}}^{(k)}(\cdot) = \int_{\mathcal{E}} dU (U_j \otimes \cdots \otimes U_j)(\cdot)(U_j^\dagger \otimes \cdots \otimes U_j^\dagger), \quad (1.8)$$

which is a superoperator.

Chaos and k -designs

First, we will prove a theorem stating that a particular set of $2k$ -point OTO correlators, averaged over an ensemble \mathcal{E} , is in a one-to-one correspondence with the k -fold channel $\Phi_{\mathcal{E}}^{(k)}$

$$2k\text{-point OTO correlators} \leftrightarrow k\text{-fold channel } \Phi_{\mathcal{E}}^{(k)}, \quad (1.9)$$

and we provide a simple formula to convert from one to the other. Such an explicit relation between OTO correlators and the k -fold channel may have practical and experimental applications such as statistical testing (e.g. a quantum analog of the χ^2 -test) and randomized bench marking [40].

Next, we prove that generic ‘‘smallness’’ of $2k$ -point OTO correlators implies that the ensemble \mathcal{E} is close to k -design. We will make this statement precise by relating OTO correlators to a useful quantity known as the frame potential

$$F_{\mathcal{E}}^{(k)} = \frac{1}{|\mathcal{E}|^2} \sum_{U, V \in \mathcal{E}} |\text{tr}\{U^\dagger V\}|^{2k}. \quad (1.10)$$

This quantity, first introduced in [45], measures the (2-norm) distance between $\Phi_{\mathcal{E}}^{(k)}(\cdot)$ and $\Phi_{\text{Haar}}^{(k)}(\cdot)$, and has been shown to be minimized if and only if the ensemble \mathcal{E} is k -design. We will derive the following formula:

$$\text{Average of } |2k\text{-point OTO correlator}|^2 \propto k\text{th frame potential } F_{\mathcal{E}}^{(k)}, \quad (1.11)$$

which shows that $2k$ -point OTO correlators $\langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle_{\mathcal{E}}$ are measures of whether an ensemble \mathcal{E} is a unitary k -design. Thus, the decay of OTO correlators can be used to quantify an increase in pseudorandomness.

the notion of time ordering to complexity ordering, where we put unitaries of smaller complexity to the right of unitaries of larger complexity. In order to (hopefully) avoid confusion, we will continue to call the $2k$ -point functions in eq. (1.5) out-of-time-order, despite there not necessarily being a notion of time.

Chaos, randomness, and complexity

We prove a lower bound on quantum circuit complexity needed to generate an ensemble of unitary operators \mathcal{E}

$$\text{Complexity of } \mathcal{E} \geq \frac{2kn \log(2) - \log F_{\mathcal{E}}^{(k)}}{\log(\text{choices})}. \tag{1.12}$$

This bound is actually given by a rather simple counting argument. The denominator should be thought of as (the log of) the number of choices made at each step in generating the circuit. For instance, if we have a set \mathcal{G} of cardinality g of q -qubit quantum gates available and at each step randomly select q qubits out of n total and select one of the gates in \mathcal{G} to apply, then we would make $g \binom{n}{q}$ choices at each step. Recalling our result relating OTO correlators and the frame potential, this result implies that generic smallness of OTO correlators leads to higher quantum circuit complexity. This is a direct and quantitative link between chaos and complexity.

However, we caution the reader that in many cases eq. (1.12) may not be a very tight lower bound. We will provide some discussion of this point as well as a few examples, however further work is most likely required to better understand the utility of this bound.

Haar vs. simpler ensemble averages

Finally, we present calculations of the Haar average of some higher-point OTO correlators and compare them to averages in simpler ensembles. These results suggest that the floor value of OTO correlators of local operators might be good diagnostics of pseudorandomness.

For 4-point OTO correlators, we find

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Haar}} = \langle AC \rangle \langle B \rangle \langle D \rangle + \langle A \rangle \langle C \rangle \langle BD \rangle - \langle A \rangle \langle C \rangle \langle B \rangle \langle D \rangle - \frac{1}{d^2 - 1} \langle\langle AC \rangle\rangle \langle\langle BD \rangle\rangle, \tag{1.13}$$

where $\langle\langle AC \rangle\rangle$ represents a connected correlator and $d = 2^n$ is the total number of states. In contrast, if the U are averaged over the Pauli operators (which form a 1-design but not a 2-design), we find

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Pauli}} = \langle AC \rangle \langle BD \rangle. \tag{1.14}$$

We will present intuitive explanations on this difference from the viewpoint of local thermal dissipations vs. global thermalization or scrambling.

For 8-point OTO correlators with Pauli operators A, B, C, D , we compute averages over the unitary group and the Clifford group (which form a 3-design on qubits but not a 4-design)

$$\begin{aligned} \langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger \rangle_{\text{Haar}} &\sim \frac{1}{d^4}, \\ \langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger \rangle_{\text{Clifford}} &\sim \frac{1}{d^2}. \end{aligned} \tag{1.15}$$

This suggests that forming a higher k -design leads to a lower value of the correlator.

The results eq. (1.13)–(1.15) are exact for any choice of operators. (The extended results for the correlators in eq. (1.15) is presented in appendix D.1.) However, for a particular ordering of OTO $4m$ -point functions where we average over choices of operators, we will also show that a Haar averaging over the unitary group scales as

$$\text{OTO}^{(4m)} \sim \frac{1}{d^{2m}}. \quad (1.16)$$

This result hints that these correlators continue to be probes of increasing pseudorandomness.

Organization of the paper

For convenience of the reader, we included a(n almost) self-contained introduction to Haar random unitary operators and unitary design in section 2. In section 3, we establish a formal connection between chaos and unitary design by proving the theorems mentioned above. In section 4, we connect complexity to unitary design by proving the complexity lower bound (1.12). In section 5, we include the explicit calculations of 2-point and 4-point functions averaged over different ensembles and discuss how these averages relate to expectations from time evolution with chaotic Hamiltonians. We also discuss results and expectations for higher-point functions. We conclude in section 6 with an extended discussion of these results, their relevance for physical situations, and outline some future research directions.

Despite page counting to the contrary, this is actually a short paper. A knowledgeable reader may learn our results by simply reading section 3, section 4 and section 5. On the other hand, a large number of extended calculations and digressions are relegated to the appendices:

- In section A, we collect some proofs that we felt interrupted the flow of the main discussion.
- In section B, we discuss the number of nearly orthogonal states in large-dimensional Hilbert spaces.
- In section C, we extend our complexity lower bound to minimum circuit depth by considering gates that may be applied in parallel. We also derive a bound on early-time complexity for evolution with an ensemble of Hamiltonians.
- In section D, we hide the details of our 8-point functions Haar averages and also derive the $\sim d^{-2m}$ scaling of Haar averages of certain $4m$ -point functions.
- In section E, we provide a generalization of the frame potential that equals an average of the square of OTO correlators for arbitrary states rather than just the maximally mixed state.
- Finally, in section F we prove some extended results relating to our earlier work [7] that are somewhat outside the main focus of the current paper.

2 Measures of Haar

The goal of this section is to provide a review of the theory of Haar random unitary operators and unitary design in a self-contained manner. The presentation of this section owes a lot to a recent paper by Webb [43] as well as a course note by Kitaev [52].¹⁰

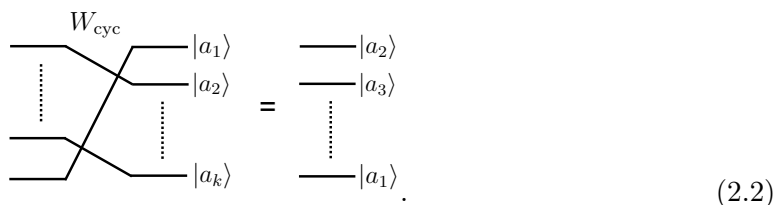
Haar random unitaries

Schur-Weyl duality

Consider a finite-dimensional Hilbert space $\mathcal{H}^{\otimes k} = (\mathbb{C}^d)^{\otimes k}$ consisting of k copies of $\mathcal{H} = \mathbb{C}^d$. A permutation operator W_π with a permutation $\pi = \pi(1) \dots \pi(k)$ is defined as follows

$$W_\pi |a_1, \dots, a_k\rangle = |a_{\pi(1)}, \dots, a_{\pi(k)}\rangle, \tag{2.1}$$

and $W_\pi(A_1 \otimes \dots \otimes A_k)W_\pi^{-1} = A_{\pi(1)} \otimes \dots \otimes A_{\pi(k)}$. If π is a cyclic permutation ($\pi(j) = j+1$), then W_{cyc} acts as follows



Theorem 1. [Schur-Weyl duality] *Let $L(\mathcal{H}^{\otimes k})$ be the algebra of all the operators acting on $\mathcal{H}^{\otimes k}$. Let $U(\mathcal{H})$ be the unitary group on \mathcal{H} . An operator $A \in L(\mathcal{H}^{\otimes k})$ commutes with all operators $V^{\otimes k}$ with $V \in U(\mathcal{H})$ if and only if A is a linear combination of permutation operators W_π*

$$[A, V^{\otimes k}] = 0, \forall V \Leftrightarrow A = \sum_{\pi \in S_k} c_\pi \cdot W_\pi. \tag{2.3}$$

When an operator A is a linear combination of permutation operators, it is clear that A commutes with $V^{\otimes k}$ (\Leftarrow). A difficult part is to prove the converse (\Rightarrow), which relies on Von Neumann’s double commutant theorem.

Pauli operators

Pauli operators for \mathbb{C}^d (i.e. d -state spins or qudits) are defined by

$$X|j\rangle = |j+1\rangle, \quad Z|j\rangle = \omega^j|j\rangle, \tag{2.4}$$

where $\omega \equiv e^{2\pi i/d}$. We note that eq. (2.4) implies $ZX = \omega XZ$ and $X^d = Z^d = I$, and that for $d > 2$, the Pauli operators are unitary and traceless, but not Hermitian.

¹⁰We also would like to highlight a Master’s thesis by Yinzheng Gu, which considers a certain matrix multiplication problem with conjugations by Haar random unitary operators. Although not directly relevant to the work, these are actually out-of-time-order correlation functions in a disguised form [53].

where the integral is taken over the Haar measure. Note, this is sometimes referred to as the k -fold twirl of A . The Haar measure is the unique probability measure on the unitary group that is both left-invariant and right-invariant [54]

$$\int_{\text{Haar}} dU = 1, \quad \int_{\text{Haar}} f(VU)dU = \int_{\text{Haar}} f(UV)dU = \int_{\text{Haar}} f(U)dU, \quad (2.12)$$

for all $V \in U(\mathcal{H})$, where f is an arbitrary function. If we take $f(U) = (U^{\otimes k})^\dagger A U^{\otimes k}$, then we can show that the twirl of A is invariant under k -fold unitary conjugation,

$$(V^{\otimes k})^\dagger (\Phi_{\text{Haar}}^{(k)}(A)) V^{\otimes k} = \int_{\text{Haar}} f(UV)dU = \Phi_{\text{Haar}}^{(k)}(A), \quad (2.13)$$

and that twirl of the k -fold unitary conjugation of A equals the twirl of A

$$\Phi_{\text{Haar}}^{(k)}((V^{\otimes k})^\dagger A V^{\otimes k}) = \int_{\text{Haar}} f(VU)dU = \Phi_{\text{Haar}}^{(k)}(A), \quad (2.14)$$

where for eq. (2.13) we used the right-invariance property, and for eq. (2.14) we used left-invariance.

Weingarten function

The content of eq. (2.13) is that $\Phi_{\text{Haar}}^{(k)}(A)$ commutes with all operators $V^{\otimes k}$. Thus, we may use the Schur-Weyl duality eq. (2.3) to rewrite it as

$$\Phi_{\text{Haar}}^{(k)}(A) = \sum_{\pi \in S_k} W_\pi \cdot u_\pi(A). \quad (2.15)$$

Here, S_k is the permutation group, and $u_\pi(A)$ is some linear function of A . Since $u_\pi(A)$ is a linear function, it can be written as

$$u_\pi(A) = \text{tr}\{C_\pi A\}, \quad (2.16)$$

for some operators C_π . From eq. (2.14), we find that C_π commutes with all operators $V^{\otimes k}$. Then again, by the Schur-Weyl duality, we have

$$\Phi_{\text{Haar}}^{(k)}(A) = \sum_{\pi, \sigma \in S_k} c_{\pi, \sigma} W_\pi \text{tr}\{W_\sigma A\}. \quad (2.17)$$

The coefficients $c_{\pi, \sigma}$ are called the Weingarten matrix [55]. Since $\Phi_{\text{Haar}}^{(k)}(W_\lambda) = W_\lambda$, we have $W_\lambda = \sum_{\pi, \sigma} c_{\pi, \sigma} W_\pi \text{tr}\{W_\sigma W_\lambda\}$. Recalling that $\text{tr}\{W_\sigma W_\lambda\} = d^{\#\text{cycles}(\sigma\lambda)}$, we have

$$\delta_{\pi, \lambda} = \sum_{\sigma \in S_k} c_{\pi, \sigma} Q_{\sigma, \lambda}, \quad Q_{\sigma, \lambda} := d^{\#\text{cycles}(\sigma\lambda)}. \quad (2.18)$$

So finally, we find

$$\Phi_{\text{Haar}}^{(k)}(A) = \sum_{\pi, \sigma \in S_k} (Q^{-1})_{\pi, \sigma} W_\pi \cdot \text{tr}\{W_\sigma A\}. \quad (2.19)$$

Here, we assumed the presence of the inverse Q^{-1} which is guaranteed for $k \leq d$.

Examples

For $k = 1$, $Q_{I,I} = d$, so one has

$$\Phi_{\text{Haar}}^{(1)}(A) = \frac{1}{d} \text{tr}\{A\}. \quad (2.20)$$

For $k = 2$, so one has

$$Q = \begin{pmatrix} Q_{I,I} & Q_{I,S} \\ Q_{S,I} & Q_{S,S} \end{pmatrix} = \begin{pmatrix} d^2 & d \\ d & d^2 \end{pmatrix} \quad C = \begin{pmatrix} C_{I,I} & C_{I,S} \\ C_{S,I} & C_{S,S} \end{pmatrix} = \begin{pmatrix} \frac{1}{d^2-1} & \frac{-1}{d(d^2-1)} \\ \frac{-1}{d(d^2-1)} & \frac{1}{d^2-1} \end{pmatrix}. \quad (2.21)$$

Explicitly, we have

$$\Phi_{\text{Haar}}^{(2)}(A) = \frac{1}{d^2-1} \left(I \text{tr}\{A\} + S \text{tr}\{SA\} - \frac{1}{d} S \text{tr}\{A\} - \frac{1}{d} I \text{tr}\{SA\} \right), \quad (2.22)$$

where S is the SWAP operator.

Haar random states

We can also consider the k -fold average of a Haar random state. Define a random state by $|\psi\rangle = U|0\rangle$, where U is sampled uniformly from the unitary group. Then, we have

$$\int_{\text{Haar}} (|\psi\rangle\langle\psi|)^{\otimes k} d\psi := \Phi_{\text{Haar}}^{(k)}(|0\rangle\langle 0|)^{\otimes k} = \sum_{\pi} c_{\pi} W_{\pi}, \quad (2.23)$$

for some coefficients c_{π} . Since $\int_{\text{Haar}} (|\psi\rangle\langle\psi|)^{\otimes k}$ commutes with $V^{\otimes k}$, we again decomposed it with permutation operators. Furthermore, one has

$$W_{\pi} \int_{\text{Haar}} (|\psi\rangle\langle\psi|)^{\otimes k} = \int_{\text{Haar}} (|\psi\rangle\langle\psi|)^{\otimes k}, \quad \forall \pi \in S_k \quad (2.24)$$

which implies $c_{\pi} = c$ for all π . By taking the trace in eq. (2.23), we have

$$c_{\pi} = \frac{1}{\sum_{\pi \in S_k} d^{\#\text{cycles}(\pi)}} = \frac{k!}{\binom{k+d-1}{k}}. \quad (2.25)$$

Defining the projector onto the symmetric subspace as $\Pi_{\text{sym}} = \frac{1}{k!} \sum_{\pi \in S_k} W_{\pi}$, one has

$$\int_{\text{Haar}} (|\psi\rangle\langle\psi|)^{\otimes k} d\psi = \frac{\Pi_{\text{sym}}}{\binom{k+d-1}{k}}. \quad (2.26)$$

Frame potential

In this paper, we will be particularly interested in the following quantity

$$F_{\text{Haar}}^{(k)} = \iint dU dV |\text{tr}\{U^{\dagger}V\}|^{2k}. \quad (2.27)$$

Using eq. (2.19), we can rewrite this

$$\begin{aligned} F_{\text{Haar}}^{(k)} &= \sum_{\pi_1, \pi_2, \pi_3, \pi_4 \in S_k} \text{tr}\{W_{\pi_1} W_{\pi_2}\} (Q^{-1})_{\pi_2, \pi_3} \text{tr}\{W_{\pi_3} W_{\pi_4}\} (Q^{-1})_{\pi_4, \pi_1}, \\ &= \sum_{\pi_1, \pi_2, \pi_3, \pi_4 \in S_k} Q_{\pi_1, \pi_2} (Q^{-1})_{\pi_2, \pi_3} Q_{\pi_3, \pi_4} (Q^{-1})_{\pi_4, \pi_1} = k!, \end{aligned} \quad (2.28)$$

for $k \leq d$, where we used $C = Q^{-1}$ and $|S_k| = k!$.

Unitary design

Consider an ensemble of unitary operators $\mathcal{E} = \{p_j, U_j\}$ where p_j are probability distributions such that $\sum_j p_j = 1$, and U_j are unitary operators. The action of the k -fold channel with respect to the ensemble \mathcal{E} is given by

$$\Phi_{\mathcal{E}}^{(k)}(A) := \sum_j p_j (U_j^{\otimes k})^\dagger A (U_j^{\otimes k}), \quad (2.29)$$

or for continuous distributions

$$\Phi_{\mathcal{E}}^{(k)}(A) := \int_{\mathcal{E}} dU (U^{\otimes k})^\dagger A (U^{\otimes k}). \quad (2.30)$$

The ensemble \mathcal{E} is a unitary k -design if and only if $\Phi_{\mathcal{E}}^{(k)}(A) = \Phi_{\text{Haar}}^{(k)}(A)$ for all A . Intuitively, a unitary k -design is as random as the Haar ensemble up to the k th moment. That is, a unitary k -design is an ensemble which satisfies the definition of the Haar measure in eq. (2.12) when $f(U)$ contains up to k th powers of U and U^\dagger (i.e. balanced monomials of degree at most k). By this definition, if an ensemble is k -design, then it is also $k-1$ -design. However, the converse is not true in general.

It is convenient to write the above definition of k -design in terms of Pauli operators. An ensemble \mathcal{E} is k -design if and only if $\Phi_{\mathcal{E}}^{(k)}(P) = \Phi_{\text{Haar}}^{(k)}(P)$ for all Pauli operators $P \in (\mathcal{P})^{\otimes k}$, since the Pauli operators are the basis of the operator space. Furthermore, for an arbitrary ensemble \mathcal{E}

$$\Phi_{\text{Haar}}(\Phi_{\mathcal{E}}(A)) = \Phi_{\text{Haar}}(A), \quad \forall \mathcal{E}, \quad (2.31)$$

due to the left/right-invariance of the Haar measure. By using eq. (2.31), we can derive the following useful criteria for k -designs [43]

$$\mathcal{E} \text{ is } k\text{-design} \iff \Phi_{\mathcal{E}}(P) \text{ is a linear combination of } W_\pi \text{ for all } P \in (\mathcal{P})^{\otimes k}. \quad (2.32)$$

To make use of this, we will look at some illustrative examples.

Pauli is a 1-design

The Pauli operators form a unitary 1-design. In fact, we have already shown this in with eq. (2.9). We have shown that an average over Pauli operators gives $\frac{1}{d^2} \sum_{P \in \mathcal{P}} P^\dagger A P = \frac{1}{d} \text{tr}\{A\}$, and the Haar random channel gives $\Phi_{\text{Haar}}^{(1)}(A) = \frac{1}{d} \text{tr}\{A\}$, so therefore

$$\frac{1}{d^2} \sum_{P \in \mathcal{P}} P^\dagger \rho P = \Phi_{\text{Haar}}^{(1)}(\rho), \quad (2.33)$$

for all ρ . For example, if $d = 2$ and $A = X$ (Pauli X operator), then we have

$$\frac{1}{4}(IXI + XXX + YXY + ZXZ) = X + X - X - X = 0, \quad (2.34)$$

which is consistent with $\text{tr}\{X\} = 0$.

Thus, an average over Pauli operators is equivalent to taking a trace. Since Pauli operators can be written in a tensor product form: $P_1 \otimes P_2 \otimes \dots \otimes P_n$ for a system of n qubits, they do not create entanglement between different qubits and do not scramble. Instead, they can only mix quantum information locally. This implies some kind of relationship between 1-designs and local thermalization that we will revisit in the discussion section 6.

Clifford is a 2-design

The Clifford operators form a unitary 2-design. The Clifford group \mathcal{C}_n is a group of unitary operators acting on a system of n qubits that transform a Pauli operator into another Pauli operator

$$C^\dagger P C = Q, \quad P, Q \in \tilde{\mathcal{P}}, \quad C \in \mathcal{C}_n. \quad (2.35)$$

Clearly, Pauli operators are Clifford operators, since $PQP = e^{i\theta}Q$ for any pairs of Pauli operators P, Q : Pauli operators transform a Pauli operator to itself up to a global phase. However, non-trivial Clifford operators are those which transform a Pauli operator into a different Pauli operator. An example of such an operator is the Control- Z gate

$$CZ|a, b\rangle = (-1)^{ab}|a, b\rangle, \quad a, b = 0, 1, \quad (2.36)$$

where summation is modulo 2. The conjugation of a Pauli operator with a Control- Z gate is as follows

$$X \otimes I \rightarrow X \otimes Z, \quad Z \otimes I \rightarrow Z \otimes I, \quad I \otimes X \rightarrow Z \otimes X, \quad I \otimes Z \rightarrow I \otimes Z. \quad (2.37)$$

Let us prove that the Clifford group is 2-design by using eq. (2.32) [43]. For qubit Pauli operators of the form $P \otimes P$ ($P \neq I$), the action of the Clifford 2-fold channel is

$$\sum_{C \in \mathcal{C}_n} (C^\dagger \otimes C^\dagger) P \otimes P (C \otimes C) \propto \sum_{Q \in \mathcal{P}_n, Q \neq I} Q \otimes Q, \quad (2.38)$$

because a random Clifford operator will transform P into some other non-identity Pauli operator. Recalling the definition of the swap operator $\text{SWAP} = \frac{1}{d} \sum_{P \in \mathcal{P}_n} P \otimes P$, the r.h.s. is a linear combination of $I \otimes I$ and SWAP . On the other hand, for other Pauli operators $P \otimes Q$ with $P \neq Q$, the action of the channel is

$$\sum_{C \in \mathcal{C}_n} (C^\dagger \otimes C^\dagger) P \otimes Q (C \otimes C) = 0. \quad (2.39)$$

This can be seen by rewriting the sum as

$$\frac{1}{2} \sum_{C \in \mathcal{C}_n} (C^\dagger \otimes C^\dagger) P \otimes Q (C \otimes C) + \frac{1}{2} \sum_{RC \in \mathcal{C}_n} (C^\dagger R^\dagger \otimes C^\dagger R^\dagger) P \otimes Q (RC \otimes RC), \quad (2.40)$$

since the Clifford group is invariant under element-wise multiplication by a Pauli R . Since we assumed the Pauli operators are different we have $PQ \neq I$, and thus we can pick R such that it anti-commutes with PQ . This implies $R^\dagger P R \otimes R^\dagger Q R = -P \otimes Q$, and therefore the two terms cancel. Finally, $I \otimes I$ remains invariant. Thus, since the action of the channel on Pauli operators gives a linear combination of permutation operators, by eq. (2.32) the Clifford group is a unitary 2-design.

Note that Clifford operators do not have a tensor product form, in general. This means that unlike evolution restricted to Pauli operators, they can change the sizes of an operator as seen in the Control- Z gate example eq. (2.37). In other words they can grow local operators into a global operators, indicative of the butterfly effect.

In fact, Clifford operators can prepare a large class of interesting quantum states called the stabilizer states. Let $|\psi_0\rangle = |0\rangle^{\otimes n}$ be an initial product state. This state satisfies $Z_j|\psi_0\rangle = |\psi_0\rangle$. Let U be an arbitrary Clifford operator and consider $|\psi\rangle = U|\psi_0\rangle$. This state $|\psi\rangle$ satisfies the following

$$S_j|\psi\rangle = |\psi\rangle, \quad S_j = UZ_jU^\dagger. \tag{2.41}$$

By definition, S_j are Pauli operators and will commute with each other. A quantum state that can be represented by a set of commuting Pauli operators S_j is called a stabilizer state. Examples of stabilizer states include ground states of the toric code and the perfect tensors used in construction of holographic quantum error-correcting codes [56]. The upshot is that Clifford operators can create a global entanglement and can scramble quantum information. We will return to this point again in the discussion section 6.

? is a higher-design

Currently there is no known method of constructing an ensemble which forms an exact k -design for $k \geq 4$ in a way which generalizes to large d . Instead, there are several constructions for preparing approximate k -design in an efficient manner [41, 48].

3 Measures of chaos and design

In this section, we show that $2k$ -point OTO correlators are probes of k -unitary designs. We will focus on a Hilbert space $\mathcal{H} = \mathbb{C}^d$ with $2k$ -point correlators of the following form

$$\langle A_1\tilde{B}_1 \cdots A_k\tilde{B}_k \rangle := \frac{1}{d} \text{tr} \{A_1\tilde{B}_1 \cdots A_k\tilde{B}_k\}, \tag{3.1}$$

where $\tilde{B}_j = U^\dagger B_j U$. We can think of this as a correlator evaluated in a maximally mixed or infinite temperature state $\rho = \frac{1}{d}I$. The trace can be rewritten as

$$\text{tr} \{ (A_1 \otimes \cdots \otimes A_k)(U^\dagger \otimes \cdots \otimes U^\dagger)(B_1 \otimes \cdots \otimes B_k)(U \otimes \cdots \otimes U)W_{\pi_{\text{cyc}}}\}, \tag{3.2}$$

by considering an enlarged Hilbert space $\mathcal{H}^{\otimes k}$ that consists of k copies of the original Hilbert space \mathcal{H} , where $W_{\pi_{\text{cyc}}}$ represents a cyclic permutation operator on $\mathcal{H}^{\otimes k}$. The action of W_{cyc} is to send the j th Hilbert space to the $(j + 1)$ th Hilbert space (modulo k), see figure 1 for a graphical representation.¹¹

Observe that eq. (3.2) contains a k -fold unitary action

$$(U \otimes \cdots \otimes U)(B_1 \otimes \cdots \otimes B_k)(U^\dagger \otimes \cdots \otimes U^\dagger),$$

suggesting correlators of the form eq. (3.1) have the potential to be sensitive to whether an ensemble is or is not a k -design. Unitary k -designs concern the k -fold channel of an ensemble of unitary operators

$$\Phi_{\mathcal{E}}(B_1 \otimes \cdots \otimes B_k) = \int_{\mathcal{E}} dU (U \otimes \cdots \otimes U)(B_1 \otimes \cdots \otimes B_k)(U^\dagger \otimes \cdots \otimes U^\dagger), \tag{3.3}$$

¹¹N.B. this trick of using cyclic permutation operators is similar to the method used for computing Rényi- k entanglement entropies in quantum field theories via the insertion of twist operators.

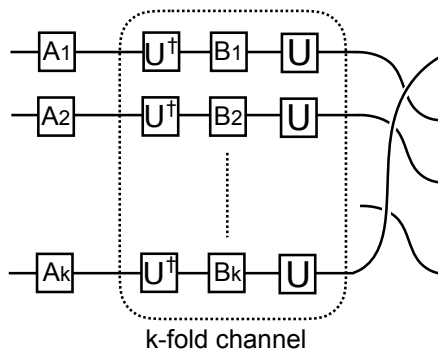


Figure 1. Schematic form of the $2k$ -point OTO correlation functions eq. (3.1), interpreted as a correlation function on the enlarged k -copied system. The dotted line diagram surrounds the k -fold channel $\Phi_{\mathcal{E}}(B_1 \otimes \cdots \otimes B_k)$, which is probed by $A_1 \otimes \cdots \otimes A_k$. (Periodic boundary conditions are implied to take the trace.)

where \mathcal{E} is an ensemble of unitary operators. To further this point, let us consider an average of these correlators over an ensemble of unitary operators \mathcal{E}

$$\left| \langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle \right|_{\mathcal{E}} := \frac{1}{d} \int_{\mathcal{E}} dU \operatorname{tr} \{ A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \}. \quad (3.4)$$

Looking back at eq. (3.2), the idea is that A_1, \dots, A_k operators probe the outcome of k -fold channel $\Phi_{\mathcal{E}}(B_1 \otimes \cdots \otimes B_k)$. Indeed, the part of figure 1 surrounded by a dotted line, is $\Phi_{\mathcal{E}}(B_1 \otimes \cdots \otimes B_k)$. Below, we will make this intuition precise by proving that this set of OTO correlators eq. (3.1) completely determine the k -fold channel $\Phi_{\mathcal{E}}^{(k)}$.

3.1 Chaos and k -designs

In this subsection, we prove that $2k$ -point OTO correlators completely determines the k -fold channel of an ensemble \mathcal{E} , denoted by $\Phi_{\mathcal{E}}^{(k)}$. To recap, we write the k -fold channel of an ensemble $\mathcal{E} = \{p_j, U_j\}$ by

$$\Phi_{\mathcal{E}}^{(k)}(\rho) = \sum_j p_j (U_j^\dagger \otimes \cdots \otimes U_j^\dagger) \rho (U_j \otimes \cdots \otimes U_j), \quad (3.5)$$

where ρ is defined over k copies of the system, $\mathcal{H}^{\otimes k}$. The map is linear, and completely-positive and trace-preserving (CPTP), i.e. a quantum channel. For simplicity of discussion, we assume that the system \mathcal{H} is made of n qubits so that $\mathcal{H} = \mathbb{C}^d$ with $d = 2^n$. The input density matrix ρ can be expanded by Pauli operators

$$\rho_{\text{in}} = \sum_{B_1, \dots, B_k} \beta_{B_1, \dots, B_k} (B_1 \otimes \cdots \otimes B_k), \quad (3.6)$$

where $\beta_{B_1, \dots, B_k} = d^{-k} \operatorname{tr} \{ (B_1^\dagger \otimes \cdots \otimes B_k^\dagger) \rho \}$. The output density matrix is given by

$$\rho_{\text{out}} = \sum_{B_1, \dots, B_k} \beta_{B_1, \dots, B_k} \Phi_{\mathcal{E}}(B_1 \otimes \cdots \otimes B_k). \quad (3.7)$$

For a given Pauli operator B_1, \dots, B_k , we would like to examine $\Phi_{\mathcal{E}}(B_1 \otimes \cdots \otimes B_k)$.

Let us fix Pauli operator B_1, \dots, B_k for the rest of the argument. Note that the output $\Phi_{\mathcal{E}}(B_1 \otimes \dots \otimes B_n)$ can be also expanded by Pauli operators

$$\Phi_{\mathcal{E}}(B_1 \otimes \dots \otimes B_k) = \sum_{C_1, \dots, C_k} \gamma_{C_1, \dots, C_k} (C_1 \otimes \dots \otimes C_k). \quad (3.8)$$

Since we have fixed $B_1 \otimes \dots \otimes B_k$, for notational simplicity we have not included B_1, \dots, B_k indices from the tensor γ . In order to characterize the k -fold channel, we need to know values of γ_{C_1, \dots, C_k} for a given B_1, \dots, B_k . We would like to show that we can determine the values of γ_{C_1, \dots, C_k} by knowing a certain collection of OTO correlators. Consider a $2k$ -point OTO correlator labeled by the set of A operators, averaged over an ensemble \mathcal{E}

$$\alpha_{A_1, \dots, A_k} = \left| \langle A_1 \tilde{B}_1 \dots A_k \tilde{B}_k \rangle_{\mathcal{E}} \right|, \quad (3.9)$$

where as always $\tilde{B}_j = U^\dagger B_j U$ and A_1, \dots, A_k are Pauli operators. As before, for simplicity of notation we have not included B_1, \dots, B_k indices on α . Now that the notation is setup, the main question is whether one can determine the coefficients γ_{C_1, \dots, C_k} from the numbers α_{A_1, \dots, A_k} .

Substituting eq. (3.8) into eq. (3.9), we see

$$\alpha_{A_1, \dots, A_k} = \frac{1}{d} \cdot M_{A_1, \dots, A_k}^{C_1, \dots, C_k} \gamma_{C_1, \dots, C_k}, \quad M_{A_1, \dots, A_k}^{C_1, \dots, C_k} = \text{tr} \{ A_1 C_1 \dots A_k C_k \}, \quad (3.10)$$

where tensor contractions are implicit following the Einstein summation convention. This shows we can compute OTO correlators α_{A_1, \dots, A_k} the coefficients defining the k -fold channel γ_{C_1, \dots, C_k} . To establish the converse, we must prove that the tensor M is invertible.

Theorem 2. Consider the tensor $M_{A_1, \dots, A_k}^{C_1, \dots, C_k}$ and its conjugate transpose $M_{C_1, \dots, C_k}^{\dagger A_1, \dots, A_k}$. Then

$$\sum_{C_1, \dots, C_k} M_{C_1, \dots, C_k}^{\dagger A_1, \dots, A_k} M_{A_1, \dots, A_k}^{C_1, \dots, C_k} = d^{2k} \cdot \delta_{A_1}^{A'_1} \dots \delta_{A_k}^{A'_k}, \quad (3.11)$$

where δ_Q^P is the delta function for Pauli operators P, Q

$$\delta_Q^P = 1, \quad (P = Q), \quad \delta_Q^P = 0, \quad (P \neq Q). \quad (3.12)$$

The proof of this theorem is sort of technical and has been relegated to appendix A.1. Thus, from the OTO correlators α_{C_1, \dots, C_k} , we can completely determine the k -fold channel γ_{A_1, \dots, A_k}

$$\gamma_{C_1, \dots, C_k} = \frac{1}{d^{2k-1}} M_{C_1, \dots, C_k}^{\dagger A_1, \dots, A_k} \alpha_{A_1, \dots, A_k}. \quad (3.13)$$

As an obvious corollary, this means that $2k$ -point OTO correlators can measure whether or not an ensemble forms k -design.

3.2 Frame potentials

In this section we introduce the *frame potential*, a single quantity that can measure whether an ensemble is a k -design. Furthermore, we show how the frame potential may be computed from OTO correlators.

Given an ensemble of unitary operators \mathcal{E} , the k th frame potential is defined by the following double sum [45]

$$F_{\mathcal{E}}^{(k)} := \frac{1}{|\mathcal{E}|^2} \sum_{U, V \in \mathcal{E}} \left| \text{tr}\{U^\dagger V\} \right|^{2k}, \tag{3.14}$$

where $|\mathcal{E}|$ denotes the cardinality of \mathcal{E} . Denote the frame potential for the Haar ensemble as $F_{\text{Haar}}^{(k)}$. Then, the following theorem holds.

Theorem 3. *For any ensemble \mathcal{E} of unitary operators,*

$$F_{\mathcal{E}}^{(k)} \geq F_{\text{Haar}}^{(k)}, \tag{3.15}$$

with equality if and only if \mathcal{E} is k -design.

The proof of this theorem is very insightful and beautiful, which we reprint from [45].

Proof. Letting $S = \int_{\mathcal{E}} (U^\dagger)^{\otimes k} \otimes U^{\otimes k} - \int_{\text{Haar}} (U^\dagger)^{\otimes k} \otimes U^{\otimes k}$, we have

$$\begin{aligned} 0 \leq \text{tr}\{S^\dagger S\} &= \int_{U \in \mathcal{E}} \int_{V \in \mathcal{E}} dU dV |\text{tr}\{U^\dagger V\}|^{2k} - 2 \int_{U \in \mathcal{E}} \int_{V \in \text{Haar}} dU dV |\text{tr}\{U^\dagger V\}|^{2k} \\ &\quad + \iint_{U, V \in \text{Haar}} dU dV |\text{tr}\{U^\dagger V\}|^{2k}. \end{aligned} \tag{3.16}$$

The first term is $F_{\mathcal{E}}^{(k)}$, and the third term is $F_{\text{Haar}}^{(k)}$ by definition. The second term is equal to $-2F_{\text{Haar}}^{(k)}$ by the left/right-invariance of the Haar measure. Thus, we see that

$$0 \leq F_{\mathcal{E}}^{(k)} - 2F_{\text{Haar}}^{(k)} + F_{\text{Haar}}^{(k)} = F_{\mathcal{E}}^{(k)} - F_{\text{Haar}}^{(k)}, \tag{3.17}$$

with equality if and only if \mathcal{E} is k -design. □

Note that we derived the minimal value of the frame potential in section 2,

$$F_{\text{Haar}}^{(k)} = k!, \tag{3.18}$$

which holds for $k \leq d$. The frame potential quantifies the 2-norm distance between the Haar ensemble and the k -fold \mathcal{E} -channel.¹² Here we show that the frame potential can be expressed as a certain average of OTO correlation functions.

¹²The distance between two quantum channels is typically measured by the diamond norm, while the frame potential measures the 2-norm (or more precisely the Frobenius norm) distance between a given ensemble and the Haar ensemble. Importantly, the 2-norm is weaker than the diamond norm. For precise statements regarding the different norms and bounds relating them, see [44].

Theorem 4. For any ensemble \mathcal{E} of unitary operators,

$$\frac{1}{d^{4k}} \sum_{A_1, \dots, B_1, \dots} \left| \langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle_{\mathcal{E}} \right|^2 = \frac{1}{d^{2(k+1)}} \cdot F_{\mathcal{E}}^{(k)}, \quad (3.19)$$

where summations are over all possible Pauli operators.

The l.h.s. of the equation is the operator average of the 2-norm of OTO correlators, and the r.h.s. is the k th frame potential up to a constant factor. There are d^{4k} Pauli operators $A_1, \dots, A_k, B_1, \dots, B_k$, which leads to $1/d^{4k}$. The theorem implies that the quantitative effect of random unitary evolution is to decrease the frame potential, which is equivalent to the decay of OTO correlators.

Proof. We take the averages over $A_1, \dots, A_k, B_1, \dots, B_k$ first. Expanding the l.h.s. gives

$$\frac{1}{d^{4k}} \frac{1}{|\mathcal{E}|^2 d^2} \sum_{U, V \in \mathcal{E}} \sum_{A_1, \dots, B_1, \dots} \text{tr}\{A_1 U^\dagger B_1 U \cdots A_k U^\dagger B_k U\} \cdot \text{tr}\{V^\dagger B_k^\dagger V A_k^\dagger \cdots V^\dagger B_1^\dagger V A_1^\dagger\}. \quad (3.20)$$

For $k = 2$, this can be depicted graphically as

$$. \quad (3.21)$$

Recall that a SWAP operator is given by $\text{SWAP} = \frac{1}{d} \sum_P P \otimes P^\dagger$

$$. \quad (3.22)$$

Thus, we replace each average of Pauli operators $A_1, \dots, A_k, B_1, \dots, B_k$ by SWAP operators. There are $2k$ loops, where k of them contribute to $\text{tr}\{UV^\dagger\}$ and the remaining k loops contribute to $\text{tr}\{VU^\dagger\}$. Keeping track of the number of factors of d , we find

$$\frac{1}{d^{2(k+1)} |\mathcal{E}|^2} \sum_{U, V \in \mathcal{E}} \text{tr}\{UV^\dagger\}^k \cdot \text{tr}\{VU^\dagger\}^k = \frac{1}{d^{2(k+1)}} \cdot F_{\mathcal{E}}^{(k)}, \quad (3.23)$$

which is the desired result. \square

Lastly, we note that we can use the frame potential to lower bound the size of the ensemble. Since all the terms in the sum are positive, by taking the diagonal part of the double sum, we find

$$F_{\mathcal{E}}^{(k)} \geq \frac{1}{|\mathcal{E}|^2} \sum_{U, V \in \mathcal{E}, U=V} |\text{tr}\{I\}|^{2k} = \frac{1}{|\mathcal{E}|} d^{2k}, \quad (3.24)$$

meaning the cardinality is lower bounded as $|\mathcal{E}| \geq d^{2k}/F_{\mathcal{E}}^{(k)}$. Using the fact that $F_{\text{Haar}}^{(k)} = k!$, we can simply bound the size of a k -design¹³

$$|\mathcal{E}| \geq \frac{d^{2k}}{k!}, \quad (k\text{-design}). \quad (3.25)$$

Large k

In appendix B, we provided an intuitive way of counting the number of nearly orthogonal states in a high-dimensional vector space \mathbb{C}^d by introducing a precision tolerance ϵ . A similar argument holds for the number of operators; if we can only distinguish operators up to some precision ϵ , then the total number of unitary operators is given by the volume of the unitary group measured in balls of size ϵ , which roughly goes like $\sim \epsilon^{-2^{2n}}$.

The key point is that if we have a tolerance ϵ , then the number of operators is finite even for a continuous ensemble. This means that there is a maximum size to any ensemble that is a subset of the unitary group. Looking at our bound eq. (3.25), we see that for $k \sim d$ we begin to reach the maximum size for some ϵ .

As a corollary, this means that for large $k \gtrsim d$, being a k -design implies that the ensemble is an approximate $k+1$ -design. In this sense, there are really only $O(d)$ nontrivial moments of the Haar ensemble.

As an explicit example, we will consider the case of $d = 2$. Here, for Haar we can compute the frame potential exactly for all k [45]

$$F_{\text{Haar}}^{(k)} = \frac{(2k)!}{k!(k+1)!}, \quad (3.26)$$

and thus we have the following relationship

$$\frac{F_{\text{Haar}}^{(k+1)}}{F_{\text{Haar}}^{(k)}} = 4 \frac{k+1/2}{k+2}. \quad (3.27)$$

On the other hand, for any ensemble the frame potential satisfies

$$F^{(k+1)} \leq d^2 F^{(k)} = 4F^{(k)}. \quad (3.28)$$

Therefore, for $d = 2$ we see that if an ensemble is a k -design, for $k \gtrsim 2$ it will automatically be close to being a $k+1$ -design.

3.3 Ensemble vs. time averages

In this subsection, we consider the time average of the frame potential to ask whether the ensemble specified by sampling $U(t) = e^{-iHt}$ at different times t will ever form a k -design. In the classical statistical mechanics and chaos literature, this is the question of whether a system is ergodic — whether the average over phase space equals an average over the time evolution of some initial state.

¹³Actually, one can slightly improve this lower bound for a k -design, see [41, 57].

Consider the one-parameter ensemble of unitary matrices defined by evolving with a fixed time-independent Hamiltonian H ,

$$\mathcal{E} = \{e^{-iHt}\}_{t=0}^{\infty}. \tag{3.29}$$

We can compute the frame potential as

$$\begin{aligned} F_{\mathcal{E}}^{(k)} &= \lim_{T \rightarrow \infty} \frac{1}{T^2} \int_0^T dt_1 dt_2 \left| \text{tr} \{e^{-iH(t_1-t_2)}\} \right|^{2k}, \\ &= \lim_{T \rightarrow \infty} \frac{1}{T^2} \int_0^T dt_1 dt_2 \sum_{\ell_1 \dots \ell_k} \sum_{m_1 \dots m_k} \exp \left\{ -i(t_2 - t_1) \sum_{i=1}^k E_{\ell_i} + i(t_2 - t_1) \sum_{j=1}^k E_{m_j} \right\}. \end{aligned} \tag{3.30}$$

If the spectrum is chaotic/generic, then the energy levels are all incommensurate. The terms in the sum evaluate to zero unless we have $E_{\ell_i} = E_{m_j}$ for all possible pairings (i, j)

$$\begin{aligned} F_{\mathcal{E}}^{(k)} &= \sum_{\ell_1 \dots \ell_k} \sum_{m_1 \dots m_k} \sum_{ij} \delta_{\ell_i m_j}, \\ &= k! \left(\sum_{\ell} I \right)^k = k! d^k. \end{aligned} \tag{3.31}$$

This is larger than $F_{\text{Haar}}^{(k)}$ by a factor of d^k ; the ensemble $\mathcal{E} = \{e^{-iHt}\}$ does not form a k -design! Recall that $F_{\mathcal{E}} = d^{2k}$ for a trivial ensemble $\mathcal{E} = \{I\}$ while $F_{\mathcal{E}} = k!$ for a Haar ensemble. The time average ensemble sits in the middle of these ensembles.

This “half-randomness” can be understood in the following way. Let us write the Hamiltonian as

$$H = \sum_j E_j |\psi_j\rangle\langle\psi_j|. \tag{3.32}$$

Rotating H by a unitary operator does not affect the frame potential, so we can consider a classical Hamiltonian

$$H' = \sum_j E_j |j\rangle\langle j|, \tag{3.33}$$

with the same frame potential. Even though H' is classical, it has an ability to generate entanglement. Namely, if an initial state is $|+\rangle = \sum_j |j\rangle$, then time-evolution will create entanglement. In terms of the original Hamiltonian H , we see that the system keeps evolving in a non-trivial manner as long as the initial state is “generic” and is different from eigenstates of the Hamiltonian H . This arguments suggests that the frame potential, in a time-average sense, can only see the spectrum distribution.

This fact, that Hamiltonian time evolution can never lead to random unitaries, can also be understood in terms of the distribution of the spacing of the eigenvalues.¹⁴ The phases of

¹⁴This argument has been made by Michael Berry, who related it to Steve Shenker, who related it to Douglas Stanford, who related it to us. As far as we know, it does not otherwise appear in the literature.

the Haar random unitary operators have Wigner-Dyson statistics; they are repulsed from being degenerate. The eigenvalues of a typical Hamiltonian H also have this property. However, these eigenvalues live on the real line, while the phases of e^{-iHt} live on the circle. In mapping the line to the circle, the eigenvalues of H wrap many times. This means that the difference of neighboring phases of e^{-iHt} will not be repulsed; e^{-iHt} will have Poisson statistics! In this sense, the ensemble formed by sampling e^{-iHt} over time may never become Haar random.¹⁵ The calculation in the beginning of this subsection provides an explicit calculation of the 2-norm distance between such an ensemble and k -designs and quantifies the degree to which the ensemble average is “too random” as compared to the time average.

4 Measures of complexity

For an operator or state, the computational complexity is a measure of the minimum number of basic elementary gates necessary to generate the operator or the state from a simple reference operator (e.g. the identity operator) or reference state (e.g. the product state). With the assumption that the elementary gates are easy to apply, the complexity is a measure of how difficult it is to create the state or operator.

On the other hand, an ensemble contains many different operators with different weights or probabilities. In that case, the computational complexity of the ensemble should be understood as the number of steps it takes to generate the ensemble by probabilistic applications of elementary gates. For instance, to generate the ensemble of Pauli operators, we randomly choose with probability 1/4 a Pauli operator I, X, Y, Z to apply to a qubit, and then repeat this procedure for all the qubits.

The complexity of an ensemble is related to the complexity of an operator in the following way. If an ensemble can be prepared in \mathcal{C} steps, then all the operators in the ensemble can be generated by applications of at most \mathcal{C} elementary gates. On the other hand, if an ensemble cannot be prepared (or approximated) in \mathcal{C} steps, then most of the operators in the ensemble cannot be generated by applications of \mathcal{C} elementary gates. In this sense, the computational complexity of an ensemble could be thought of as the mean complexity (i.e. complexity of typical operators in the ensemble). In the extreme case, generating the Haar ensemble will take exponential circuit complexity since, on average, individual elements have exponential complexity.

The complexity of the ensemble can be lower bounded in terms of the number of elements or cardinality of the ensemble $|\mathcal{E}|$. If all the elements are represented equally (with uniform probabilities), then clearly at least \mathcal{E} circuits need to be generated from probabilistic applications of the elementary gates. Making use of a fact introduced in the previous section that $F_{\mathcal{E}}^{(k)}$ provides a lower bound on $|\mathcal{E}|$, here we show that the frame potential provides a lower bound on a circuit complexity of generating \mathcal{E} . We will also explain how this bound applies to ensembles that depend continuously on some parameters and thus have a divergent number of elements.

¹⁵Relatedly, the space of unitaries with a fixed Hamiltonian is d -dimensional, while the space of unitaries is d^2 -dimensional.

Two additional bounds that are somewhat outside the scope of the main presentation, one on circuit depth and one on the early-time complexity growth with a disordered ensemble of Hamiltonians, are relegated to appendix C.

4.1 Discrete ensembles

Consider a system of n qubits. Let \mathcal{G} denote an elementary gate set that consists of a finite number of two-qubit quantum gates. We denote the number of elementary two-qubit gates by $g := |\mathcal{G}|$. At each time step we assume that we can implement any of the gates from \mathcal{G} . One typically chooses \mathcal{G} so that gates in \mathcal{G} enables a universal quantum computation. A well-known example is

$$\mathcal{G} = \{2\text{-qubit Clifford}, T\}, \tag{4.1}$$

where T is the $\pi/4$ phase shift operator; $T = \text{diag}(1, e^{i\pi/4})$. (Of course, this is not the only choice of elementary gate sets.)

Our goal is to generate an ensemble of unitary operators \mathcal{E} by sequentially implementing quantum gates from \mathcal{G} . Let us denote the necessary number of steps (i.e. the circuit complexity) to generate \mathcal{E} by $\mathcal{C}(\mathcal{E})$. Then one has the following complexity lower bound.

Theorem 5. *Let g be the number of distinct two-qubit gates from the elementary gate set. Then the circuit complexity $\mathcal{C}(\mathcal{E})$ to generate an ensemble \mathcal{E} is lower bounded by*

$$\mathcal{C}(\mathcal{E}) \geq \frac{\log |\mathcal{E}|}{\log(gn^2)}. \tag{4.2}$$

The proof relies on an elementary counting argument. Arguments along this line of thought have been used commonly in the literature.

Proof. At each step, we randomly pick a pair of qubits. Since there are g implementable quantum gates and $\binom{n}{2}$ qubit pairs, there are in total $\simeq gn^2$ choices at each step. If this procedure runs for \mathcal{C} steps, the number of unique circuits this procedure can implement is upper bounded by

$$\# \text{ of circuits} \leq (gn^2)^{\mathcal{C}}. \tag{4.3}$$

Since there are $|\mathcal{E}|$ unitary operators in an ensemble \mathcal{E} , we must have

$$(gn^2)^{\mathcal{C}} \geq |\mathcal{E}|, \tag{4.4}$$

which implies

$$\mathcal{C}(\mathcal{E}) \geq \frac{\log |\mathcal{E}|}{\log(gn^2)}. \tag{4.5}$$

□

In appendix B, we provide an intuitive way of counting the number of states in a $d = 2^n$ -dimensional Hilbert space (which was well known for a long time from [50]). As a sanity check on Theorem 5, if we substitute $|\mathcal{E}| \gtrsim 2^{2^n}$ into eq. (4.2) we see that the complexity of most states is exponential in the number of qubits $\mathcal{C} > 2^n \log 2$.

Finally, let us examine the relation between the frame potential and the circuit complexity. Using eq. (3.24) to trade $|\mathcal{E}|$ for $F_{\mathcal{E}}^{(k)}$, we find

$$\mathcal{C}(\mathcal{E}) \geq \frac{2kn \log(2) - \log F_{\mathcal{E}}^{(k)}}{\log(gn^2)}. \tag{4.6}$$

Of course, this bound obviously depends on the choice of basic elements g and the fact that we are using two-qubit gates. If we had considered q -body gates, we would have found a denominator $\log(g^{\binom{n}{q}}) \approx \log(gn^q)$ for $n \gg q$. This is no more than a choice of “units” with which to measure complexity. Thus, we state our key result as:

Theorem 6. *For an ensemble \mathcal{E} with the k th frame potential $F_{\mathcal{E}}^{(k)}$, the circuit complexity is lower bounded by*

$$\mathcal{C}(\mathcal{E}) \geq \frac{2kn \log(2) - \log F_{\mathcal{E}}^{(k)}}{\log(\text{choices})}, \tag{4.7}$$

In this context, $\log(\text{choices})$ simply indicates the logarithm of the number of decisions that are made at each step. If we imagine we have some kind of decision tree for determining which gate to apply where we make a binary decision at each step (and use \log_2), then we may set the denominator to unity and measure complexity in bits rather than gates, i.e. $\mathcal{C}(\mathcal{E}) \geq 2kn - \log_2 F_{\mathcal{E}}^{(k)}$.

In the above discussion, we glossed over a subtlety. Here, we considered the quantum circuit complexity to prepare or approximate an entire ensemble \mathcal{E} . A closely related but different question concerns the quantum circuit complexity required to implement a typical unitary operator from the ensemble \mathcal{E} . Nevertheless, in ordinary settings the typical operator complexity and the ensemble complexity are roughly of the same order. While establishing a rigorous result in this direction is beyond the scope of this paper, see [50] for some basic proof techniques that are useful in establishing this connection.

An important consequence of Theorem 6 is that the smallness of the frame potential (i.e. generic smallness of OTO correlators) implies increases in quantum circuit complexity of generating the ensemble \mathcal{E} . As a corollary, we can simply rewrite eq. (4.7) as

$$\mathcal{C}(\mathcal{E}) \geq (2k - 1)2n - \log_2 \sum_{A_1, \dots, B_1, \dots} \left| \langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle_{\mathcal{E}} \right|^2. \tag{4.8}$$

In this sense, we see how the decay of OTO correlators is directly related to an increase in the (lower-bound) of the complexity.

Next, recall that the frame potential for a k -design is given by $F_{\text{Haar}}^{(k)} = k!$, which does not grow with n . The complexity of a k -design is thus lower bounded as

$$\mathcal{C}(k\text{-design}) \geq 2kn - k \log_2(k) + \log_2 k + \dots, \tag{4.9}$$

which for large n grows roughly linearly in k and n (at least). In section C.1, we show that the minimum depth circuit to make a k -design also grows linearly in k (at least).

Finally, we offer an additional information-theoretic interpretation for our lower bound and generalize it for ensembles with non-uniform probability distributions. Consider an ensemble $\mathcal{E} = \{p_j, U_j\}$ with probability distribution $\{p_j\}$ such that $\sum_j p_j = 1$. The second R enyi entropy of the distribution $\{p_j\}$ is defined as $S^{(2)} = -\log(\sum_j p_j^2)$. In this more general situation, we can still bound the frame potential by considering the diagonal part of the sum

$$F_{\mathcal{E}}^{(k)} = \sum_{i,j} p_i p_j |\text{tr}\{U_i U_j^\dagger\}|^{2k} \geq \sum_i p_i^2 |\text{tr}\{I\}|^{2k} = e^{-S^{(2)}} d^{2k}. \tag{4.10}$$

Since the von Neumann entropy $S^{(1)} = -\sum_j p_j \log(p_j)$ is always greater than the second R enyi entropy, $S^{(1)} \geq S^{(2)}$, we can bound the von Neumann entropy as

$$S^{(1)} \geq 2kn - \log_2 F_{\mathcal{E}}^{(k)}. \tag{4.11}$$

The entropy of the ensemble is a notion of complexity measured in bits.¹⁶

4.2 Continuous ensembles

Many interesting ensembles of unitary operators are defined by continuous parameters, e.g. a disordered system has a time evolution that may be modeled by an ensemble of Hamiltonians.¹⁷ While the counting argument in section 4.1 is not directly applicable to these systems with continuous parameters, the complexity lower bound generalizes to such systems by allowing approximations of unitary operators. To be concrete, imagine that we wish to create some unitary operator U_0 by combining gates from the elementary gate set. In practice, we do not need to create an exact unitary operator U_0 . Instead, we may be fine with preparing some U that faithfully approximate U_0 to within a trace distance

$$\|U_0 - U\|_1 \leq \epsilon, \tag{4.12}$$

where the notation $\|\cdot\|_p \equiv (\text{tr}\{|\cdot|^p\})^{1/p}$ specifies the p -norm of an operator.¹⁸

Now, let us derive a complexity lower bound up to an ϵ -tolerance. We begin by taking N_s samples from the ensemble and use them to estimate the frame potential of the continuous distribution

$$F_{\mathcal{E}}^{(k)} \approx \frac{1}{N_s^2} \sum_{i,j} |\text{tr}\{U_i^\dagger V_j\}|^{2k}, \tag{4.13}$$

¹⁶However, this is not to be confused with the entanglement entropy. The entropy of the ensemble is essentially the logarithm of the number of different operators, and therefore can be exponential in the size of the system. Instead, the entanglement entropy (as a measure of entanglement) can only be as large as (half) the size of the system.

¹⁷A notable example of recent interest to the holography and condensed matter community is the ensemble implied by time evolving with the Sachdev-Ye-Kitaev Hamiltonian [58–60].

¹⁸We use the trace norm here because we are ultimately interested in states (which we represent as operators using the Choi-Jamiolkowski isomorphism) that are created by time evolution of the thermofield double state.

where the each of the two sums runs over all N_s samples. We can lower bound eq. (4.13) as follows

$$F_{\mathcal{E}}^{(k)} \geq \frac{1}{N_s^2} \sum_i \sum_{\substack{j \\ \|U_i - V_j\|_1 < \epsilon}} |\text{tr}\{U_i^\dagger V_j\}|^{2k}, \quad (4.14)$$

where the sum over i runs from 1 to N_s . The sum over j includes only a smaller subset $N_\epsilon(U_i)$, which is the number of operators within a trace distance ϵ of a particular U_i .

To continue, let's bound the summand. First, note that

$$|\text{tr}\{U^\dagger V\}| > \text{Re}\{\text{tr}\{U^\dagger V\}\} = d - \frac{1}{2}\|U - V\|_2^2. \quad (4.15)$$

The 2-norm is upper bounded by the 1-norm as $\|\mathcal{O}\|_2 \leq \sqrt{d}\|\mathcal{O}\|_1$, which let's us rewrite this as

$$|\text{tr}\{U^\dagger V\}|^{2k} > d^{2k} \left(1 - \frac{1}{2}\|U - V\|_1^2\right)^{2k}. \quad (4.16)$$

For this formula to be sensible, this approximation requires that $\epsilon < \sqrt{2}$. Substituting eq. (4.16) into eq. (4.14), we can bound the frame potential

$$F_{\mathcal{E}}^{(k)} \geq \frac{1}{N_s} d^{2k} \left(1 - \frac{\epsilon^2}{2}\right)^{2k} \left[\frac{1}{N_s} \sum_{i=1}^{N_s} N_\epsilon(U_i)\right] = d^{2k} \left(\frac{\overline{N}_\epsilon}{N_s}\right) \left(1 - \frac{\epsilon^2}{2}\right)^{2k}. \quad (4.17)$$

The term in brackets in the middle expression is the average number of operators within a trace distance ϵ of an operator in our sample set. In the final expression this is represented by the symbol \overline{N}_ϵ .

Now, let's run the counting argument again. If we want to make N_s circuits exactly, then in \mathcal{C} steps we must have

$$(\text{choices})^{\mathcal{C}} > N_s, \quad (4.18)$$

where as before (choices) summarizes the information about our choice of gate set, etc. Instead, if you only care about making circuits to within an ϵ -accuracy, then in \mathcal{C}_ϵ steps N_s instead satisfies

$$(\text{choices})^{\mathcal{C}_\epsilon} \overline{N}_\epsilon > N_s. \quad (4.19)$$

This lets us lower bound the complexity of the ensemble at precision ϵ as

$$\mathcal{C}_\epsilon(\mathcal{E}) > \frac{2k \log(d) - k\epsilon^2 - \log F_{\mathcal{E}}^{(k)}}{\log(\text{choices})}. \quad (4.20)$$

We then take the continuum limit by taking $N_s \rightarrow \infty$. The number of operators within an ϵ -ball of a given sample will also diverge, but the ratio $N_s/\overline{N}_\epsilon$ should remain finite and converge to some value, roughly the volume of the ensemble as measured in balls of ϵ -radius.¹⁹

Finally, in section C.2, we further extend this notion of bounding complexity for continuous ensembles to show that the initial early-time growth of complexity for evolution with an ensemble of Hamiltonians grows initially as t^2 for a time $t < 1/\sqrt{\log(d)}$.

¹⁹Note that $\log(\text{choices})$ diverges if the elementary gate set is continuous. This problem may be also fixed by employing the ϵ -tolerance.

5 Measures of correlators

While much of the focus of this paper has been on the behavior of ensembles, we were originally motivated by the following question: when is a random unitary operator an appropriate approximation to the underlying dynamics? In this section, we will attempt to return the focus to this question by computing random averages over correlation functions and comparing them to expectations for chaotic time evolution in physical systems.

5.1 Haar random averages

In this subsection, we will explicitly compute some ensemble averages of OTO correlators for different choices of ensembles. A particular goal will be to understand the asymptotic behavior of these averages in the limit of a large number of degrees of freedom $d \rightarrow \infty$. We present explicit calculations for 2-point and 4-point functions here and provide results for 6-point and 8-point functions. Additional calculations may be found in appendix D.

2-point functions

Consider a 2-point correlator, averaged over Haar random unitary operators

$$\langle A\tilde{B} \rangle_{\text{Haar}} = \frac{1}{d} \int_{\text{Haar}} dU \text{tr} \{ A U^\dagger B U \}. \tag{5.1}$$

Since U and U^\dagger each only appear in the expression once, we will obtain the same answer if the average is instead performed over a 1-design: $\langle A\tilde{B} \rangle_{\text{Haar}} = \langle A\tilde{B} \rangle_{1\text{-design}}$. By using a formula from section 2, we can derive the following expression

$$\langle A\tilde{B} \rangle_{\text{Haar}} = \langle A \rangle \langle B \rangle. \tag{5.2}$$

Graphically, the calculation goes as follows

$$\frac{1}{d} \text{---} \boxed{A} \text{---} \boxed{U^\dagger} \text{---} \boxed{B} \text{---} \boxed{U} \text{---} = \text{---} \boxed{A} \text{---} \boxed{B} \text{---} \tag{5.3}$$

It is often convenient to consider physical observables with zero mean by shifting $A \rightarrow A - \langle A \rangle$. Then, we see that these 2-point correlation function vanish. Of course, this always holds for Pauli operators

$$\langle A\tilde{B} \rangle_{\text{Haar}} = 0, \quad A, B \in \mathcal{P}, \quad A, B \neq I. \tag{5.4}$$

Next, let us consider the norm squared of a 2-point correlator averaged over Haar random unitary operators $|\langle A\tilde{B} \rangle_{\text{Haar}}|^2 = \frac{1}{d^2} \int_{\text{Haar}} dU \text{tr} \{ A U^\dagger B U \} \text{tr} \{ U^\dagger B^\dagger U A^\dagger \}$. Note that we take the Haar average after squaring the correlator. Since there are two pairs of U and U^\dagger appearing, we can perform the average over a 2-design: $|\langle A\tilde{B} \rangle_{\text{Haar}}|^2 = |\langle A\tilde{B} \rangle_{2\text{-design}}|^2$. Let us assume that A, B are Pauli operators so that we can neglect contributions from $\langle A \rangle$ and

$\langle B \rangle$. There are four terms, but only one term survives because the trace of non-identity Pauli operators is zero. We depict the calculation graphically as

$$\frac{1}{d^2} \begin{array}{c} \text{---} [A] \text{---} [U^\dagger] \text{---} [B] \text{---} [U] \text{---} \\ \text{---} [A^\dagger] \text{---} [U^\dagger] \text{---} [B^\dagger] \text{---} [U] \text{---} \end{array} = \frac{1}{d^2} \begin{array}{c} [A] \quad [B] \\ | \quad | \\ [A^\dagger] \quad [B^\dagger] \end{array} C_I \quad (5.5)$$

where $C_I = 1/(d^2 - 1)$ comes from the Weingarten function as shown in section 2. The final result is

$$|\langle A\tilde{B} \rangle_{\text{Haar}}|^2 = \frac{1}{d^2 - 1}, \quad A, B \in \mathcal{P}, \quad A, B \neq I. \quad (5.6)$$

Thus, the variance of the Haar averaged 2-point function is exponentially small in the number of qubits.

4-point functions

Next, consider a 4-point OTO correlator averaged over Haar random unitary operators:

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Haar}} = \frac{1}{d} \int_{\text{Haar}} dU \text{tr}\{A U^\dagger B U C U^\dagger D U\}. \quad (5.7)$$

As has already been explained, we will obtain the same answer if the average is performed with a 2-design: $\langle A\tilde{B}C\tilde{D} \rangle_{\text{Haar}} = \langle A\tilde{B}C\tilde{D} \rangle_{2\text{-design}}$. By using formulas from section 2 we can derive the following expression²⁰

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Haar}} = \langle AC \rangle \langle B \rangle \langle D \rangle + \langle A \rangle \langle C \rangle \langle BD \rangle - \langle A \rangle \langle C \rangle \langle B \rangle \langle D \rangle - \frac{1}{d^2 - 1} \langle\langle AC \rangle\rangle \langle\langle BD \rangle\rangle, \quad (5.8)$$

where $d = 2^n$ and $\langle\langle AC \rangle\rangle \equiv \langle AC \rangle - \langle A \rangle \langle C \rangle$. In particular, for Pauli operators $A, B, C, D \neq I$, one has

$$\begin{aligned} \langle A\tilde{B}C\tilde{D} \rangle_{\text{Haar}} &= -\frac{1}{d^2 - 1} & (A = C^\dagger, B = D^\dagger), \\ &= 0 & (\text{otherwise}). \end{aligned} \quad (5.9)$$

When nonzero, the result is exponential small in the number of qubits n . The derivation of the aforementioned formula can be understood graphically as follows

$$\begin{array}{c} \text{---} [A] \text{---} [U^\dagger] \text{---} [B] \text{---} [U] \text{---} \\ \text{---} [C] \text{---} [U^\dagger] \text{---} [D] \text{---} [U] \text{---} \end{array} = \frac{1}{d^2 - 1} \begin{array}{c} (A-C) \quad (B) \\ \circ \quad \circ \\ (D) \end{array} - \frac{1}{d^2 - 1} \begin{array}{c} (A) \quad (B-D) \\ \circ \quad \circ \\ (C) \end{array} - \frac{1}{d(d^2 - 1)} \begin{array}{c} (A) \quad (B) \\ \circ \quad \circ \\ (C) \quad (D) \end{array} - \frac{1}{d(d^2 - 1)} \begin{array}{c} (A-C) \quad (B-D) \\ \circ \quad \circ \end{array}. \quad (5.10)$$

By rewriting the expression in terms of connected correlators, we obtain the formula eq. (5.8).

²⁰Note: this formula was independently obtained by Kitaev.

Of course, we can obtain the same result by instead averaging over the Clifford group. When $A \neq C^\dagger$ or $B \neq D^\dagger$, it is easy to show $\langle A\tilde{B}C\tilde{D} \rangle_{\text{Clifford}} = 0$. When $A = C^\dagger$ and $B = D^\dagger$, the value of the correlator depends on the commutation relations between A and B

$$\begin{aligned} \langle A\tilde{B}A^\dagger\tilde{B}^\dagger \rangle &= 1, & [A, B] &= 0, \\ &= -1, & \{A, B\} &= 0. \end{aligned} \tag{5.11}$$

Since by definition Clifford operators transform a Pauli operators to another Pauli operator, \tilde{B} is a random Pauli operator with $\tilde{B} \neq I$. There are $d^2 - 1$ non-identity Pauli operators. Among them, $d^2/2 - 1$ Pauli operators commute with A , and $d^2/2$ anti-commute with A . Therefore, we find

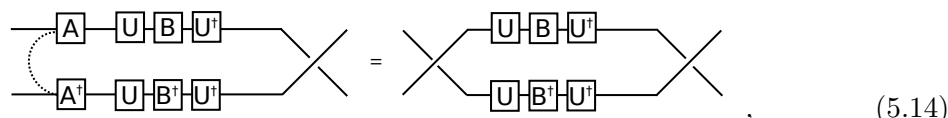
$$\langle A\tilde{B}A^\dagger\tilde{B}^\dagger \rangle_{\text{Clifford}} = \frac{d^2/2 - 1}{d^2 - 1} - \frac{d^2/2}{d^2 - 1} = \frac{-1}{d^2 - 1}. \tag{5.12}$$

As expected, the 4-point OTO correlator ensemble average over the Clifford group equals the Haar average. Recalling our result from section 3 that 4-point OTO values completely determine the 2-fold channel, this explicit calculation gives an alternative proof that the Clifford group forms a unitary 2-design.

Finally, we will present one additional way of computing the Haar average of 4-point OTO correlators. For convenience, we introduce the following notation

$$\text{OTO}^{(4)}(A, B) := \langle A\tilde{B}A^\dagger\tilde{B}^\dagger \rangle_{\text{Haar}}. \tag{5.13}$$

Since U is sampled uniformly over the unitary group, $\text{OTO}^{(4)}(A, B)$ does not depend on A, B as long as $A, B \neq I$. Consider the average of OTO correlation functions over all Pauli operators A , including identity operators: $\sum_A \langle A\tilde{B}A^\dagger\tilde{B}^\dagger \rangle_{\text{Haar}}$. Since $\frac{1}{d} \sum_A A \otimes A^\dagger$ is the swap operator, we have



where a dotted line represents an average over all the Pauli operators. This expression must be zero for $B \neq I$. Thus, we have

$$\sum_A \text{OTO}^{(4)}(A, B) = 0, \quad B \neq I. \tag{5.15}$$

If $A = I$, we have $\text{OTO}(A, B) = 1$. Since there are d^2 Pauli operators, we have

$$\text{OTO}^{(4)}(A, B) = -\frac{1}{d^2 - 1}, \quad A, B \neq I. \tag{5.16}$$

In appendix D.2, we use this method to estimate the scaling of higher-point OTO correlators with d , finding $4m$ -point functions of a related ordering scale as $\sim 1/d^{2m}$.

6-point functions

Next, consider the Haar average of 6-point OTO correlators, $\langle A\tilde{B}C\tilde{D}E\tilde{F}\rangle_{\text{Haar}}$. We will assume that $A, \dots, F \neq I$ are Pauli operators. In order to have non-zero contributions, we must have $ACE \propto I$ and $BDF \propto I$. Thus, we will only consider cases with $ACE \propto I$ and $BDF \propto I$.

The results depend on commutation relations between A, C and B, D , but always have the following scaling

$$\langle \text{6-point} \rangle_{\text{Haar}} \sim \frac{1}{d^2}, \quad (ACE = I, \quad BDF = I). \quad (5.17)$$

Explicitly, when $[A, C] = 0$ and $[B, D] = 0$, we find

$$\langle \text{6-point} \rangle_{\text{Haar}} = \frac{2d^2}{(d^2 - 1)(d^2 - 4)}. \quad (5.18)$$

The more general expression is slightly complicated though has the same scaling. Thus, the Haar average of 6-point OTO correlators does not reach any lower a floor value than the Haar average of 4-point OTO correlators.

8-point functions

Finally, we will study Haar averages of 8-point OTO correlators. In this case, there are two different types of nontrivial out-of-time ordering, which behave differently at large d . These computations are annoyingly technical, and so the details are hidden in appendix D.1.

The 8-point OTO correlators of the first type can be written in the following manner

$$\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{B}^\dagger C^\dagger\tilde{D}^\dagger \rangle, \quad (\text{non-commutator type}). \quad (5.19)$$

For Hermitian operators, this essentially repeats $A\tilde{B}C\tilde{D}$ twice. For reasons that will subsequently become clear, we will call such OTO correlators “non-commutator types.” (However, the result does depend on the commutation relations between A, C and B, D .) For these correlators, the scaling of the Haar average with respect to d is

$$\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{B}^\dagger C^\dagger\tilde{D}^\dagger \rangle_{\text{Haar}} \sim \frac{1}{d^2}, \quad (\text{non-commutator type}), \quad (5.20)$$

and this scaling does not depend on any commutation relations. Similar to what we found for the Haar average of the 6-point functions, these non-commutator type 8-point OTO correlators have the same scaling with d as the Haar average of 4-point OTO correlators.

The 8-point OTO correlators of the second type take the form

$$\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger \rangle, \quad (\text{commutator type}), \quad (5.21)$$

and are denoted “commutator-type” correlators. These correlators have the property that they can be written in the form

$$\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger \rangle = \langle K A^\dagger K^\dagger \rangle, \quad K = \tilde{B}C\tilde{D}, \quad (5.22)$$

i.e. they are the expectation value of the group commutator of the operator $AKA^\dagger K^\dagger$. The OTO correlators eq. (5.19) cannot be written in this way. As with the non-commutator types, the exact Haar average depends on commutation relations between A, C and B, D . However, the scaling with respect to d does not

$$\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger \rangle_{\text{Haar}} \sim \frac{1}{d^4}, \quad (\text{commutator type}). \quad (5.23)$$

The Haar average of these correlators is much smaller than the Haar average of the non-commutator types and the 4- and 8-point Haar averages! This suggests they might be a useful statistic for distinguishing ensembles that form a 4-design and ensembles that form a 2-design but do not form a higher design.

To test this idea, we can take an average of the commutator type 8-point OTO correlators averaged over the Clifford group. Since we have assumed the operators A, \dots, D are Pauli operators, we find

$$\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger \rangle_{\text{Clifford}} = \langle A\tilde{B}\tilde{D}CA^\dagger C^\dagger\tilde{D}^\dagger\tilde{B}^\dagger \rangle_{\text{Clifford}} = \frac{K(A, C^\dagger)}{d} \text{tr}\{A\tilde{B}\tilde{D}A^\dagger\tilde{D}^\dagger\tilde{B}^\dagger\}, \quad (5.24)$$

where in the first equality we commuted C, \tilde{D} and $C^\dagger, \tilde{D}^\dagger$, which holds because C, D are Pauli operators, and in the second equality we have defined $K(P, Q)$ by

$$Q^\dagger PQ = K(P, Q)P, \quad (5.25)$$

for Pauli operators P, Q . The final answer is

$$\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger \rangle_{\text{Clifford}} = \frac{-K(A, C^\dagger)}{d^2 - 1} \sim \frac{1}{d^2}. \quad (5.26)$$

Recall that the Clifford group is a unitary 2-design, is not a 3-design in general (except for a system of qubits) [43], and is never a 4-design. Therefore, we see that commutator-type correlators may provide a statistical test of whether an ensemble forms a k -design but not a $k + 1$ -design. We explore this idea further in section D.2.

5.2 Dissipation vs. scrambling

In this subsection, we will return to the 2- and 4-point averages and compare them against expectations from time evolution. Furthermore, we will attempt to provide some physical intuition for the behavior of these averages over different ensembles. This will support our picture of chaotic time evolution leading to increased pseudorandomness.

For strongly coupled thermal systems, it is expected that the connected part of the 2-point correlation functions decays exponentially within a time scale t_d of order the inverse temperature β

$$\langle A(0)B(t) \rangle \rightarrow \langle A \rangle \langle B \rangle + O(e^{-t/t_d}). \quad (5.27)$$

This time scale is often referred to as a “dissipation” or “thermalization” time and is related to the time it takes local thermodynamic quantities reaching equilibrium.²¹ It is suggestive that the results eq. (5.2) and eq. (5.27) are so similar. After a short time t_d , for these 2-point functions the chaotic dynamics give the same results as the Haar random dynamics.

Next, we turn to the variance of the 2-point correlator $\langle A(0)B(t) \rangle$. For a closed system of finite number of degrees of freedom, the 2-point function will be quasi-periodic with recurrences after a timescale $t_r \sim e^d$ that is exponential in the dimension and doubly exponential in the number of degrees of freedom $d = 2^n$. As such, the long-time average of $|\langle A(0)B(t) \rangle|^2$ must be nonzero. This can be estimated by performing a time average and gives a well known result [61–63]²²

$$\lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T |\langle A(0)B(t) \rangle|^2 dt \sim \frac{1}{d^2}. \quad (5.28)$$

Comparing against our result for the Haar-averaged dynamics eq. (5.6), we see that they coincide.

Next, let’s consider 4-point correlators in strongly-coupled theories with a large number of degrees of freedom N .²³ (For example, this can be thought of a system of N qubits where all the qubits interact but the interactions are at most q -local, with $q \ll N$ and $N \rightarrow \infty$.) First, let’s consider the case of a *time-ordered* correlator. Similar to the case of the 2-point functions, two of the three Wick contractions are expected to decay exponentially within a dissipation time t_d

$$\langle A(0)C(0)B(t)D(t) \rangle \rightarrow \langle AC \rangle \langle BD \rangle + O(e^{-t/t_d}), \quad (5.29)$$

which for qubits is analogous to considering a 2-point function between the composite operators AC and BD .²⁴ Thus, this correlator will equilibrate after a time t_d with a late-time value that depends on the expectations $\langle AC \rangle$ and $\langle BD \rangle$.

Now, let’s consider the out-of-time-order 4-point correlator in a large N strongly interacting theory. For $t \sim t_d$, this will behave similarly to the time-ordered correlator with two of the three Wick contractions decaying exponentially

$$\langle A(0)B(t)C(0)D(t) \rangle \rightarrow \langle AC \rangle \langle BD \rangle + O(e^{-t/t_d}), \quad t < t_d. \quad (5.30)$$

However, for $t > t_d$ the correlator obtains an exponentially growing connected component

$$\langle A(0)B(t)C(0)D(t) \rangle \rightarrow \langle AC \rangle \langle BD \rangle - O(e^{\lambda(t-t_*)}), \quad t_d < t < t_*. \quad (5.31)$$

This growth occurs in the regime $t_d < t < t_*$. The time scale $t_* = \lambda^{-1} \log N$, known as the fast scrambling time, is the time at which the exponentially growing piece of the

²¹For weakly coupled systems where the quasiparticle picture is valid (e.g. Fermi-liquids) the time scale is instead be given by $t_d \sim \beta^2$.

²²N.B. there is an error in this calculation as presented in [61, 62] and so interested readers should consult [63] for the actual details.

²³We thank Douglas Stanford for conversations relating to dissipative behavior of 4-point functions.

²⁴Note that the exact timescale t_d might depend on the operators being correlated and the particular contraction.

correlator compensates its $1/N$ suppression and becomes $O(1)$. The coefficient λ has the interpretation of a new kind of Lyapunov exponent [15] and is bounded from above by $2\pi/\beta$ [4]. Finally, for $t > t_*$, these OTO 4-point correlators are expected to decay to a small floor value that is exponentially small in N . A natural guess for this floor is

$$\langle A(0)B(t)C(0)D(t) \rangle \rightarrow e^{-O(N)} \langle AC \rangle \langle BD \rangle, \quad t > t_*, \quad (5.32)$$

which is reproduced from eq. (5.8) with 1-point functions assumed to be subtracted off.

As we mentioned, the 2-point function eq. (5.27) reached its Haar random value after a short dissipation time t_d . This is very suggestive of a picture where chaotic dynamics behave as a pseudo-1-design after a time t_d . Taking this point further, let's consider the 4-point OTO correlator averaged over Pauli operators, an ensemble that forms a 1-design, but not a 2-design. Furthermore, we will assume that the operators A and B have zero overlap. Under this assumption, we can show that

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Pauli}} = \langle AC \rangle \langle BD \rangle. \quad (5.33)$$

The proof of this is relegated to section A.2. Apparently, Pauli operators capture the behavior of the dynamics around $t \sim t_d$, i.e. from after the dissipative regime until the scrambling regime, but then a 2-design is required to capture the behavior after $t \sim t_*$, i.e. the post-scrambling regime.²⁵

Thus, we might say that after a time $\sim t_d$, the system becomes a pseudo-1-design, and then after $\sim t_*$ the system becomes a pseudo-2-design. (See figure 2 for a cartoon of this behavior.) However, it remains an open question whether there are any additional meaningful timescales that can be probed with correlators after t_* , though we are hopeful that such timescales might be hiding in higher-point OTO correlators.

6 Discussion

In this paper, we have connected the related ideas of chaos and complexity to pseudo-randomness and unitary design. A cartoon of these ideas is expressed nicely by figure 3. Operators can be thought of as being organized by increasing complexity. Regions defined by circles of larger and larger radius can be thought of as defining designs with increasing k .²⁶ In the rest of the discussion, we will make some related points, tie up loose ends, and mention future work.

²⁵Note that these observations depend on the ensemble we average over actually being the Pauli operators, and not just any ensemble that forms a 1-design without forming a 2-design. Furthermore, we assume that A, B, C, D are simply few-body operators so that the correlator is of local operators. These choices are determined for us by the basis in which the Hamiltonian is q -local.

²⁶While this picture is a cartoon, the manifold for the unitary group $U(n)$ has a dimension exponentially large in n . However, following [64], one can find a metric in which the length of a minimal geodesic between points computes operator complexity and in which most sections are expected to be hyperbolic. Taking this further, [65] considered an interesting analog system on a hyperbolic plane that captures many of the expected properties of complexity.

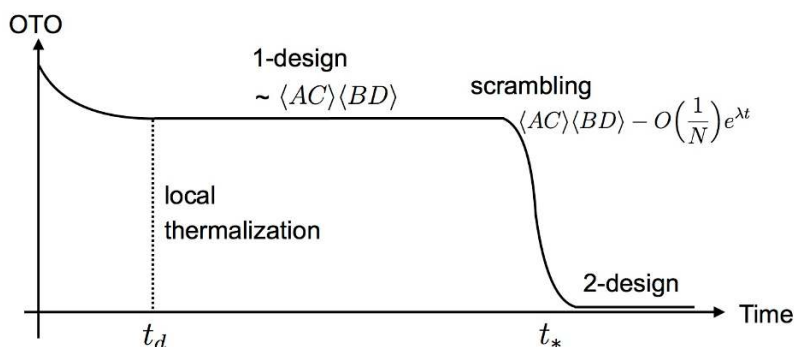


Figure 2. Thermalization and scrambling in the decay of a four-point OTO correlator. These correlators typically decay to $\langle AC \rangle \langle BD \rangle$ in a thermal dissipation time t_d , and then they decay to a floor value $\sim d^{-2}$ at around the scrambling time t_* . These regimes are very well captured by replacing the dynamics with 1-designs or 2-designs, respectively.

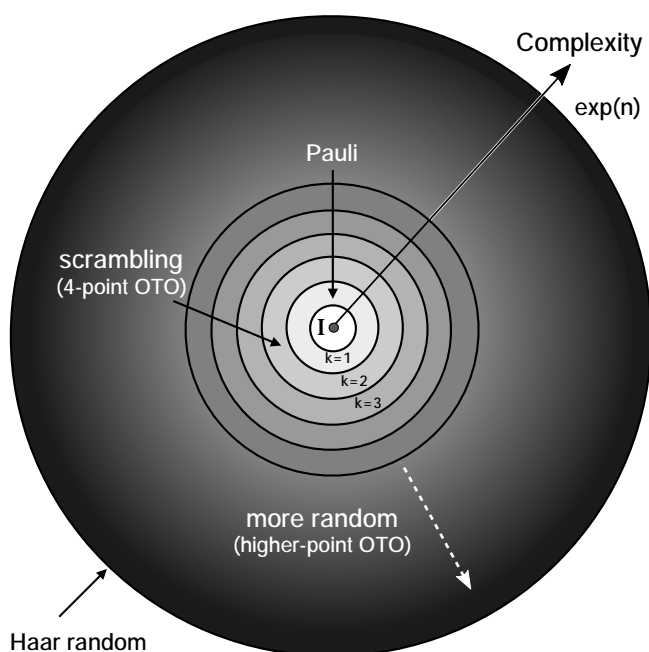


Figure 3. A cartoon of the unitary group, with operators arranged by design. We pick the identity operator to be the reference operator of zero complexity and place it at the center. Typical operators have exponential complexity and live near the edge. Operators closer to the center have lower complexity, which makes them both atypical and more physically realizable in a particular computational model.

6.1 Generalized frame potentials and designs

In realistic physical systems, one usually does not have access to the full Hilbert space. For example, there may be some conserved quantities, such as energy or particle numbers, or the system may be at some finite temperature β . In that case, one would be interested in understanding pseudorandomness inside a subspace of the Hilbert space, i.e. restricted to some state ρ . In appendix E, we generalize the frame potential for an arbitrary state ρ finding that the quantity

$$\mathcal{F}_{\mathcal{E}}^{(k)}(\rho) = \iint dU dV [\text{tr}\{\rho^{1/k}UV^\dagger\} \text{tr}\{\rho^{1/k}VU^\dagger\}]^k, \quad (6.1)$$

has all the useful properties desired of a frame potential. In particular, it is minimized by the Haar ensemble, and it provides a lower bound on ensemble size and complexity.

However, if the state ρ is the thermal density matrix, $\propto e^{-\beta H}$ and the ensemble is given by time evolution with an ensemble of Hamiltonians $\mathcal{E} = \{e^{-iHt}\}$, then we need to take into account the fact that the state itself depends on the ensemble. Instead, we can define a *thermal* frame potential

$$\mathcal{W}_{\beta}^{(k)}(t) = \iint dG dH \frac{|\text{tr}\{e^{-(\beta/2k-it)G} e^{-(\beta/2k+it)H}\}|^{2k}}{\text{tr}\{e^{-\beta G}\} \text{tr}\{e^{-\beta H}\}}. \quad (6.2)$$

In this case, even at $t = 0$ one can derive an interesting bound on the complexity of the ensemble. We hope to return to this in the future to analyze the *complexity of formation*: the computational complexity of forming the thermal state ρ_{β} from a suitable reference state.²⁷

Finally, it would be similarly interesting to consider a different generalization of unitary designs where, under some physical constraints, we can only access some limited degrees of freedom in the system. In this sense, one could think of the unitary ensemble (as opposed to the state) as being generated by tracing over these additional degrees of freedom. These “subsystem designs” would then be “purified” by integrating back in the original degrees of freedom.²⁸ This interesting direction is a potential subject of future work.

More chaos in quantum channels

In appendix F, we revisit some ideas from our previous work [7], though these ideas are also relevant to the current work. In particular, in section F.1 we reconsider the Hayden-Preskill notion of black hole scrambling [1]. In this thought experiment, Alice throws a secret quantum state into a black hole. Assuming Bob knows the initial state and dynamics of the black hole, we show how the question of whether Bob can reconstruct Alice’s secret is related to the decay of an average of a certain set of OTO four-point correlators.

In section F.2, we provide an operational interpretation to taking averages over OTO correlators. We show that this is related to a quantum game of “catch” where Alice may “spit-on” or otherwise perturb the ball before throwing it to Bob. The average over four-point OTO correlators gives the probability that Alice did not modify the ball. We also

²⁷This is also a question of interest in holography, see e.g. [66].

²⁸We thank Patrick Hayden and Michael Walter for initial discussions about this idea.

show that an average over higher-point OTO correlators can be interpreted as an “iterated” game of catch (i.e. what normally people just call “catch”) where both Alice and Bob have the opportunity to modify the ball each turn. In this case, the OTO correlator average is related to the joint probability that neither Alice nor Bob perturb the ball.

Finally, in section F.3 we show that an average over a particular ordering of $2k$ -point OTO correlators can be related to the k th Rényi entropy of the operator U interpreted as a state. We find that

$$-\log(\text{a certain average of } 2k\text{-point OTO correlators}) \propto S_{\text{subsystem}}^{(k)}(U), \quad (6.3)$$

where $S_{\text{subsystem}}^{(k)}$ is the Rényi k -entropy of a particular subsystem of the density matrix $\rho = |U\rangle\langle U|$.

Volume of unitary operators

The argument in section 4.2 led to a bound on the ratio $N_s/\overline{N}_\epsilon$, which can be interpreted as the volume of \mathcal{E} in terms of ϵ -balls. An interesting application of this bound might be to think about the volume of unitary operators in $U(d)$ that can be probed in a finite time scale T , i.e. the volume of operators with depth $\mathcal{D} \sim T$. (See section C.1 for further discussion of a lower bound on circuit depth in terms of the frame potential.)

In fact, in certain situations (such as the Brownian circuit introduced in [5] or the random circuit model), it is not difficult to show that the volume of unitary operators with depth T grows at least $\sim \exp(\text{const} \cdot nT)$ for some small T and some constant independent of n by computing the $k = 1$ frame potential. This implies that the space of unitary operators, with the metric being quantum gate complexity, has hyperbolic structure with constant curvature, as discussed in e.g. [64, 65, 67] (see also [68]). On the other hand, one can upper bound the volume of unitary operators with circuit depth T by thinking about how the depth can grow $V(T) \sim \binom{n}{2} \binom{n-2}{2} \binom{n-4}{2} \cdots \binom{2}{2} \approx \exp(n \log n \cdot T)$. Thus, for small T and large n , the lower bound seems to be reasonably tight.

Once a lower bound on the volume of unitary operators in an ensemble is obtained in the unit of ϵ -balls, we can also obtain a lower bound (of the same order) on the complexity of a typical operator in the ensemble. This seems possible by using the formal arguments given in [50] even when the elementary gate set is not discrete, e.g. all the two-qubit gates.

Finally, it’s a curious fact that for systems with time-dependent Hamiltonian ensembles (such as the random circuit models or the Brownian circuit of [5]) that we get an initial linear growth of the volume with T . As argued in section C.2 (and confirmed numerically), for time independent Hamiltonian evolution — e.g. in SYK or in the Gaussian unitary ensemble (GUE) — we get a lower bound $V(T) \sim \exp(\text{const} \cdot nT^2)$, which persists for a short time $T \sim 1/\sqrt{n}$. It would be very interesting to understand the difference in this scaling.²⁹

²⁹One might worry that this bound saturates at a value smaller than unity. However, we expect that there may be a continuous definition of complexity sensible for small complexities, see e.g. [69].

Tightness of the complexity bound

While the frame potential provides a rigorous lower bound on the complexity of generating an ensemble of unitary operators, there may be a cost: the bound may not be very tight when applied to time evolution by an ensemble of Hamiltonians.³⁰

Let us try to understand this better. To be concrete, consider the $k = 2$ frame potential for a strongly coupled spin systems that scrambles in $t_* \sim \log n$ time. In such a system, for local operators W, V of unit weight, OTO four-point correlators $\langle W(t)^\dagger V^\dagger W(t) V \rangle$ will begin to decay after $t \sim O(\log n)$. Since the $k = 2$ frame potential is the average of four-point OTO correlators, one might expect that the frame potential will also start to decay at $t \sim O(\log n)$.

However, this is not quite right. We expect the decay time for more general correlators of larger operators to be reduced to $\bar{t}_* \sim t_* - O(\log(\text{size } W)) - O(\log(\text{size } V))$, where $t_* \sim O(\log n)$ is the scrambling when V and W are low-weight operators. If we randomly select Pauli operators W and V , they will typically be nonlocal operators with $O(n)$ weights, and therefore the OTO decay time \bar{t}_* will be reduced to $O(1)$ for V and W of typical sizes.

In fact, the above estimate suggests most of the correlators determining the complexity bound should begin to decay immediately. As we can see in eq. (4.8), each correlator itself only makes a logarithmic contribution to the complexity and so we shouldn't expect the remaining slow decaying local correlators to be dominant. (To be sure, a further investigation of this point is required.)

One possible way to fix this problem would be to generalize the frame potential by using p -norm with $p \neq 2$ so that it is more sensitive to the slower decaying local correlators. We leave the study of such a generalization to the future.

Complexity and holography

Finally, we will return to the question of complexity and holography discussed in the introduction. In the context of holography, computational complexity was “introduced” [70] as a possible resolution to the firewall paradox of [6, 71]. A direct connection between complexity and black hole geometry was first proposed by Susskind [72, 73], which culminated in proposals that the interior of the black hole geometry is holographically dual to the spatial volume [74] or the spacetime action [75, 76]. These proposals are motivated by the fact that the black hole interior continues to grow as the state evolves long past the time entropic quantities equilibrate [77]. While there is nice qualitative evidence for both of these proposals [13, 65, 67], missing is a direct understanding of computational complexity in systems that evolve continuously in time with a time-independent Hamiltonian.

A hint can be obtained by considering some of the motivations for these holographic complexity proposals. In particular, building on the work of [77] and previous work of Swingle [78, 79], Maldacena suggested that the black hole interior could be found in the boundary theory by a tensor network construction of the state [80]. A tensor network toy model of the evolution of the black hole interior was investigated in [7]. In this toy model, the interior of the black hole was modeled as a flat tiling of perfect tensors, see figure 4.

³⁰We have learned this by some numerical investigations of the frame potential.

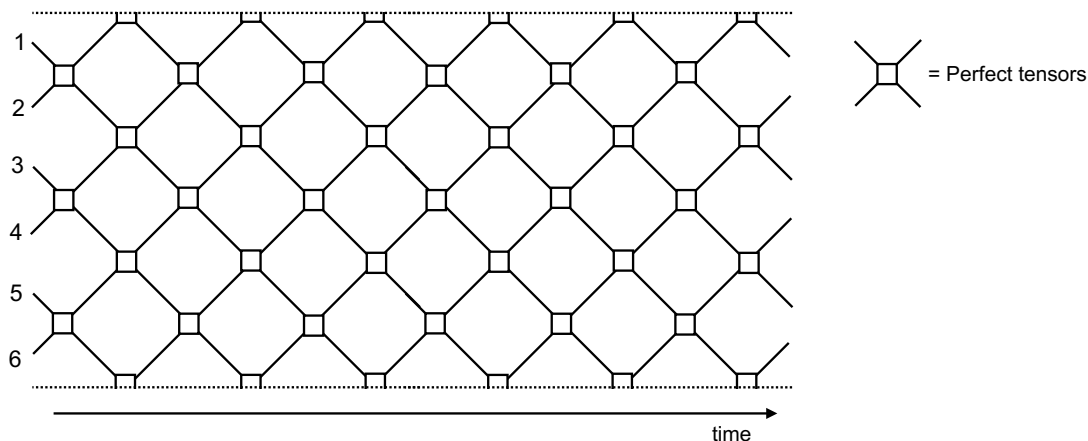


Figure 4. A 6-qubit tensor network model for the geometry of the interior of a black hole. Via holography, the growth of the interior is expected to correspond to chaotic time evolution of a strongly coupled quantum theory. Here, each node corresponds to a perfect tensor and the numbers label the qubit.

These tensors were elements of the Clifford group and acted as two-qubit unitary operators that highly entangled neighboring qubits at each time step. From the perspective of the boundary theory, this is a model for Hamiltonian time evolution.³¹

This toy model captures some important features of the complexity growth of the black hole state. The number of tensors in the network grows linearly in time, by construction. Operators will grow ballistically, exhibiting the butterfly effect, and the network scrambles in linear time. Thus, this network captures the aspects black hole chaos related to local scrambling and ballistic operator growth discussed in [13] as well as aspects of complexity growth discussed in [73–75, 77].

However, since in this model the perfect tensor is a repeated element of the Clifford group, the complexity can never actually grow to be very big. In fact, the quantum recurrence time of the model was investigated in [7] and was found to be exponential in the entropy $\sim e^n$ rather than doubly exponential $\sim e^{e^n}$ as expected in a fully chaotic model. This is related to our oft stated fact that the Clifford group generally does not form a higher-than-2-design. In fact, this model can actually be mapped to a classical problem, and by the Gottesman-Knill theorem its complexity can be no greater than $O(n^2)$ gates [82].³²

These observations were the inspiration for this current work, since in this toy model 4-point OTO correlators behave chaotically, but higher-point OTO correlators do not. Nevertheless, this model can be “improved” by using random 2-qubit tensors rather than

³¹In addition to providing a model for the black hole interior, Swingle’s identification of the ground state of AdS with a tensor network [78, 79] has led to numerous other quantum information insights in holography (e.g. quantum error correction and its relationship to bulk operator reconstruction [81]) as well as additional toy models that demonstrate those features (e.g. [11, 56]).

³²Since the Clifford group is a group, the complexity of any particular circuit in our model is an element of the group. Thus, at most we should be able to reach it by a polynomial number of applications of 2-qubit gates.

a repeated perfect tensor.³³ In [41], it was shown that this local random quantum circuit approaches a unitary k -design in a circuit depth that scales at most as $O(k^{10})$. Our complexity lower bound for a k -design eq. (4.9) suggests that the time to become a k -design is lower bounded by k , and we suspect that this can be saturated.³⁴

It is in this sense that we speculate that the complexity growth of the chaotic black hole is pseudorandom. That is, we suspect that as the complexity of the black hole state increases linearly with time evolution t , the dynamics evolve to become pseudo- k -designs, with the value k roughly scaling with t

$$\mathcal{C}(e^{-iHt}) \sim t \sim k, \tag{6.4}$$

and that this may be quantified by either representative $2k$ -point OTO correlators or by an appropriate generalization of unitary design. With this in mind, it would be interesting to see whether one could use the tools of unitary design to prove a version of the conjectures of [75, 76] suggesting that complexity (is greater than or) equal to action.

Acknowledgments

We are grateful to Fernando Brandao, Adam Brown, Jordan Cotler, Guy Gur-Ari, Patrick Hayden, Alexei Kitaev, Márk Mezei, Xiao-Liang Qi, Steve Shenker, Lenny Susskind, Douglas Stanford, and Michael Walter for discussions.

DR and BY both acknowledge support from the Simons Foundation through the “It from Qubit” collaboration. DR is supported by the Fannie and John Hertz Foundation, the National Science Foundation grant number PHY-1606531 and the Paul Dirac Fund, and is also very thankful for the hospitality of the Stanford Institute for Theoretical Physics and the Perimeter Institute of Theoretical Physics during the completion of this work. Research at Center for Theoretical Physics at MIT is supported by the U.S. Department of Energy under cooperative research agreement Contract Number DESC0012567. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. This paper was brought to you unitarily by the Haar measure.

A More proofs

Here, we collect some proofs.

A.1 Proof of theorem 2

Proof. The l.h.s. of eq. (3.11) can be written explicitly as

$$\sum_{C_1, \dots, C_k} \text{tr} \{C_k^\dagger A_k'^\dagger \dots C_1^\dagger A_1'^\dagger\} \text{tr} \{A_1 C_1 \dots A_k C_k\}. \tag{A.1}$$

³³Note: the case of a averaging over a single random tensor is like time evolution with a time independent Hamiltonian. On the other hand, the case of averaging separately over all tensors has a continuum limit of time evolution with a time-dependent Hamiltonian with couplings that evolve at each time step. This model is known as the Brownian circuit [5].

³⁴It is believed that this is actually saturated by the local random circuit of [41]. For example, there is some numerical evidence for this claim in [83].

Both $C_k^\dagger A_k'^\dagger \cdots C_1^\dagger A_1'^\dagger$ and $A_1 C_1 \cdots A_k C_k$ are Pauli operators with complex phases. This means that the traces will give a nonzero contribution only if both $A_1 \cdots A_k C_1 \cdots C_k \propto I$ and $A_1' \cdots A_k' C_1 \cdots C_k \propto I$. Thus, the sum will vanish unless $A_1 \cdots A_k \propto A_1' \cdots A_k'$. So, we consider the case where $A_1 \cdots A_k \propto A_1' \cdots A_k' \propto P$ for some Pauli operator P . Then, the summation can be written as

$$\begin{aligned} & \sum_{C_1 \cdots C_k \propto P^\dagger} \text{tr} \{C_k^\dagger A_k'^\dagger \cdots C_1^\dagger A_1'^\dagger\} \text{tr} \{A_1 C_1 \cdots A_k C_k\} \\ &= d \cdot \sum_{C_1 \cdots C_k \propto P^\dagger} \text{tr} \{C_k^\dagger A_k'^\dagger \cdots C_1^\dagger A_1'^\dagger A_1 C_1 \cdots A_k C_k\}. \end{aligned} \quad (\text{A.2})$$

Here we expanded the trace because $C_k^\dagger A_k'^\dagger \cdots C_1^\dagger A_1'^\dagger$ and $A_1 C_1 \cdots A_k C_k$ are proportional to identity operators when $C_1 \cdots C_k \propto P^\dagger$, and the d comes from the trace of an identity operator. By using the cyclic property of the trace, we can eliminate C_k^\dagger and C_k

$$d \cdot \sum_{C_1, \dots, C_{k-1}} \text{tr} \{A_k'^\dagger \cdots C_1^\dagger A_1'^\dagger A_1 C_1 \cdots A_k\}. \quad (\text{A.3})$$

Here we used the fact that fixing C_1, \dots, C_{k-1} uniquely determines C_k when $C_1 \cdots C_k \propto P$. Next, recall the relationship for summing over Pauli operators eq. (2.9)

$$\sum_{C_1} (\cdots) C_1^\dagger A_1'^\dagger A_1 C_1 (\cdots) = d^2 \cdot \delta_{A_1}^{A_1'} (\cdots) (\cdots) \quad (\text{A.4})$$

where (\cdots) represents arbitrary operators. This gives

$$d^3 \cdot \sum_{C_2, \dots, C_{k-1}} \text{tr} \{A_k'^\dagger \cdots C_2^\dagger A_2'^\dagger A_2 C_2 \cdots A_k\} \delta_{A_1}^{A_1'}. \quad (\text{A.5})$$

By repeated action of eq. (A.4), we can establish the desired result. \square

A.2 Proof of eq. (5.33)

We can expand operators A, B, C, D by using Pauli operators as a basis of operators

$$A = \sum_i a_i Q_i, \quad B = \sum_i b_i Q_i, \quad C = \sum_i c_i Q_i, \quad D = \sum_i d_i Q_i, \quad (\text{A.6})$$

where Q_i are Pauli operators

$$\langle A \tilde{B} C \tilde{D} \rangle_{\text{Pauli}} = \frac{1}{d^2} \sum_{P \in \text{Pauli}} \sum_{i,j,k,\ell} a_i b_j c_k d_\ell \langle Q_i P Q_j P^\dagger Q_k P Q_\ell P^\dagger \rangle. \quad (\text{A.7})$$

Notice that

$$\langle Q_i P Q_j P^\dagger Q_k P Q_\ell P^\dagger \rangle = \frac{1}{d} \text{tr} \{K(P, Q_j Q_\ell)\} \cdot \langle Q_i Q_j Q_j Q_\ell \rangle, \quad (\text{A.8})$$

and

$$\begin{aligned} \frac{1}{d^2} \sum_P \frac{1}{d} \text{tr} \{K(P, Q_j Q_\ell)\} &= 0, & j \neq \ell, \\ &= 1, & j = \ell, \end{aligned} \quad (\text{A.9})$$

where again we have defined $K(P, Q)$ by $Q^\dagger P Q = K(P, Q)P$. Thus, the desired average becomes

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Pauli}} = \sum_{i,j,k} a_i b_j c_k d_j \langle Q_i Q_j Q_k Q_j \rangle. \quad (\text{A.10})$$

Observe that $\langle Q_i Q_j Q_k Q_j \rangle \neq 0$ only when $Q_i = Q_k$, which gives

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Pauli}} = \sum_{i,j} a_i b_j c_i d_j \langle Q_i Q_j Q_i Q_j \rangle. \quad (\text{A.11})$$

Next, we assume that A and B have no overlap. This implies that $[Q_i, Q_j] = 0$ if $a_i, b_j \neq 0$, and we obtain

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Pauli}} = \sum_{i,j} a_i b_j c_i d_j. \quad (\text{A.12})$$

Since $\langle AC \rangle = \sum_i a_i c_i$ and $\langle BD \rangle = \sum_j b_j d_j$, we see that

$$\langle A\tilde{B}C\tilde{D} \rangle_{\text{Pauli}} = \langle AC \rangle \langle BD \rangle, \quad (\text{A.13})$$

as desired.

B More orthogonal states

In the Hilbert space $\mathcal{H} = \mathbb{C}^d$, there are d orthogonal states which form the basis of the Hilbert space

$$\langle i|j \rangle = \delta_{ij}, \quad (i, j = 1, \dots, d). \quad (\text{B.1})$$

Yet, there are $\sim 2^d$ states which are nearly orthogonal to each other

$$\langle \tilde{i}|\tilde{j} \rangle \ll 1, \quad (i, j = 1, \dots, O(2^d)), \quad (\text{B.2})$$

for $i \neq j$. A quantum state in this Hilbert space can be written as

$$|\psi \rangle = a_1|1 \rangle + a_2|2 \rangle + \dots + a_d|d \rangle, \quad (\text{B.3})$$

where $|a_1|^2 + |a_2|^2 + \dots + |a_d|^2 = 1$. Thus, a quantum state can be associated with a point on a $2d$ -dimensional unit sphere. By computing the volume of states whose inner product with a given reference state is larger than ϵ , we can find the number of nearly orthogonal states. Such a volume was explicitly computed in [50], but the point is that

$$\frac{\text{Vol}(S_{2d})}{\text{Vol}(\epsilon\text{-ball})} \sim \left(\frac{1}{\epsilon}\right)^d, \quad (\text{B.4})$$

meaning that there are a doubly exponential number of nearly orthogonal states in terms of the number of degrees of freedom n , with $d = 2^n$.

Here we provide another simple argument for this scaling.³⁵ Define $\{a\} = (a_1, \dots, a_d)$ with $a_j = \pm 1$. We consider the following state

$$|\{a\}\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d a_j |j\rangle, \quad a_j = \pm 1. \tag{B.5}$$

There are $2^d = 2^{2^n}$ states which can be represented in this way. Let us pick $\{a\}$ and $\{b\}$ randomly, and consider an inner product between two states $|\{a\}\rangle$ and $|\{b\}\rangle$

$$\langle \{a\} | \{b\} \rangle = \frac{1}{d} \sum_{j=1}^d a_j b_j. \tag{B.6}$$

Since we chose $\{a\}$ and $\{b\}$ randomly, the product $a_j b_j = \pm 1$ is random, and the inner product will be close to zero

$$|\langle \{a\} | \{b\} \rangle| = O(d^{-1/2}), \tag{B.7}$$

implying that there are $O(2^d) = O(2^{2^n})$ nearly orthogonal states.

C More complexity bounds

In this appendix we consider complexity lower bounds for when gates can be applied in parallel section C.1 and for disordered Hamiltonian systems at early times section C.2.

C.1 Circuit depth

In Theorem 6, the complexity $\mathcal{C}(\mathcal{E})$ was defined as the number of steps required to generate the ensemble \mathcal{E} when only a single two-qubit gate from the gate set can be applied at each step. Yet, quantum gates may be applied in parallel if they do not act on the same qubits. By allowing simultaneous applications of quantum gates, we can instead consider the minimum quantum circuit depth $\mathcal{D}(\mathcal{E})$ to generate \mathcal{E} and obtain a lower bound with a very similar argument. At each step, we can pair up the qubits in $\binom{n}{q} \binom{n-q}{q} \binom{n-2q}{q} \dots \binom{q}{q} = n!/(q!)^{n/q}$ different ways (assuming n is divisible by q for simplicity). So, in a depth 1 circuit there are roughly $gn!/(q!)^{n/q}$ choices.³⁶ Thus, the lower bound on the depth is

$$\mathcal{D}(\mathcal{E}) \geq \frac{2kn \log(2) - \log F_{\mathcal{E}}^{(k)}}{\log(g) + n \log(n) - (n/q) \log(q!)}. \tag{C.1}$$

For $q \ll n$, the denominator is $\log g + n \log(n)$. For large n, q , the denominator goes like $\log g + n \log(n/q)$. Essentially, the effect of large q is only important if there's larger than an exponential number of gates $g \gtrsim 2^n$.

³⁵Part of this presentation follows a nice talk given by Adam Brown [84].

³⁶We thank Fernando Brandao for this suggestion.

C.2 Early times

Here, we consider complexity lower bounds for disordered Hamiltonian systems at early times. This discussion is intended to be completely general, but for concreteness you may imagine that we are referring to the ensemble implied by time evolving with the Sachdev-Ye-Kitaev Hamiltonian [58–60]

$$H = (i)^{q/2} \sum_{1 \leq i_1 < \dots < i_q \leq N} j_{i_1 \dots i_q} \psi_{i_1} \dots \psi_{i_q}, \quad \overline{j_{i_1 \dots i_q}^2} = \frac{\mathcal{J}^2}{q} \frac{2^{q-1}}{\binom{N-1}{q-1}}, \quad (\text{C.2})$$

where the overline denotes an ensemble average. The model consists of N Majorana fermions ψ_i , and each term in the Hamiltonian involves q of the fermions interacting with a random coupling independently picked from a Gaussian with variance $\overline{j_{i_1 \dots i_q}^2}$.

We want to understand the initial growth of complexity of an ensemble of time evolution operators $\mathcal{E}(t) = \{e^{-iHt}\}$, where H is disordered e.g. defined by eq. (C.2). In general, we assume that $\text{tr}\{\overline{H}\} = 0$, and so the first nontrivial moment is the second moment. Start by expanding $U_i(t) = e^{-iH_i t}$ and $V_j(t) = e^{-iG_j t}$ for early times

$$U_i(t) = 1 - iH_i t - \frac{1}{2}H_i^2 t^2 + \dots, \quad V_j(t) = 1 - iH_j t - \frac{1}{2}H_j^2 t^2 + \dots \quad (\text{C.3})$$

Plugging in to the definition of the frame potential, we get

$$F_{\mathcal{E}}^{(k)}(t) = \sum_{i,j} p_i p_j d^{2k} \left| 1 + \frac{t^2}{d} \left(\text{tr}\{H_i H_j\} - \frac{1}{2} \text{tr}\{H_i^2\} - \frac{1}{2} \text{tr}\{H_j^2\} \right) + \dots \right|^{2k}. \quad (\text{C.4})$$

Next, we use the fact that $\text{tr}\{\overline{H_i H_i}\} = 0$ by independence, and expand assuming $t^2 \text{tr}\{H^2\} \ll d$ to get an expression for the frame potential

$$F_{\mathcal{E}}^{(k)}(t) = d^{2k} \left(1 - \frac{2kt^2}{d} \text{tr}\{\overline{H^2}\} + \dots \right). \quad (\text{C.5})$$

This implies a lower bound on the initial growth of complexity of³⁷

$$\mathcal{C}(t) > \frac{2kt^2}{d} \text{tr}\{\overline{H^2}\}, \quad (\text{C.6})$$

valid for early times such that $\text{tr}\{\overline{H^2}\} t^2/d \ll 1$. For the SYK model eq. (C.2), we have $\text{tr}\{\overline{H^2}\} = \mathcal{J}^2 d(N/2q^2)$, and $\mathcal{C}(t) > k(\mathcal{J}t)^2(N/q^2)$ for times $t \ll \sqrt{2q^2/\mathcal{J}^2 N}$.

Thus, while complexity is expected to eventually grow linearly in time [50, 51], for early times our bound predicts a quadratic phase of growth.

D More Haar random averages

In this appendix, we present the details of the Haar random averages of 8-point OTO correlators as well as an argument for the scaling with d of higher-point functions.

³⁷We thank Jordan Cotler for discussions.

D.1 8-point functions

A general formula to compute the Haar average of $2k$ -point OTO correlators is

$$\begin{aligned} &\langle A_1 \tilde{B}_1 \dots A_k \tilde{B}_k \rangle_{\text{Haar}} \\ &= \frac{1}{d} \sum_{\pi, \sigma} \text{Wg}(\pi\sigma) \text{tr}\{W_\pi W_{\text{cyc}}(A_1 \otimes \dots \otimes A_k)\} \text{tr}\{W_\sigma(B_1 \otimes \dots \otimes B_k)\}, \end{aligned} \quad (\text{D.1})$$

where $\text{Wg}(\pi)$ is the Weingarten function. Because of the Weingarten function, this is difficult to evaluate.

The unitary Weingarten function on S_n is given by [55]

$$\text{Wg} = \frac{1}{n!} \sum_{\lambda} \frac{f^\lambda}{s_\lambda} \chi^\lambda, \quad (\text{D.2})$$

where summation is over all partitions λ of n . s_λ is a polynomial in d given by

$$s_\lambda = \prod_{i=1}^{l(\lambda)} \prod_{j=1}^{\lambda_i} (d + j - i), \quad (\text{D.3})$$

where $l(\lambda)$ is the length of λ . f^λ is the dimension of the irreducible representation associated with λ . χ^λ is the irreducible characters.

For S_2 , the character table is given by

	(1, 1)	(2)	
(2)	1	-1	.
(1, 1)	1	1	

We have

$$s_{(1,1)} = d(d-1), \quad s_{(2)} = d(d+1). \quad (\text{D.4})$$

Thus,

$$\begin{aligned} \text{Wg}(1, 1) &= \frac{1}{2} \left(\frac{1}{d(d-1)} + \frac{1}{d(d+1)} \right) = \frac{1}{d^2 - 1}, \\ \text{Wg}(2) &= \frac{1}{2} \left(\frac{-1}{d(d-1)} + \frac{1}{d(d+1)} \right) = \frac{-1}{d(d^2 - 1)}. \end{aligned} \quad (\text{D.5})$$

For S_3 , the character table is given by

	(1, 1, 1)	(2, 1)	(3)	
(3)	1	1	1	
(2, 1)	2	0	-1	.
(1, 1, 1)	1	-1	1	

We have

$$\begin{aligned} s_{(1,1,1)} &= d(d-1)(d-2), \\ s_{(2,1)} &= d(d+1)(d-1), \\ s_{(3)} &= d(d+1)(d+2). \end{aligned} \quad (\text{D.6})$$

Thus

$$\begin{aligned}
 \text{Wg}(1, 1, 1) &= \frac{1}{6} \left(\frac{1}{d(d-1)(d-2)} + \frac{4}{d(d+1)(d-1)} + \frac{1}{d(d+1)(d+2)} \right), \\
 &= \frac{d^2 - 2}{d(d^2 - 2)(d^2 - 4)}, \\
 \text{Wg}(2, 1) &= \frac{1}{6} \left(\frac{-1}{d(d-1)(d-2)} + \frac{1}{d(d+1)(d+2)} \right), \\
 &= \frac{-1}{(d^2 - 1)(d^2 - 4)}, \\
 \text{Wg}(3) &= \frac{1}{6} \left(\frac{1}{d(d-1)(d-2)} + \frac{-2}{d(d+1)(d-1)} + \frac{1}{d(d+1)(d+2)} \right), \\
 &= \frac{2}{d(d^2 - 1)(d^2 - 4)}.
 \end{aligned} \tag{D.7}$$

For S_4 , the character table is given by

	(1, 1, 1, 1)	(2, 1, 1)	(2, 2)	(3, 1)	(4)
(4)	1	1	1	1	1
(3, 1)	3	1	-1	0	-1
(2, 2)	2	0	2	-1	0
(2, 1, 1)	3	-1	-1	0	1
(1, 1, 1, 1)	1	-1	1	1	-1

We have

$$\begin{aligned}
 s_{(4)} &= d(d+1)(d+2)(d+3), \\
 s_{(3,1)} &= d(d+1)(d+2)(d-1), \\
 s_{(2,2)} &= d(d+1)(d-1)d, \\
 s_{(2,1,1)} &= d(d+1)(d-1)(d-2), \\
 s_{(1,1,1,1)} &= d(d-1)(d-2)(d-3).
 \end{aligned} \tag{D.8}$$

Thus

$$\begin{aligned}
 \text{Wg}(1, 1, 1, 1) &= \frac{d^4 - 8d^2 + 6}{d^2(d^2 - 1)(d^2 - 4)(d^2 - 9)}, \\
 \text{Wg}(2, 1, 1) &= \frac{-d^3 + 4d}{d^2(d^2 - 1)(d^2 - 4)(d^2 - 9)}, \\
 \text{Wg}(2, 2) &= \frac{d^2 + 6}{d^2(d^2 - 1)(d^2 - 4)(d^2 - 9)}, \\
 \text{Wg}(3, 1) &= \frac{2d^2 - 3}{d^2(d^2 - 1)(d^2 - 4)(d^2 - 9)}, \\
 \text{Wg}(4) &= \frac{-5d}{d^2(d^2 - 1)(d^2 - 4)(d^2 - 9)}.
 \end{aligned} \tag{D.9}$$

We also note here the large d asymptotic behavior

$$\text{Wg}(\lambda) \sim \frac{1}{d^{2n - \# \text{ of cycles in } \lambda}}. \tag{D.10}$$

We now will evaluate the following 8-point OTO correlator average of the commutator-type correlators

$$|8\text{-point}|_{\text{Haar}} = \left| \frac{1}{d} \text{tr} \{ A \tilde{B} C \tilde{D} C^\dagger \tilde{B}^\dagger A^\dagger \tilde{D}^\dagger \} \right|_{\text{Haar}}, \quad (\text{commutator type}) \quad (\text{D.11})$$

where $\tilde{B} = UBU^\dagger$ and $\tilde{D} = UDU^\dagger$. We assume that A, B, C, D are Pauli operators, $A, B, C, D \neq I$ and $AC, BD \neq I$. We write the correlator as

$$\frac{1}{d} \text{tr} \{ (A \otimes C \otimes C^\dagger \otimes A^\dagger) \Phi_4(B \otimes D \otimes B^\dagger \otimes D^\dagger) W_{2341} \}, \quad (\text{D.12})$$

where W_{2341} is a cyclic permutation. We have

$$\frac{1}{d} \sum_{\pi_1, \pi_2 \in S_4} \text{Wg}(\pi_1 \pi_2) \text{tr} \{ (A \otimes C \otimes C^\dagger \otimes A^\dagger) W_{\pi_1} W_{2341} \} \text{tr} \{ (B \otimes D \otimes B^\dagger \otimes D^\dagger) W_{\pi_2} \}. \quad (\text{D.13})$$

Let us assume that $[A, C] = [B, D] = 0$. This gives

$$\text{Wg}(1, 1, 1, 1)d^2 + \text{Wg}(2, 1, 1)(d^3 + 16d) + \text{Wg}(3, 1)7d^2 + \text{Wg}(2, 2)3d^2 + \text{Wg}(4)(d^2 + 20d). \quad (\text{D.14})$$

For large d , the coefficients $\text{Wg}(\pi)$ scales as follows

$$\text{Wg}(\pi) \sim O\left(\frac{1}{d^{8-\#\text{of cycles in } \pi}}\right). \quad (\text{D.15})$$

At first sight, the dominant contribution might seem to be $O\left(\frac{1}{d^2}\right)$

$$(\text{Wg}(1, 1, 1, 1) + \text{Wg}(2, 1, 1)d)d^2, \quad (\text{D.16})$$

but, due to nice cancellation, the above expression becomes

$$\begin{aligned} & \left(\frac{d^4 - 8d^2 + 6}{d^2(d^2 - 1)(d^2 - 4)(d^2 - 9)} + \frac{-d^3 + 4d}{d^2(d^2 - 1)(d^2 - 4)(d^2 - 9)} d \right) d^2, \\ & = \frac{-4d^2 + 6}{(d^2 - 1)(d^2 - 4)(d^2 - 9)}, \end{aligned} \quad (\text{D.17})$$

which is $O(d^{-4})$. Finally, we can write down the complete answer

$$|8\text{-point}|_{\text{Haar}} = \frac{-3d^2 - 5d - 33}{(d^2 - 1)(d^2 - 4)(d^2 - 9)}, \quad (\text{commutator type}), \quad (\text{D.18})$$

which scales as $O(d^{-4})$ for large d . We have also checked other commutation relations between A, B, C, D , and although the exact form of the answer is different, the scaling is always $O(d^{-4})$.

Next, let us evaluate the Haar average of the non-commutator type 8-point OTO correlators

$$|8\text{-point}|_{\text{Haar}} = \left| \frac{1}{d} \text{tr} \{ A \tilde{B} C \tilde{D} A^\dagger \tilde{B}^\dagger C^\dagger \tilde{D}^\dagger \} \right|_{\text{Haar}}, \quad (\text{non-commutator type}), \quad (\text{D.19})$$

which we rewrite as

$$\frac{1}{d} \sum_{\pi_1, \pi_2 \in S_4} \text{Wg}(\pi_1 \pi_2) \text{tr}\{(A \otimes C \otimes A^\dagger \otimes C^\dagger) W_{\pi_1} W_{2341}\} \text{tr}\{(B \otimes D \otimes B^\dagger \otimes D^\dagger) W_{\pi_2}\}. \quad (\text{D.20})$$

The difference from the commutator type is that the first trace contains the operator $A \otimes C \otimes A^\dagger \otimes C^\dagger$ instead of the operator $A \otimes C \otimes C^\dagger \otimes A^\dagger$. Let us assume the commutation relations $[A, C] = [B, D] = 0$. Then we find

$$\text{Wg}(1, 1, 1, 1)2d^2 + \text{Wg}(2, 1, 1)16d + \text{Wg}(3, 1)8d^2 + \text{Wg}(2, 2)(2d^2) + \text{Wg}(4)(d^3 + 20d) \quad (\text{D.21})$$

which scales as $O(d^{-2})$. For other choices of commutation relations, it's easy to check that the scaling is always $O(d^{-2})$.

D.2 Higher-point functions

Finally, we will make a conjecture regarding the behaviors of higher-point OTO correlation functions. We speculate that $4m$ -point OTO correlators of the commutator-type form

$$\langle A_1(\tilde{B}_1 \cdots A_m \tilde{B}_m) A_1^\dagger(\tilde{B}_1 \cdots A_m \tilde{B}_m)^\dagger \rangle, \quad (\text{commutator type}), \quad (\text{D.22})$$

will have the following asymptotic scaling.

Conjecture 1. *The $4m$ -point OTO correlation functions asymptotically scale as*

$$\langle A_1(\tilde{B}_1 \cdots A_m \tilde{B}_m) A_1^\dagger(\tilde{B}_1 \cdots A_m \tilde{B}_m)^\dagger \rangle_{\text{Haar}} \sim \frac{1}{d^{2m}}, \quad (\text{D.23})$$

when averaged over Haar random unitary operators.

For $m = 1, 2$, we recover the analytical results we have already obtained. Below, we provide a supporting argument for this conjecture.

First, let's consider 8-point functions using the method from section 5. We are interested in computing the following quantity

$$\text{OTO}^{(8)}(A_1, B_1, A_2, B_2) = \langle A_1 \tilde{B}_1 A_2 \tilde{B}_2 A_2^\dagger \tilde{B}_1^\dagger A_1^\dagger \tilde{B}_2^\dagger \rangle_{\text{Haar}}, \quad B_1, B_2 \neq I, \quad A_1 A_2 \neq I. \quad (\text{D.24})$$

From a simple calculation, we find

$$\sum_{B_1} \text{OTO}^{(8)}(A_1, B_1, A_2, B_2) = 0, \quad B_2 \neq I. \quad (\text{D.25})$$

If $B_1 = I$, we have

$$\text{OTO}^{(8)}(A_1, I, A_2, B_2) = \langle A_1 A_2 \tilde{B}_2 A_2^\dagger A_1^\dagger \tilde{B}_2^\dagger \rangle_{\text{Haar}} = \text{OTO}^{(4)}(A_1 A_2, B_2) = -\frac{1}{d^2 - 1}, \quad (\text{D.26})$$

since $A_1 A_2 \neq I$ and $B_2 \neq I$. Thus, we have

$$|\text{OTO}^{(8)}(A_1, B_1, A_2, B_2)|_{B_1, B_2 \neq I, A_1 A_2 \neq I} = \frac{1}{(d^2 - 1)^2}. \quad (\text{D.27})$$

This method shows what we already know, that the Haar average of commutator-type 8-point OTO correlators equals $\sim d^{-4}$.

Now, let us consider the Haar average of commutator-type $4m$ -point OTO correlation functions³⁸

$$\text{OTO}^{(4m)}(A_1, B_1, \dots, A_m, B_m) = \langle A_1 \tilde{B}_1 \cdots A_m \tilde{B}_m A_m^\dagger B_{m-1} \tilde{A}_{m-1}^\dagger \cdots \tilde{B}_1^\dagger A_1^\dagger \tilde{B}_m^\dagger \rangle_{\text{Haar}}. \quad (\text{D.28})$$

By a recursive argument, we can show the following

$$\text{OTO}^{(4m)}(A_1, B_1, \dots, A_m, B_m)|_{B_1, B_2, \dots, B_k \neq I, A_1 A_2 \cdots A_k \neq I} = \left(\frac{-1}{d^2 - 1} \right)^k. \quad (\text{D.29})$$

The average of $\text{OTO}(A_1, B_1, \dots, A_m, B_m)$ over B_1 is zero as long as $B_m \neq I$. If $B_1 = I$, then we have

$$\text{OTO}^{(4m)}(A_1, I, \dots, A_m, B_m) = \text{OTO}^{(4m-4)}(A_1 A_2, B_2, \dots, A_m, B_m). \quad (\text{D.30})$$

Thus, we see

$$\text{OTO}^{(4m)}(A_1, B_1, \dots, A_m, B_m)|_{B_1, \dots, B_k \neq I, A_1 \cdots A_k \neq I} \quad (\text{D.31})$$

$$= \left(\frac{-1}{d^2 - 1} \right) \text{OTO}^{(4m-4)}(A_1 A_2, B_2, \dots, A_{m-1}, B_{m-1})|_{B_2, \dots, B_k \neq I, A_1 \cdots A_k \neq I}. \quad (\text{D.32})$$

This argument suggests that the Haar average of $4m$ -point OTO correlators have a scaling $\sim d^{-2m}$. One would need to evaluate the Weingarten function for S_{2m} in order to check this exactly, and we will not attempt to do that. In particular, the Haar average of $\text{OTO}^{(4)}(A, B)$ does not depend on A, B as long as $A, B \neq I$. For 8-point or higher-point OTO correlators, $\text{OTO}^{(4m)}(A_1, B_1, \dots, A_m, B_m)$ depends on the details of $A_1, B_1, \dots, A_m, B_m$, even when we impose $B_1, \dots, B_k \neq I$ and $A_1 \cdots A_k \neq I$. Namely, this suggests that the exact result will depend on the commutation relations of the A_j and B_j , and we do not know an exact form of dependence. Our argument can only tell us that eq. (D.29) has a value that scales as $O(d^{-2m})$.

Finally, for these commutator-type higher-point OTO correlators, we can compute Clifford averages easily

$$\langle A_1 (\tilde{B}_1 \cdots A_m \tilde{B}_m) A_1^\dagger (\tilde{B}_1 \cdots A_m \tilde{B}_m)^\dagger \rangle_{\text{Clifford}} \sim \frac{1}{d^2}, \quad (\text{commutator type}), \quad (\text{D.33})$$

by using the fact that A_j and \tilde{B}_j are Pauli operators. This supports our belief that higher-point correlators might be useful probes of whether an ensemble forms a k -design but does not form a higher-design.

³⁸The ordering here is inspired by the correlators considered in [16] and is related to a 2-point correlation function in an AdS black hole geometry perturbed by $(2m - 1)$ -shock waves.

E More (general) frame potentials

In this appendix, we generalize the notion of unitary design for states described by an arbitrary density matrix ρ . We will find two possible generalizations of the frame potential:

$$\mathcal{F}_{\mathcal{E}}^{(k)}(\rho) = \iint dU dV [\text{tr}\{\rho^{1/k}UV^\dagger\} \text{tr}\{\rho^{1/k}VU^\dagger\}]^k, \quad (\text{E.1})$$

$$\mathcal{G}_{\mathcal{E}}^{(k)}(\rho) = \iint dU dV [\text{tr}\{\rho^{1/k}UV^\dagger\} \text{tr}\{\rho^{1/k}U^\dagger V\}]^k. \quad (\text{E.2})$$

The difference is the ordering of V and U^\dagger in the second trace. For the maximally mixed state $\rho = \frac{I}{d}$, both expressions are reduced to the original frame potential $F_{\mathcal{E}}^{(k)}$ up to factor of proportionality:

$$\mathcal{F}_{\mathcal{E}}^{(k)}\left(\frac{I}{d}\right) = \mathcal{G}_{\mathcal{E}}^{(k)}\left(\frac{I}{d}\right) = \frac{1}{d^2} F_{\mathcal{E}}^{(k)}. \quad (\text{E.3})$$

However, the two expressions behave quite differently when ρ is not the maximally mixed state. Below, we explain how we arrived at these expressions and study their basic properties such as their Haar average values and the fact that they are minimized when the ensemble is a k -design. Our conclusion is that the first expression, $\mathcal{F}_{\mathcal{E}}^{(k)}$, seems to be a more appropriate generalization of the frame potential.

Properties

The original k th frame potential, defined for $\rho \propto I$, is minimized if and only if the unitary ensemble \mathcal{E} is a k -design. We expect any sensible generalization of the frame potential should have similar minimization property. If so, then e.g. if $\mathcal{F}_{\mathcal{E}}^{(k)}(\rho) = \mathcal{F}_{\text{Haar}}^{(k)}(\rho)$, we can think of the ensemble \mathcal{E} as forming k -design with respect to the state ρ . We prove the following lemma.

Lemma 1. *For generalized frame potentials $\mathcal{F}_{\mathcal{E}}^{(k)}(\rho)$ and $\mathcal{G}_{\mathcal{E}}^{(k)}(\rho)$, we have*

$$\mathcal{F}_{\mathcal{E}}^{(k)}(\rho) \geq \mathcal{F}_{\text{Haar}}^{(k)}(\rho), \quad \mathcal{G}_{\mathcal{E}}^{(k)}(\rho) \geq \mathcal{G}_{\text{Haar}}^{(k)}(\rho), \quad (\text{E.4})$$

with equality if \mathcal{E} is a k -design.

Proof. We begin with $\mathcal{G}^{(k)}$. Consider the following operator

$$S \equiv \int_{\mathcal{E}} dU (U)^{\otimes k} \otimes (U^\dagger)^{\otimes k} - \int_{\text{Haar}} dU (U)^{\otimes k} \otimes (U^\dagger)^{\otimes k}. \quad (\text{E.5})$$

Observe

$$\text{tr}\{(\rho^{1/k} \otimes \rho^{1/k} \otimes \dots)SS^\dagger\} = \mathcal{G}_{\mathcal{E}}^{(k)}(\rho) - \mathcal{G}_{\text{Haar}}^{(k)}(\rho) \geq 0. \quad (\text{E.6})$$

For $\mathcal{F}^{(k)}$, consider the following quantity

$$\text{tr}\{\sigma_L S \sigma_R S^\dagger\} = \mathcal{F}_{\mathcal{E}}^{(k)}(\rho) - \mathcal{F}_{\text{Haar}}^{(k)}(\rho) \quad (\text{E.7})$$

where $\sigma_L = (\rho^{1/k})^{\otimes k} \otimes (I)^{\otimes k}$ and $\sigma_R = (I)^{\otimes k} \otimes (\rho^{1/k})^{\otimes k}$. Define

$$X = \sigma_L^{1/2} S \sigma_R^{1/2}, \quad X^\dagger = \sigma_R^{1/2} S^\dagger \sigma_L^{1/2}. \quad (\text{E.8})$$

We then have

$$\text{tr}\{\sigma_L S \sigma_R S^\dagger\} = \text{tr}\{X X^\dagger\} \geq 0. \quad (\text{E.9})$$

□

In section 3, we showed that the k th frame potential is proportional to the average of certain $2k$ -point OTO correlators, where the correlators are evaluated for maximally mixed states. Here, we compute an average of OTO correlators for general ρ to derive a candidate expression of generalized frame potential. Inspired by [4], we consider regulated OTO correlators of the form

$$\langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle_\rho = \text{tr}\{\rho^{1/2k} A_1 \rho^{1/2k} \tilde{B}_1 \cdots \rho^{1/2k} A_k \rho^{1/2k} \tilde{B}_k\}, \quad (\text{E.10})$$

instead of unregulated correlators

$$\langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle_{\rho, \text{unregulated}} = \text{tr}\{\rho A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k\}. \quad (\text{E.11})$$

When ρ is the thermal density matrix, eq. (E.10) uniformly distributes the operators around the thermal circle. Using eq. (E.10), it is not difficult to prove the following lemma.

Lemma 2. *For regulated $2k$ -point OTO correlators, we have*

$$\sum_{A_1, B_1, \dots} |\langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle_\rho|^2 \propto \mathcal{F}^{(k)}(\rho). \quad (\text{E.12})$$

This is one of our motivations for considering $\mathcal{F}^{(k)}(\rho)$ as the proper generalization of the frame potential.³⁹ Also, we note that due to the fact that the maximally mixed state is normalized with a factor of $1/d$, for these generalized frame potentials the scaling with respect to d is a bit different from the original definition of the frame potential $F^{(k)}$. For a maximally mixed state ($\rho = I/d$), we have

generalized	original	ensemble	
$\mathcal{F}^{(k)} = d^{2(k-1)},$	$F^{(k)} = d^{2k},$	$\mathcal{E} = \{I\},$	(E.14)
$\mathcal{F}^{(k)} = \frac{k!}{d^2},$	$F^{(k)} = k!,$	$\mathcal{E} = \text{Haar}.$	(E.15)

³⁹From an operational viewpoint, it might be more sensible to define $\mathcal{F}_\mathcal{E}^{(k)}(\rho)$ with $\rho^{1/k} \rightarrow \rho$

$$\mathcal{F}_\mathcal{E}^{(k)}(\rho) = \iint dU dV [\text{tr}\{\rho U V^\dagger\} \text{tr}\{\rho V U^\dagger\}]^k, \quad (\text{E.13})$$

so that there is one ρ per trace. However, this means that the correlators eq. (E.10) will have many copies of ρ . This is similar to what happens when using correlators to compute Rényi entropies.

Next, we will analyze the properties of $\mathcal{F}_{\mathcal{E}}^{(1)}(\rho)$ for arbitrary ρ . First, we compute the Haar value:

$$\mathcal{F}_{\text{Haar}}^{(1)}(\rho) = \frac{\text{tr}\{\rho^2\}}{d}. \quad (\text{E.16})$$

Thus, it behaves differently on pure states vs. mixed states, e.g.

$$\mathcal{F}_{\text{Haar}}^{(1)} = \frac{1}{d}, \quad (\text{pure state}), \quad (\text{E.17})$$

$$\mathcal{F}_{\text{Haar}}^{(1)} = \frac{1}{d^2}, \quad (\text{maximally mixed state}). \quad (\text{E.18})$$

For $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle = |0\rangle^{\otimes n}$, we find that random Pauli- X operators, operators that can either act as X or I on each qubit, achieve the Haar value. To see this, we can evaluate $\text{tr}\{|\psi\rangle\langle\psi|UV^\dagger\}$. Since we choose U and V randomly from a set of Pauli- X operators, then $UV^\dagger|\psi\rangle$ will be given by a random product state $|a_1, \dots, a_n\rangle$ with the $a_j = 0, 1$. Since $\text{tr}\{|\psi\rangle\langle\psi|UV^\dagger\} = \langle 0, \dots, 0 | a_1, \dots, a_n \rangle$, the non-zero contribution has probability $1/d$. This means that $\mathcal{F}_{\text{Pauli-}X}^{(1)} = 1/d$, which is the Haar value. Finally, as before we can use the generalized frame potential to bound the size of the ensemble

$$\mathcal{F}_{\mathcal{E}}^{(1)}(\rho) = \frac{1}{|\mathcal{E}|^2} \sum_{U, V \in \mathcal{E}} |\text{tr}\{\rho UV^\dagger\}|^2 \geq \frac{1}{|\mathcal{E}|} |\text{tr}\{\rho\}|^2 = \frac{1}{|\mathcal{E}|} \rightarrow |\mathcal{E}| \geq \frac{1}{\mathcal{F}_{\mathcal{E}}^{(1)}(\rho)}. \quad (\text{E.19})$$

Note that random Pauli- X operators for $\rho = |0\rangle\langle 0|$ are tight in terms of this lower bound since there are exactly d different Pauli X operators.

Next, we will analyze the properties of $\mathcal{G}_{\mathcal{E}}^{(1)}(\rho)$. As before, first we compute the Haar value of $\mathcal{G}_{\mathcal{E}}^{(1)}(\rho)$:

$$\mathcal{G}_{\text{Haar}}^{(1)}(\rho) = \frac{\text{tr}\{\rho\}^2}{d^2} = \frac{1}{d^2}. \quad (\text{E.20})$$

Note that the result does not depend on ρ . The cardinality bound gives

$$|\mathcal{E}| \geq \frac{1}{\mathcal{G}^{(1)}}. \quad (\text{E.21})$$

Thus, to become a k -design requires $|\mathcal{E}| \geq d^2$. Note that this is a tight lower bound since a set of all the Pauli operators consists of d^2 different operators. Therefore, the minimization of $\mathcal{G}^{(1)}$ requires a 1-design, regardless of ρ .

The fact that all these properties of $\mathcal{G}^{(1)}$ are independent of the state ρ , in conjunction with Lemma 2, suggests that $\mathcal{F}^{(k)}$ is the more interesting generalization of the frame potential. As a result, we will continue by focusing only on $\mathcal{F}^{(k)}$.

We continue by considering $\mathcal{F}_{\text{Haar}}^{(2)}$. The Haar value is

$$\mathcal{F}_{\text{Haar}}^{(2)}(\rho) = \frac{2 \text{tr}\{\rho\}^2}{d^2 - 1} - \frac{2 \text{tr}\{\rho^2\}}{d(d^2 - 1)}. \quad (\text{E.22})$$

We can evaluate this for a maximally mixed state $\rho = I/d$ and for a pure state $\rho = |\psi\rangle\langle\psi|$, finding

$$\mathcal{F}_{\text{Haar}}^{(2)} = \frac{2}{d^2}, \quad (\text{maximally mixed state}). \quad (\text{E.23})$$

$$\mathcal{F}_{\text{Haar}}^{(2)} = \frac{2}{d(d+1)}, \quad (\text{pure state}). \quad (\text{E.24})$$

On the other hand, the maximum is given by evaluating $\mathcal{F}^{(2)}$ for a trivial ensemble, i.e. $\mathcal{E} = \{I\}$

$$\mathcal{F}_{\{I\}}^{(2)} = \text{tr}\{\rho^{1/2}\}^4 = d^2, \quad (\text{maximally mixed state}). \quad (\text{E.25})$$

$$\mathcal{F}_{\{I\}}^{(2)} = 1, \quad (\text{pure state}). \quad (\text{E.26})$$

While the minimal values of $\mathcal{F}_{\mathcal{E}}^{(2)}(\rho)$ are of the same order regardless of the state ρ , we see that the maximum values are significantly different.

Finally, there is an easy way to compute the minimal value of the generalized frame potential $\mathcal{F}^{(k)}$ for any pure state e.g. $\rho = |0\rangle\langle 0|$. Let us write the frame potential as follows

$$\mathcal{F}_{\mathcal{E}}^{(k)}(|0\rangle\langle 0|) = \frac{1}{|\mathcal{E}|^2} \sum_{U,V} [\langle 0|UV^\dagger|0\rangle\langle 0|VU^\dagger|0\rangle]^k. \quad (\text{E.27})$$

Next, we define an ensemble of wavefunctions

$$\mathcal{E}_{|0\rangle} = \{U|0\rangle : U \in \mathcal{E}\}. \quad (\text{E.28})$$

The frame potential is given by expression

$$\mathcal{F}_{\mathcal{E}}^{(k)}(|0\rangle\langle 0|) = \frac{1}{|\mathcal{E}|^2} \sum_{|\psi\rangle, |\phi\rangle \in \mathcal{E}_{|0\rangle}} |\langle\psi|\phi\rangle|^{2k}. \quad (\text{E.29})$$

This is minimized when $\mathcal{E}_{|0\rangle}$ forms a k -design as an ensemble of quantum states. To obtain the Haar value, recall eq. (2.26) for the k -fold average of a Haar random state

$$\int_{\text{Haar}} (|\psi\rangle\langle\psi|)^{\otimes k} d\psi = \frac{\Pi_{\text{sym}}}{\binom{k+d-1}{k}}, \quad (\text{E.30})$$

where $\Pi_{\text{sym}} = \frac{1}{k!} \sum_{\pi \in S_k} W_\pi$. From this, we see that the Haar value of $\mathcal{F}^{(k)}$ evaluated on a pure state will be

$$\mathcal{F}_{\text{Haar}}^{(k)}(|0\rangle\langle 0|) = \left(\binom{k+d-1}{k} \right)^{-1}. \quad (\text{E.31})$$

In summary, we have

$\mathcal{F}_{\mathcal{E}}^{(k)}(\rho)$	$\rho = 0\rangle\langle 0 $	$\rho = \frac{I}{d}$	(E.32)
$\mathcal{E} = \{I\}$	1	$d^{2(k-1)}$	
$\mathcal{E} = \text{Haar}$	$\left(\binom{k+d-1}{k} \right)^{-1}$	$\frac{k!}{d^2}$	

At large d , the Haar value for pure states averaged over the Haar ensemble scales like $\sim k!/d^k$, which for $k > 2$ is much smaller than for the Haar average of a mixed state. It's also interesting to point out that if we consider the time average of the generalized frame potential on a pure state $|+\rangle$, this is exactly equal to $k!/d^k$. Thus, in comparison to section 3.3, the time average of this generalized frame potential can actually obtain an almost Haar value with respect to $|+\rangle$.

Thermal frame potentials

The above generalization is incorrect for a system in a thermal state that evolves in time by an ensemble of Hamiltonians. This is because the thermal state $\rho_\beta = e^{-\beta H}/\text{tr}\{e^{-\beta H}\}$ depends on the Hamiltonian and thus the ensemble itself. Instead, we will define a *thermal* frame potential $\mathcal{W}_\beta^{(k)}(t)$ by taking an average over the squares of $2k$ -point OTO correlators as the definition. Define a collection of thermally regulated $2k$ -point OTO correlators as

$$\langle A_1(0)B_1(t) \cdots A_k(0)B_k(t) \rangle = \frac{\text{tr}\{e^{-\frac{\beta H}{2k}} A_1 e^{-\frac{\beta H}{2k}} B_1(t) \cdots e^{-\frac{\beta H}{2k}} A_k e^{-\frac{\beta H}{2k}} B_k(t)\}}{\text{tr}\{e^{-\beta H}\}}. \quad (\text{E.33})$$

By first averaging over Hamiltonians and then taking an average over all choices of operators of the norm squared of these correlators, we find

$$\mathcal{W}_\beta^{(k)}(t) = \iint dGdH \frac{|\text{tr}\{e^{-(\beta/2k-it)G} e^{-(\beta/2k+it)H}\}|^{2k}}{\text{tr}\{e^{-\beta G}\}\text{tr}\{e^{-\beta H}\}}. \quad (\text{E.34})$$

For $\beta = 0$ (infinite temperature) the thermal frame potential reduces to the original frame potential $F^{(k)}$ up to a factor of proportionality

$$\mathcal{W}_{\beta=0}^{(k)}(t) = \frac{1}{d^2} \iint dGdH |\text{tr}\{e^{iGt} e^{-iHt}\}|^{2k} = \frac{1}{d^2} F^{(k)} = \mathcal{F}^{(k)}\left(\frac{I}{d}\right), \quad (\text{E.35})$$

where $F^{(k)}$ is the original frame potential, $\mathcal{F}^{(k)}(I/d)$ is the generalized frame potential from the previous section, and both are evaluated on the ensemble $\mathcal{E}(t) = \{e^{-iHt}\}$.

We can also use $\mathcal{W}_\beta^{(k)}(t)$ to make a bound on the cardinality of the ensemble. For simplicity, let's assume that the ensemble $\mathcal{E}(t)$ is a discrete set of e^{-iHt} taken with a uniform weight. This let's us make a bound

$$\mathcal{W}_\beta^{(k)}(t) \geq \frac{1}{|\mathcal{E}(t)|^2} \sum_H \frac{\text{tr}\{e^{-\beta H/k}\}^{2k}}{\text{tr}\{e^{-\beta H}\}^2}, \quad (\text{E.36})$$

or in terms of the cardinality,

$$|\mathcal{E}(t)|^2 \geq \frac{1}{\mathcal{W}_\beta^{(k)}(t)} \sum_H \frac{\text{tr}\{e^{-\beta H/k}\}^{2k}}{\text{tr}\{e^{-\beta H}\}^2}. \quad (\text{E.37})$$

For $k = 1$, the bound takes a particularly simple form

$$|\mathcal{E}(t)| \geq \frac{1}{\mathcal{W}_\beta^{(k=1)}(t)}. \quad (\text{E.38})$$

One nice property of the thermal frame potential is that even when $t = 0$ we may obtain a non-trivial bound. For example, with $k = 1$ we can express the thermal frame potential as

$$\mathcal{W}_\beta^{(1)}(0) = \iint dGdH \frac{\text{tr} \{e^{-\frac{\beta}{2}G} e^{-\frac{\beta}{2}H}\}^2}{\text{tr} \{e^{-\beta G}\} \text{tr} \{e^{-\beta H}\}}. \tag{E.39}$$

If $\beta = 0$, the bound is trivial $|\mathcal{E}(0)| \geq 1$. However, if $\beta > 0$ the thermal frame potential can be smaller than unity, which gives a non-trivial lower bound on $|\mathcal{E}(0)|$! We can see this straightforwardly by applying the Cauchy-Schwartz inequality to the integrand of eq. (E.39)

$$\frac{\text{tr} \{e^{-\frac{\beta}{2}G} e^{-\frac{\beta}{2}H}\}^2}{\text{tr} \{e^{-\beta G}\} \text{tr} \{e^{-\beta H}\}} \leq 1. \tag{E.40}$$

The intuition for such a lower bound at $t = 0$ comes from the fact that $e^{-\beta G}, e^{-\beta H}$ contain imaginary time evolution. We suspect that this will also let us bound the ‘‘complexity of formation’’ of such states ρ_β with respect to an ensemble of Hamiltonians.

F More chaos in quantum channels

Finally, in this appendix we expand on some of the results of [7] that are otherwise somewhat outside the main focus of the current paper:

- In section F.1, we revisit the black hole thought experiment of Hayden and Preskill [1] and discuss its relationship to the decay of OTO four-point functions.
- Next, in section F.2 we provide an operational meaning to taking averages over OTO correlation functions as introduced in [7]. The argument is partly inspired by a course taught by Kitaev [52].
- Finally, in section F.3 we generalize the relationship between OTO correlators and Rényi entropy obtained in [7] relating an average over $2k$ -point functions and to an expression involving the k th Rényi entropy.

F.1 OTO correlators and black holes as mirrors

In the conventional black hole information thought experiment, Alice throws some quantum state (or herself!) into a black hole, the system evolves by some chaotic unitary operator U , and then Bob attempts to reconstruct Alice’s quantum state (or Alice!) by collecting the outgoing Hawking radiation emitted by the black hole.

Hayden and Preskill [1] added an interesting twist to this classic setup by assuming that Bob knows both the initial state and the dynamics U of the black hole. In this scenario, they showed that if the dynamics U are sampled from a 2-design, Alice’s m -qubit quantum state can be immediately reconstructed by collecting $m + \epsilon$ qubits of the Hawking radiation. The black hole acts as if it is a quantum information mirror, ‘‘reflecting’’ Alice’s state almost immediately.

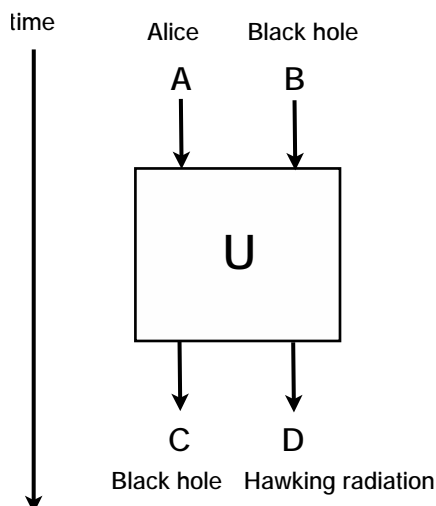


Figure 5. A unitary operator U representing the dynamics in the Hayden-Preskill thought experiment.

To be more precise, let's split the input state into subsystems A and B , and let's split the output state into different subsystems C and D . We let A represent Alice or her input quantum state, B represents initial black hole state, C represents the remaining black hole state after some evolution and evaporation, and D represents the emitted Hawking radiation. The black hole dynamics U take AB to CD . This setup is shown in figure 5. In the conventional setting, Bob has an access to only D . However, in the Hayden-Preskill modification, Bob has access to both B and D .

The mirror phenomenon can be better understood by interpreting the unitary operator U as a state via the Choi-Jamilkowski isomorphism [7]

$$U = \sum_{i,j} u_{ij} |i\rangle\langle j| \quad \rightarrow \quad |U\rangle = \frac{1}{2^{n/2}} \sum_{i,j} u_{ij} |j\rangle \otimes |i\rangle. \tag{F.1}$$

The original operator U acts unitarily on n -qubit states, while the state $|U\rangle$ is defined on a $2n$ -qubit Hilbert space. This interpretation lets us compute entropies and informations between the input and the output. In particular, whether Bob is able to reconstruct Alice's quantum state A can be quantified by the mutual information

$$I(A : BD) = S_A + S_{BD} - S_{ABD}, \tag{F.2}$$

where e.g. $S_A = -\text{tr} \{ \rho_A \log \rho_A \}$ is the entanglement entropy evaluated on the density matrix $\rho_A = \text{tr}_{BCD} \{ |U\rangle\langle U| \}$. If $I(A : BD)$ is near its maximal value $2S_A$, then Bob can reconstruct Alice's unknown quantum state.⁴⁰ It's easy to show that for a 2-design unitary operator U that the mutual information is close to its maximum $I(A : BD) \approx 2S_A$, thus enabling reconstruction of Alice's quantum state [1].

⁴⁰Here we assumed $S_A \leq S_B, S_D$. For a more precise criteria, see ref. [1].

The information reconstruction problem is closely related to four-point OTO correlators. It was shown in [7] that four-point OTO correlation functions averaged over all Pauli operators in A and D is related to the second Rényi entropy by the formula

$$\int dAdD \langle A(0)D(t)A^\dagger(0)D^\dagger(t) \rangle = \frac{d}{d_{AdD}} 2^{-S_{AC}^{(2)}}, \quad (\text{F.3})$$

where $\int dAdD$ means an average over all Pauli operators in A and D , $S_{AC}^{(2)}$ is the Rényi-2 entropy for the joint region AC , and $d_A = 2^{S_A}$ is the Hilbert space dimension of A , etc. From a simple calculation, we obtain

$$-\log_2 \left\{ \int dAdD \langle A(0)D(t)A^\dagger(0)D^\dagger(t) \rangle \right\} = I^{(2)}(A : BD) \leq I^{(1)}(A : BD), \quad (\text{F.4})$$

where $I^{(2)}(A : BD) = S_A^{(2)} + S_{BD}^{(2)} - S_{ABD}^{(2)}$ is the Rényi-2 mutual information. This inequality holds since $S_A = S_A^{(2)}$, $S_{ABD} = S_{ABD}^{(2)} = S_C$, and $S_{BD}^{(2)} \leq S_{BD}$. The decay of all the four-point OTO correlators between Alice A and the Hawking radiation D implies a strong correlation between Alice A and BD (the subsystem that Bob has access to), thus establishing a direct link between four-point OTO correlators and the information reconstruction problem.

F.2 Operational interpretation

In this subsection, we attempt to provide an operational interpretation to sum over out-of-time-order correlation functions discussed in [7] and in this work.

Consider the following classical analogy. Alice and Bob are playing a game of catch, and Alice is about to throw the ball to Bob. However, Alice is known to cheat sometimes by perturbing the ball (she throws a mean spitball!), and so Bob would like to determine whether Alice has cheated. One way for Bob to check is to ask someone that he trusts, Charlie, to throw an identical ball to Bob. Then, Bob can compare the two balls and determine whether Alice has modified the ball. This setup is shown in figure 6. As we will explain, the average of all OTO correlators over the operators being correlated is closely related to the probability of Bob detecting Alice's perturbation.

In a quantum setting, we prepare the state $|EPR\rangle$ of n EPR pairs and give Alice one half of all the pairs so that Alice's density matrix ρ_A is a maximally mixed state. We give the other half of the pairs to Charlie. Thus, Charlie has a perfectly correlated copy of Alice's initial state for Bob to later compare against. Now, Alice applies a perturbation, the Pauli operators A_i with probability p_i , which corresponds to the following superoperator

$$\sum_i p_i A_i(\cdot)A_i^\dagger. \quad (\text{F.5})$$

Of course, included in this set is the identity operator I and an associated probability p_I that Alice does not modify her state.⁴¹

⁴¹If $p_I = 0$, then Bob would already know that Alice always applies a perturbation.

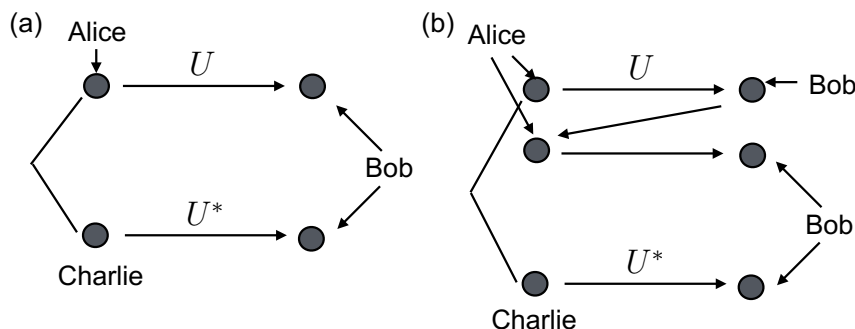


Figure 6. Alice and Bob play a game of catch, and Alice modifies the ball with some nonzero probability. **(a)** Charlie throws an identical but unmodified ball to Bob. This represents an average of 4-point OTO correlation functions. **(b)** Bob throws the ball back to Alice who then throws it back to Bob. This represents an average of 8-point OTO correlaton functions.

Next, Alice throws her ball to Bob by applying U , and Charlie throws his ball to Bob by applying U^* .⁴² The overall state is described by the statistical ensemble

$$\rho(p) = \sum_j p_j (U \otimes U^*)(A_i \otimes I) |EPR\rangle \langle EPR| (A_i^\dagger \otimes I) (U^\dagger \otimes U^T). \quad (\text{F.6})$$

Bob would like to compare the two quantum states from Alice and Charlie to determine whether Alice applied a perturbation. Note that if Alice did not apply a perturbation $A_i = I$, then the final state is equal to the initial state $|EPR\rangle$ because

$$U \otimes U^* |EPR\rangle = |EPR\rangle, \quad \forall U. \quad (\text{F.7})$$

Therefore, Bob's strategy is to perform a projective measurement $\Pi = |EPR\rangle \langle EPR|$ on his state. The projection operator $|EPR\rangle \langle EPR|$ can be represented as an average over all the Pauli operators on Bob's state:

$$\frac{1}{2^{2n}} \sum_{B_j \in \text{Pauli}} B_j \otimes B_j^* = |EPR\rangle \langle EPR|. \quad (\text{F.8})$$

Thus, the probability of Bob's measuring of $|EPR\rangle$ is given by

$$\frac{1}{2^{2n}} \sum_{i,j} p_i \langle EPR| (A_i^\dagger \otimes I) (U^\dagger \otimes U^T) (B_j \otimes B_j^*) (U \otimes U^*) (A_i \otimes I) |EPR\rangle = p_I, \quad (\text{F.9})$$

which is easy to check by making use of eq. (F.7). Eq. (F.9) is depicted graphically in figure 7, which makes it clear that we can interpret it as an average over four-point OTO correlators of the form⁴³

$$\frac{1}{2^{2n}} \sum_{i,j} p_i \langle \tilde{B}_j^\dagger A_i^\dagger \tilde{B}_j A_i \rangle = p_I. \quad (\text{F.10})$$

⁴²The conjugation appears because Charlie's copy of Alice's original state is actually a CPT conjugate. The application of U^* can be also interpreted as Bob's *uncomputation*.

⁴³Note that the result does not depend on the time evolution operator U since Bob performed measurements on the whole system.

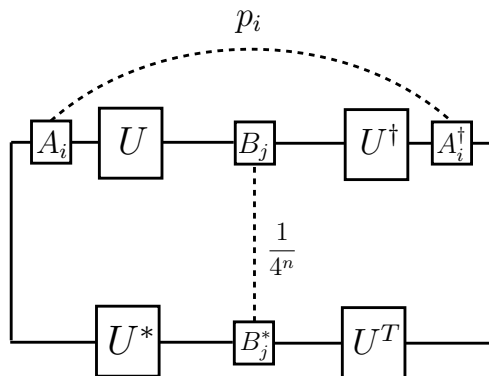


Figure 7. A graphical depiction of eq. (F.9) equal to the probability that Alice did not apply a perturbation, $p_i = p_I$ for $A_i = I$. Starting from the top left and reading clockwise, we see that this corresponds to an average over all choices of A_i, B_j of 4-point OTO correlators of the form $\langle A_i \tilde{B}_j A_i^\dagger \tilde{B}_j^\dagger \rangle$. Note that the average over A_i is with probabilities p_i , but the average over B_j is uniform with probabilities $p_j = 2^{-2n}$.

In the Hayden-Preskill setup, Bob performs a projective measurement $|EPR\rangle\langle EPR|$ only on qubits on D . Then, assuming that Alice applies perturbations A_i to qubits on A with equal probabilities, the probability of Bob’s measuring $|EPR\rangle$ on D is exactly given by eq. (F.3).

This game of “catch” can be “generalized” by considering multiple rounds of throwing the ball back and forth between Alice and Bob. In this case, both Alice and Bob have the option of applying perturbations at any round of the game (except for the final time Bob receives the ball), but Charlie always faithfully throws a copy of the original ball to Bob for comparison at the end. This process turns out to be equal to an average over $4m$ -point OTO correlators with the same ordering as those studied in section D.2. This setup, with $m = 2$ rounds of catch, is shown in figure 6(b).

F.3 Rényi- k entropy

Finally, we generalize the relationship between the second Rényi entropy and an average over four-point OTO correlators that was obtained in [7].⁴⁴ We will consider $2k$ -point OTO correlation functions of the form

$$\left\langle A_1 \tilde{D}_1 A_2 \tilde{D}_2 \cdots A_k \tilde{D}_k \right\rangle = \frac{1}{d} \text{tr} \left\{ A_1 \tilde{D}_1 A_2 \tilde{D}_2 \cdots A_k \tilde{D}_k \right\}. \quad (\text{F.11})$$

We assume that A_j and D_j only act on subsets of qubits, and we will denote these subregions by A and D , respectively.

We are interested in taking an average of correlators of the form eq. (F.11), where we will let one of the operators from each subregion A_k, D_k depend on the other operators such that the average gives a permutation operator (see eq. (2.7) and the discussion in section 2). In particular, to get a cyclic permutation $\pi_{\text{cyc}} = \pi_{23\dots k1}$, we will take an average

⁴⁴We thank Xiao-Liang Qi for providing useful insights leading to this generalization. Additionally, the possibility of such a generalization is briefly mentioned in [30].

in the following way

$$\frac{1}{d_A^{2(k-1)}} \sum_{\substack{A_1, \dots, A_{k-1} \in \mathcal{P}, \\ A_k = A_1^\dagger A_2^\dagger \dots A_{k-1}^\dagger}}, \quad (\text{F.12})$$

where $d_A^{2(k-1)}$ is the total number of Pauli operators A_1, \dots, A_{k-1} that we average over. We will denote such an average as follows

$$|\text{OTO}|_{\pi_A, \pi_D} = \left| \frac{1}{d} \text{tr} \left\{ A_1 \tilde{D}_1 A_2 \tilde{D}_2 \dots A_k \tilde{D}_k \right\} \right|_{\pi_A, \pi_D}, \quad (\text{F.13})$$

where the subscript notation π_A, π_D mean that we took the average such that $A_1 \otimes A_2 \otimes \dots \otimes A_k$ and $D_1 \otimes D_2 \otimes \dots \otimes D_k$ form the permutation operators associated with π_A, π_D .

Now, let us represent U as a state $|U\rangle$ by using the channel-state isomorphism eq. (F.1) discussed in section F.1. We divide the input into subsystems A and B , and we divide the output into subsystems C and D . Our key result is a formula relating an average over $2k$ -point OTO correlators with operators in A and D to the exponential of the k -th Rényi entropy of the subsystem AC

$$|\text{OTO}|_{\pi_{\text{cyc}}^{-1}, \pi_{\text{cyc}}} = \left(\frac{d}{d_A d_D} \right)^{k-1} 2^{-(k-1)S_{AC}^{(k)}}, \quad (\text{F.14})$$

with $S_{AC}^{(k)}$ the Rényi k -entropy of AC . To derive this, we also use the following relation

$$\text{tr} \left\{ A_1 \tilde{D}_1 \dots A_k \tilde{D}_k \right\} = \text{tr} \left\{ (A_1 \otimes \dots \otimes A_k) \cdot (\tilde{D}_1 \otimes \dots \otimes \tilde{D}_k) \cdot W_{\pi_{\text{cyc}}} \right\}, \quad (\text{F.15})$$

discussed in the beginning of section 3, or graphically

$$(\text{F.16})$$

From eq. (2.7) we know that taking an average of the form eq. (F.12) replaces $(A_1 \otimes \dots \otimes A_k)$ and $(\tilde{D}_1 \otimes \dots \otimes \tilde{D}_k)$ by permutation operators $W_{\pi_{\text{cyc}}^{-1}}$ and $W_{\pi_{\text{cyc}}}$, which act on A and D , respectively. Graphically, we have

$$(\text{F.17})$$

where $\pi_A = \pi_{\text{cyc}}^{-1}$ and $\pi_D = \pi_{\text{cyc}}$. Careful consideration of this picture elucidates that it is proportional to $\text{tr} \{ \rho_{AC}^k \}$.

Open Access. This article is distributed under the terms of the Creative Commons Attribution License ([CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/)), which permits any use, distribution and reproduction in any medium, provided the original author(s) and source are credited.

References

- [1] P. Hayden and J. Preskill, *Black holes as mirrors: quantum information in random subsystems*, *JHEP* **09** (2007) 120 [[arXiv:0708.4025](#)] [[INSPIRE](#)].
- [2] Y. Sekino and L. Susskind, *Fast scramblers*, *JHEP* **10** (2008) 065 [[arXiv:0808.2096](#)] [[INSPIRE](#)].
- [3] S.H. Shenker and D. Stanford, *Black holes and the butterfly effect*, *JHEP* **03** (2014) 067 [[arXiv:1306.0622](#)] [[INSPIRE](#)].
- [4] J. Maldacena, S.H. Shenker and D. Stanford, *A bound on chaos*, *JHEP* **08** (2016) 106 [[arXiv:1503.01409](#)] [[INSPIRE](#)].
- [5] N. Lashkari, D. Stanford, M. Hastings, T. Osborne and P. Hayden, *Towards the fast scrambling conjecture*, *JHEP* **04** (2013) 022 [[arXiv:1111.6580](#)] [[INSPIRE](#)].
- [6] A. Almheiri, D. Marolf, J. Polchinski, D. Stanford and J. Sully, *An apologia for firewalls*, *JHEP* **09** (2013) 018 [[arXiv:1304.6483](#)] [[INSPIRE](#)].
- [7] P. Hosur, X.-L. Qi, D.A. Roberts and B. Yoshida, *Chaos in quantum channels*, *JHEP* **02** (2016) 004 [[arXiv:1511.04021](#)] [[INSPIRE](#)].
- [8] F. Dupuis, M. Berta, J. Wullschleger and R. Renner, *One-shot decoupling*, *Comm. Math. Phys.* **328** (2014) 251 [[arXiv:1012.6044](#)].
- [9] W. Brown and O. Fawzi, *Decoupling with random quantum circuits*, *Comm. Math. Phys.* **340** (2015) 867.
- [10] . Chamon, A. Hamma and E.R. Mucciolo, *Emergent irreversibility and entanglement spectrum statistics*, *Phys. Rev. Lett.* **112** (2014) 240501 [[arXiv:1310.2702](#)].
- [11] P. Hayden, S. Nezami, X.-L. Qi, N. Thomas, M. Walter and Z. Yang, *Holographic duality from random tensor networks*, *JHEP* **11** (2016) 009 [[arXiv:1601.01694](#)] [[INSPIRE](#)].
- [12] A. Nahum, J. Ruhman, S. Vijay and J. Haah, *Quantum entanglement growth under random unitary dynamics*, [arXiv:1608.06950](#) [[INSPIRE](#)].
- [13] D.A. Roberts, D. Stanford and L. Susskind, *Localized shocks*, *JHEP* **03** (2015) 051 [[arXiv:1409.8180](#)] [[INSPIRE](#)].
- [14] A. Larkin and Y. Ovchinnikov, *Quasiclassical method in the theory of superconductivity*, *JETP* **28** (1969) 1200.
- [15] A. Kitaev, *Hidden correlations in the Hawking radiation and thermal noise*, talk given at the *Fundamental Physics Prize Symposium*, November 10 (2014).
- [16] S.H. Shenker and D. Stanford, *Multiple shocks*, *JHEP* **12** (2014) 046 [[arXiv:1312.3296](#)] [[INSPIRE](#)].
- [17] D.A. Roberts and D. Stanford, *Two-dimensional conformal field theory and the butterfly effect*, *Phys. Rev. Lett.* **115** (2015) 131603 [[arXiv:1412.5123](#)] [[INSPIRE](#)].
- [18] S.H. Shenker and D. Stanford, *Stringy effects in scrambling*, *JHEP* **05** (2015) 132 [[arXiv:1412.6087](#)] [[INSPIRE](#)].
- [19] D. Stanford, *Many-body chaos at weak coupling*, *JHEP* **10** (2016) 009 [[arXiv:1512.07687](#)] [[INSPIRE](#)].
- [20] A.L. Fitzpatrick and J. Kaplan, *A quantum correction to chaos*, *JHEP* **05** (2016) 070 [[arXiv:1601.06164](#)] [[INSPIRE](#)].
- [21] Y. Gu and X.-L. Qi, *Fractional statistics and the butterfly effect*, *JHEP* **08** (2016) 129 [[arXiv:1602.06543](#)] [[INSPIRE](#)].

- [22] P. Caputa, T. Numasawa and A. Veliz-Osorio, *Out-of-time-ordered correlators and purity in rational conformal field theories*, *PTEP* **2016** (2016) 113B06 [[arXiv:1602.06542](#)] [[INSPIRE](#)].
- [23] B. Swingle, G. Bentsen, M. Schleier-Smith and P. Hayden, *Measuring the scrambling of quantum information*, *Phys. Rev. A* **94** (2016) 040302 [[arXiv:1602.06271](#)] [[INSPIRE](#)].
- [24] E. Perlmutter, *Bounding the space of holographic CFTs with chaos*, *JHEP* **10** (2016) 069 [[arXiv:1602.08272](#)] [[INSPIRE](#)].
- [25] M. Blake, *Universal charge diffusion and the butterfly effect in holographic theories*, *Phys. Rev. Lett.* **117** (2016) 091601 [[arXiv:1603.08510](#)] [[INSPIRE](#)].
- [26] D.A. Roberts and B. Swingle, *Lieb-Robinson bound and the butterfly effect in quantum field theories*, *Phys. Rev. Lett.* **117** (2016) 091602 [[arXiv:1603.09298](#)] [[INSPIRE](#)].
- [27] M. Blake, *Universal diffusion in incoherent black holes*, *Phys. Rev. D* **94** (2016) 086014 [[arXiv:1604.01754](#)] [[INSPIRE](#)].
- [28] B. Swingle and D. Chowdhury, *Slow scrambling in disordered quantum systems*, *Phys. Rev. B* **95** (2017) 060201 [[arXiv:1608.03280](#)] [[INSPIRE](#)].
- [29] Y. Huang, Y.-L. Zhang and X. Chen, *Out-of-time-ordered correlator in many-body localized systems*, [arXiv:1608.01091](#) [[INSPIRE](#)].
- [30] R. Fan, P. Zhang, H. Shen and H. Zhai, *Out-of-time-order correlation for many-body localization*, [arXiv:1608.01914](#) [[INSPIRE](#)].
- [31] N. Yunger Halpern, *Jarzynski-like equality for the out-of-time-ordered correlator*, *Phys. Rev. A* **95** (2017) 012120 [[arXiv:1609.00015](#)] [[INSPIRE](#)].
- [32] D.P. DiVincenzo, D.W. Leung and B.M. Terhal, *Quantum data hiding*, *IEEE Trans. Inf. Theory* **48** (2002) 580.
- [33] J. Emerson, E. Livine and S. Lloyd, *Convergence conditions for random quantum circuits*, *Phys. Rev. A* **72** (2005) 060302.
- [34] A. Ambainis and J. Emerson, *Quantum t -designs: t -wise independence in the quantum world*, in the proceedings of the *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, June 13–16, Washington, U.S.A. (2007).
- [35] D. Gross, K. Audenaert and J. Eisert, *Evenly distributed unitaries: on the structure of unitary designs*, *J. Math. Phys.* **48** (2007) 052104 [[quant-ph/0611002](#)].
- [36] C. Dankert, R. Cleve, J. Emerson and E. Livine, *Exact and approximate unitary 2-designs and their application to fidelity estimation*, *Phys. Rev. A* **80** (2009) 012304.
- [37] J. Emerson et al., *Pseudo-random unitary operators for quantum information processing*, *Science* **302** (2003) 2098.
- [38] W.G. Brown and L. Viola, *Convergence rates for arbitrary statistical moments of random quantum circuits*, *Phys. Rev. Lett.* **104** (2010) 250501.
- [39] A.W. Harrow and R.A. Low, *Random quantum circuits are approximate 2-designs*, *Comm. Math. Phys.* **291** (2009) 257 [[arXiv:0802.1919](#)].
- [40] E. Knill et al., *Randomized benchmarking of quantum gates*, *Phys. Rev. A* **77** (2008) 012307.
- [41] F.G.S.L. Brandao, A.W. Harrow and M. Horodecki, *Local random quantum circuits are approximate polynomial-designs*, [arXiv:1208.0692](#).
- [42] R. Kueng and D. Gross, *Qubit stabilizer states are complex projective 3-designs*, [arXiv:1510.02767](#).
- [43] Z. Webb, *The Clifford group forms a unitary 3-design*, [arXiv:1510.02769](#).

- [44] R.A. Low., *Pseudo-randomness and learning in quantum computation*, [arXiv:1006.5227](#).
- [45] A.J. Scott, *Optimizing quantum process tomography with unitary 2-designs*, *J. Phys. A* **41** (2008) 055308.
- [46] H. Zhu, *Multiqubit clifford groups are unitary 3-designs*, [arXiv:1510.02619](#).
- [47] B. Collins and I. Nechita, *Random matrix techniques in quantum information theory*, *J. Math. Phys.* **57** (2016) 015215 [[arXiv:1509.04689](#)].
- [48] Y. Nakata, C. Hirche, M. Koashi and A. Winter, *Efficient unitary designs with nearly time-independent Hamiltonian dynamics*, [arXiv:1609.07021](#) [[INSPIRE](#)].
- [49] D.N. Page, *Average entropy of a subsystem*, *Phys. Rev. Lett.* **71** (1993) 1291 [[gr-qc/9305007](#)] [[INSPIRE](#)].
- [50] E. Knill, *Approximation by quantum circuits*, [quant-ph/9508006](#) [[INSPIRE](#)].
- [51] L. Susskind, *The Typical-State Paradox: Diagnosing Horizons with Complexity*, *Fortsch. Phys.* **64** (2016) 84 [[arXiv:1507.02287](#)] [[INSPIRE](#)].
- [52] A. Kitaev, *Ph/CS 219C: quantum computation*, course taught at Caltech, California, U.S.A. (2016).
- [53] Y. Gu, *Moments of random matrices and weingarten functions*, M.Sc. thesis, Queen's University, Ontario, Canada (2013).
- [54] J. Watrous, *Theory of quantum information*, lecture notes (2015)
- [55] B. Collins, *Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability*, *Int. Math. Res. Not.* **2003** (2003) 953.
- [56] F. Pastawski, B. Yoshida, D. Harlow and J. Preskill, *Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence*, *JHEP* **06** (2015) 149 [[arXiv:1503.06237](#)] [[INSPIRE](#)].
- [57] A. Roy and A.J. Scott, *Unitary designs and codes*, *Des. Codes Cryptogr.* **53** (2009) 13.
- [58] S. Sachdev and J. Ye, *Gapless spin fluid ground state in a random, quantum Heisenberg magnet*, *Phys. Rev. Lett.* **70** (1993) 3339 [[cond-mat/9212030](#)] [[INSPIRE](#)].
- [59] A. Kitaev, *A simple model of quantum holography*, talks given at KITP, April 7 and May 27 Santa Barbara, U.S.A. (2015).
- [60] J. Maldacena and D. Stanford, *Remarks on the Sachdev-Ye-Kitaev model*, *Phys. Rev. D* **94** (2016) 106002 [[arXiv:1604.07818](#)] [[INSPIRE](#)].
- [61] L. Dyson, M. Kleban and L. Susskind, *Disturbing implications of a cosmological constant*, *JHEP* **10** (2002) 011 [[hep-th/0208013](#)] [[INSPIRE](#)].
- [62] J.L.F. Barbon and E. Rabinovici, *Very long time scales and black hole thermal equilibrium*, *JHEP* **11** (2003) 047 [[hep-th/0308063](#)] [[INSPIRE](#)].
- [63] J.L.F. Barbon and E. Rabinovici, *Geometry and quantum noise*, *Fortsch. Phys.* **62** (2014) 626 [[arXiv:1404.7085](#)] [[INSPIRE](#)].
- [64] M.R. Dowling and M.A. Nielsen, *The geometry of quantum computation*, [quant-ph/0701004](#).
- [65] A.R. Brown, L. Susskind and Y. Zhao, *Quantum complexity and negative curvature*, *Phys. Rev. D* **95** (2017) 045010 [[arXiv:1608.02612](#)] [[INSPIRE](#)].
- [66] S. Chapman, H. Marrochio and R.C. Myers, *Complexity of formation in holography*, to appear.
- [67] L. Susskind and Y. Zhao, *Switchbacks and the bridge to nowhere*, [arXiv:1408.2823](#) [[INSPIRE](#)].

- [68] W. Chemissany and T.J. Osborne, *Holographic fluctuations and the principle of minimal complexity*, *JHEP* **12** (2016) 055 [[arXiv:1605.07768](#)] [[INSPIRE](#)].
- [69] A.R. Brown and L. Susskind, *The second law of quantum complexity*, [arXiv:1701.01107](#) [[INSPIRE](#)].
- [70] D. Harlow and P. Hayden, *Quantum computation vs. firewalls*, *JHEP* **06** (2013) 085 [[arXiv:1301.4504](#)] [[INSPIRE](#)].
- [71] A. Almheiri, D. Marolf, J. Polchinski and J. Sully, *Black holes: complementarity or firewalls?*, *JHEP* **02** (2013) 062 [[arXiv:1207.3123](#)] [[INSPIRE](#)].
- [72] L. Susskind, *Computational complexity and black hole horizons*, *Fortsch. Phys.* **64** (2016) 24 [[arXiv:1403.5695](#)] [[INSPIRE](#)].
- [73] L. Susskind, *Computational complexity and black hole horizons*, *Fortsch. Phys.* **64** (2016) 24 [[arXiv:1403.5695](#)] [[INSPIRE](#)].
- [74] D. Stanford and L. Susskind, *Complexity and shock wave geometries*, *Phys. Rev. D* **90** (2014) 126007 [[arXiv:1406.2678](#)] [[INSPIRE](#)].
- [75] A.R. Brown, D.A. Roberts, L. Susskind, B. Swingle and Y. Zhao, *Holographic complexity equals bulk action?*, *Phys. Rev. Lett.* **116** (2016) 191301 [[arXiv:1509.07876](#)] [[INSPIRE](#)].
- [76] A.R. Brown, D.A. Roberts, L. Susskind, B. Swingle and Y. Zhao, *Complexity, action and black holes*, *Phys. Rev. D* **93** (2016) 086006 [[arXiv:1512.04993](#)] [[INSPIRE](#)].
- [77] T. Hartman and J. Maldacena, *Time Evolution of Entanglement Entropy from Black Hole Interiors*, *JHEP* **05** (2013) 014 [[arXiv:1303.1080](#)] [[INSPIRE](#)].
- [78] B. Swingle, *Entanglement Renormalization and Holography*, *Phys. Rev. D* **86** (2012) 065007 [[arXiv:0905.1317](#)] [[INSPIRE](#)].
- [79] B. Swingle, *Constructing holographic spacetimes using entanglement renormalization*, [arXiv:1209.3304](#) [[INSPIRE](#)].
- [80] J. Maldacena, *Spacetime from entanglement*, talk give at *KITP*, August 20, Santa Barbara, U.S.A. (2013).
- [81] A. Almheiri, X. Dong, and D. Harlow, *Bulk locality and quantum error correction in AdS/CFT*, *JHEP* **04** (2015) 163 [[arXiv:1411.7041](#)].
- [82] M.A. Nielsen and I.L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, U.K. (2000).
- [83] M. Mozrymas et al., *Local random quantum circuits are approximate polynomial-designs: numerical results*, *J. Phys. A* **46** (2013) 305301 [[arXiv:1212.2556](#)].
- [84] A. Brown, *Wormholes and complexity*, talk given at the *Perimeter Institute for Theoretical Physics*, August 21, Waterloo, Canada (2015).