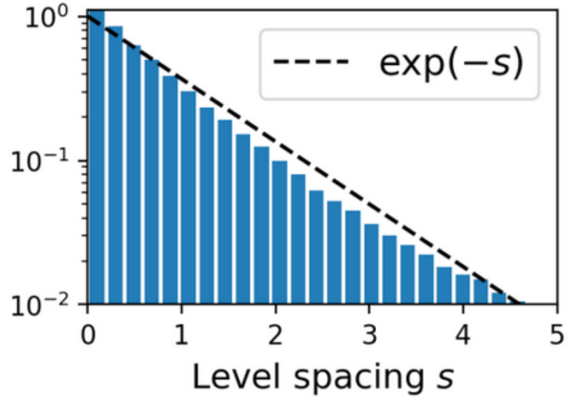
Random unitary evolution, *t*-designs, and applications to quantum chaos

UNM CQuIC Summer 2021 Course, “Many-body Quantum Chaos”

Andrew Zhao

Random matrix ensembles to model quantum chaos

Spectral distributions



- Circular orthogonal ensemble (COE) has time-reversal symmetry. It has eigenvalue distribution:

$$P(\phi_1, \phi_2, \cdots, \phi_n) = \prod_{j<k} |e^{-i\phi_j} - e^{-i\phi_k}|$$

- Circular unitary ensemble (CUE), on the other hand, is similar to GUE:

$$P(\phi_1, \phi_2, \cdots, \phi_n) = \prod_{j<k} |e^{-i\phi_j} - e^{-i\phi_k}|^2$$

Fidelity decay

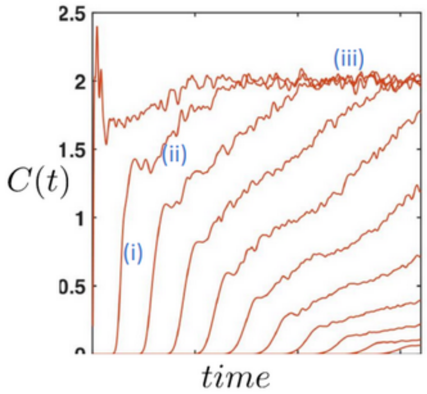
Assume V is a Gaussian random matrix

$$\langle \exp(-i\, V_{ii} \epsilon t) \rangle_V = \exp(-\frac{\epsilon^2 t^2}{2})$$

$$\Downarrow$$

$$\boxed{F(t) \simeq \eta_{\mathrm{IPR}} + e^{-\epsilon^2 t^2} (1 - \eta_{\mathrm{IPR}})}$$

OTOC scrambling



Overview

Is there a more practical way to understand this randomness?

What are sufficient conditions for reproducing this randomness?

Can we gain a deeper understanding of quantum chaos?

The Haar measure

For any compact group G there exists a unique (up to normalization), translationally invariant measure called the Haar measure:

"bounded"

$$\mu(S) = \text{volume of } S \subseteq G$$

$$\mu(gS) = \mu(Sg) = \mu(S)\ \forall g \in G$$

Def. A *group* is a set G with associative binary operation $G \times G \to G$ such that:

$$!\exists e \in G : ge = eg = g\ \forall g \in G\ \text{(identity element)}$$

$$\forall g \in G, !\exists g^{-1} \in G : gg^{-1} = g^{-1}g = e\ \text{(inverse element)}$$

Provides a notion of integration over groups: $\int_G d\mu(g)\, f(g),\ \text{where}\ f : G \to \mathbb{C}$

Probability distributions over groups

Normalizing $\mu(G) = 1$ allows us to interpret μ as a probability measure:

$$\mathbb{E}[f] = \int_G d\mu(g)\, f(g)$$

Uniform distribution over G = Haar distribution over G

How to sample from μ? Simplest example is when G is finite:

$$\mathbb{E}[f] = \frac{1}{|G|} \sum_{g \in G} f(g) \leftarrow \text{choose all } g \text{ with probability } \frac{1}{|G|}$$

Sampling from continuous groups

Focus on unitary group over n qubits: $\mathrm{U}(2^n)$ (generalization to $\mathrm{U}(d)$ straightforward)

We *can in principle* sample from this matrix group, but:

What do the corresponding quantum circuits look like?

- Exponentially long circuits [quant-ph/9508006]

Can we do away with the complicated continuous measures/integrals?

$$\int_G dg\, f(g) = \frac{1}{W(G)} \int_T |\Delta(t)|^2 \int_{G/T} f(gtg^{-1})\, d(gT)\, dt$$

(Weyl integration formula)

Spherical t-designs

J.J. Benedetto, M. Fickus / Finite normalized tight frames

Adv. Comput. Math. 18 357 (2003)

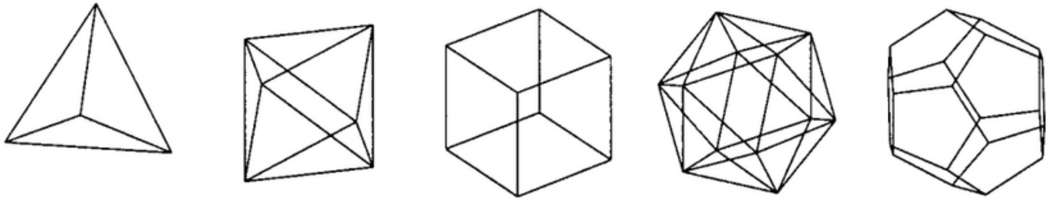


Figure 2. The five Platonic solids.

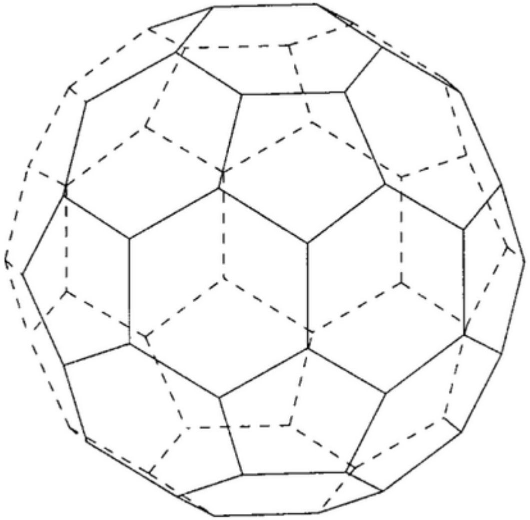


Figure 3. The “soccer ball”, a truncated icosahedron.

Unitary t-designs

Def. Let $D = \{U_k \in \mathrm{U}(2^n) \mid k = 1, \ldots, K\}$. We say D is a *unitary t-design* for some $t \in \mathbb{N}$ if

$$\frac{1}{K} \sum_{k=1}^{K} P(U_k) = \int_{\mathrm{U}(2^n)} dU \, P(U)$$

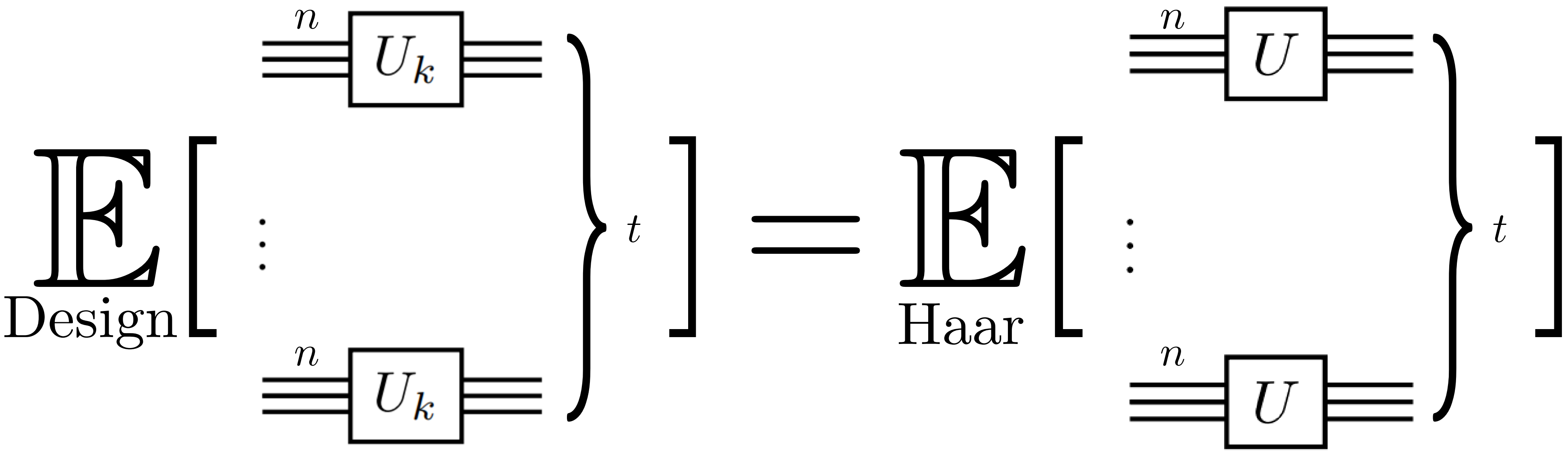
for all complex polynomials P of degree (t, t), where the polynomial is understood as a function of matrix elements, $P(U) = P(U_{11}, U_{11}^*, U_{12}, U_{12}^*, \ldots, U_{2^n,2^n}, U_{2^n,2^n}^*)$.

Sampling from a unitary t-design reproduces the first t moments of the unitary group

Primary reference: [quant-ph/0611002]

Unitary t-designs

Sampling from a unitary t-design reproduces the first t moments of the unitary group



Twirling channel: $\displaystyle \frac{1}{K}\sum_{k=1}^{K} U_k^{\otimes t} A (U_k^{\dagger})^{\otimes t} = \int_{\mathrm{U}(2^n)} dU\, U^{\otimes t} A (U^{\dagger})^{\otimes t}$

Unitary t-designs

Sampling from a unitary t-design reproduces the first t moments of the unitary group

Twirling channel: $$\frac{1}{K}\sum_{k=1}^{K} U_k^{\otimes t} A (U_k^\dagger)^{\otimes t} = \int_{\mathrm{U}(2^n)} dU\, U^{\otimes t} A (U^\dagger)^{\otimes t}$$

$$A = O^{\otimes t}$$

$$\frac{1}{K}\sum_{k=1}^{K} \langle U_k O U_k^\dagger \rangle^t = \int_{\mathrm{U}(2^n)} dU\, \langle U O U^\dagger \rangle^t$$

Representation theory primer

Def. A *representation* of a group G on a vector space V is map

$$\Phi : G \to \mathrm{GL}(V) = \{\text{invertible matrices on } V\}$$

such that $\Phi(g)\Phi(h) = \Phi(gh) \; \forall g, h \in G$ (i.e., it is a *group homomorphism*).

Def. A representation Φ is *reducible* if there is a nontrivial subspace $W \subset V$ such that

$$\Phi|_W : G \to \mathrm{GL}(W)$$

is itself a representation. Otherwise, Φ is said to be an *irreducible representation* (*irrep*).

Representation theory primer

Thm (Peter-Weyl). Every unitary representation $\Phi : G \to \mathrm{U}(V)$ admits the decomposition

$$\Phi = \bigoplus_{\lambda} \phi_{\lambda}^{\oplus m_{\lambda}}$$

where $\phi_\lambda : G \to \mathrm{U}(V_\lambda)$ are irreps, $\bigoplus_\lambda V_\lambda = V$, and m_λ is the multiplicity of each V_λ.

What this means: every unitary representation is completely characterized by its irreps

Why do we care: twirling is intimately connected with irreps

Representation theory primer

Lemma (Schur). Let $\phi_\lambda : G \to \mathrm{GL}(V_\lambda)$ be an irrep. The only linear maps on V_λ which commute with ϕ_λ, i.e.,

$$f \phi_\lambda(g) = \phi_\lambda(g) f \;\; \forall g \in G$$

are multiples of the identity, $f = \alpha_\lambda \mathbf{1}_{V_\lambda}$.

Twirling over an irrep yields a multiple of the identity:

$$\begin{aligned} \mathcal{T}_{\phi_\lambda}(A)\phi_\lambda(h) &= \int_G dg\, \phi_\lambda(g) A \phi_\lambda(g)^\dagger \phi_\lambda(h) \\ &= \int_G d(h^{-1}g)\, \phi_\lambda(g) A \phi_\lambda(h^{-1}g)^\dagger \\ &= \int_G d(g')\, \phi_\lambda(hg') A \phi_\lambda(g')^\dagger \qquad (g' = h^{-1}g) \end{aligned}$$

$$\begin{aligned} &= \phi_\lambda(h) \int_G d(g')\, \phi_\lambda(g') A \phi_\lambda(g')^\dagger \\ &= \phi_\lambda(h) \mathcal{T}_{\phi_\lambda}(A) \end{aligned}$$

A representation-theoretic perspective

For a reducible representation (no multiplicities):

projector onto V_λ

$$\mathcal{T}_\Phi(A) = \left[\bigoplus_\lambda \mathcal{T}_{\phi_\lambda}\right](A) = \sum_\lambda \alpha_\lambda(A)\Pi_\lambda$$

Back to *t*-designs: the *t*-fold twirl over:

The unitary group

$$\Psi : \mathrm{U}(2^n) \to \mathrm{U}(2^n)^{\otimes t},\ U \mapsto U^{\otimes t}$$

$$\mathcal{T}_\Psi(A) = \int_{\mathrm{U}(2^n)} dU\, U^{\otimes t} A (U^\dagger)^{\otimes t}$$

The subgroup $D = \{U_k \mid k = 1, \ldots, K\}$

$$\Phi : D \to D^{\otimes t}$$

$$\mathcal{T}_\Phi(A) = \frac{1}{K}\sum_{k=1}^{K} U_k^{\otimes t} A (U_k^\dagger)^{\otimes t}$$

$\boxed{\textbf{Goal: } \text{match the irreps of } \Phi \text{ with } \Psi}$

The frame potential

With some work we can determine the irreps of Ψ (Schur-Weyl duality)

OTOH, checking the irreps of Φ for arbitrary D may be arduous

An equivalent formulation can be found via the theory of *frames*:

Def. The $t\text{th}$ *frame potential* of $D = \{U_k \in \mathrm{U}(2^n) \mid k = 1, \ldots, K\}$ is

$$F_t(D) = \frac{1}{K^2} \sum_{k,k'=1}^{K} |\mathrm{tr}(U_k U_{k'}^\dagger)|^{2t}$$

If D is a group then

$$F_t(D) = \frac{1}{K} \sum_{k=1}^{K} |\mathrm{tr}(U_k)|^{2t}$$

Representation theory primer pt. 2

Def. Let Φ be a representation for a finite group G. The *character* of Φ is the trace map,

$$\begin{aligned}\zeta_\Phi : G &\to \mathbb{C}, \\ g &\mapsto \zeta(g) = \mathrm{tr}[\Phi(g)]\end{aligned}$$

Characters live in $L^2(G)$, which has the natural inner product

$$\langle \zeta, \eta \rangle = \int_G dg\, \zeta(g)^* \eta(g) = \frac{1}{|G|} \sum_{g \in G} \zeta(g)^* \eta(g)$$

The characters of irreps are orthonormal (Schur orthogonality),

$$\langle \chi_{\phi_\lambda}, \chi_{\phi_{\lambda'}} \rangle = \delta_{\lambda\lambda'}$$

hence form a basis for $L^2(G)$: $\eta = \sum_\lambda c_\lambda \chi_{\phi_\lambda}$

Back to the frame potential

Where did it come from?

$$\begin{aligned} F_t(D) &= \frac{1}{K}\sum_{k=1}^{K}\left|\operatorname{tr}(U_k)\right|^{2t} \\ &= \frac{1}{K}\sum_{k=1}^{K}\left[\operatorname{tr}(U_k)^*\operatorname{tr}(U_k)\right]^t \\ &= \frac{1}{K}\sum_{k=1}^{K}\left[\operatorname{tr}(U_k^{\otimes t})^*\operatorname{tr}(U_k^{\otimes t})\right] \\ &= \langle \zeta_\Phi, \zeta_\Phi\rangle \equiv \|\zeta_\Phi\|^2 \end{aligned}$$

How does it relate to designs?

1. $\zeta_{\rho\oplus\sigma} = \zeta_\rho + \zeta_\sigma \implies \zeta_\Phi = \sum_\lambda m_\lambda \chi_{\phi_\lambda}$
2. $\|\zeta_\Phi\|^2 = \sum_\lambda m_\lambda^2$
3. D is a *t*-design iff $\|\zeta_\Phi\|^2 = \|\zeta_\Psi\|^2$

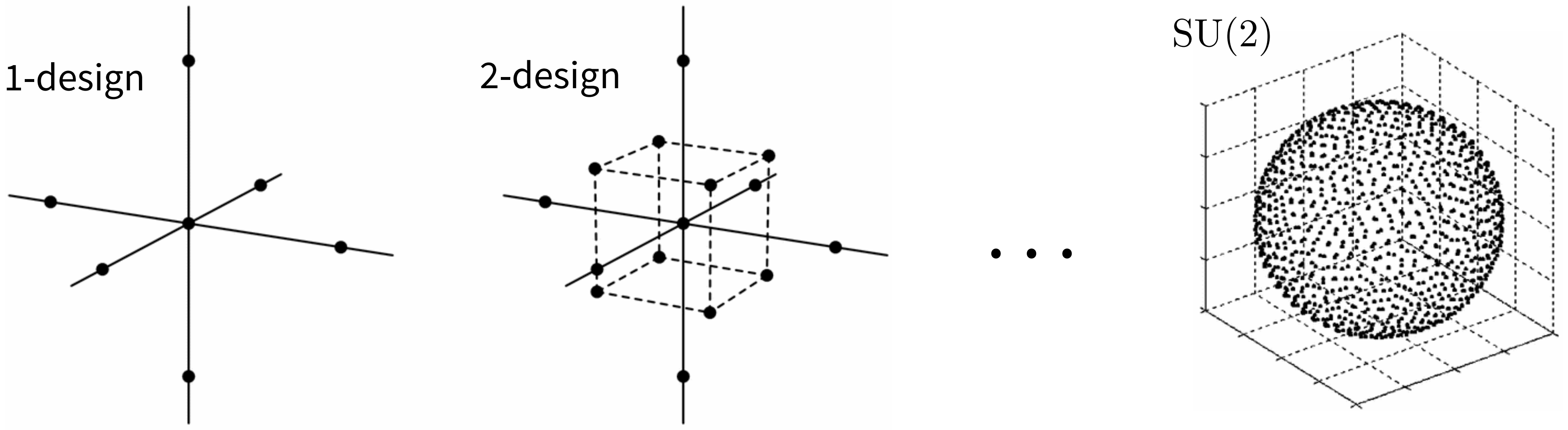
$$\text{Note: } \|\zeta_\Psi\|^2 = \begin{cases} \frac{(2t)!}{t!(t+1)!} & n = 1 \\ t! & 2^n \geq t \end{cases}$$

(Calculated using Schur-Weyl duality for $\mathrm{U}(2^n)$)

Interpreting the frame potential

Representation theory gives a clean **algebraic** interpretation

Frames, however, are very **geometrical** in nature



The frame potential measures how “evenly distributed” the frame is: think of $|\mathrm{tr}(U_k U_{k'}^\dagger)|^{2t}$ as a repulsive force, and we want to minimize the average potential $F_t(D)$

The Clifford group

A prominent example of a unitary design

Let $\mathcal{P}(n) = \{I, X, Y, Z\}^{\otimes n} \times \langle i \rangle$ denote the *n*-qubit *Pauli group*. The *n*-qubit *Clifford group* is the set of all unitary transformations which **permute Paulis** among themselves:

$$\mathcal{C}(n) = \{U \in \mathrm{U}(2^n) \mid \forall P \in \mathcal{P}(n) : UPU^\dagger \in \mathcal{P}(n)\}$$

Clifford transformations are:

- classically simulable [quant-ph/9807006]
- generated by {H, S, CNOT} [quant-ph/9807006]
- implemented with $\mathcal{O}(n^2/\log n)$ elementary gates [quant-ph/0406196]
- randomly sampled with classical time complexity $\mathcal{O}(n^2)$ [2003.09412, 2008.06011]

The Clifford group is a 3-design

Recognized early that the Clifford group is a 2-design

- [quant-ph/0103098, quant-ph/0405016, quant-ph/0512217]

In fact, it is a 3-design

- [1510.02619, 1510.02769]
- It is a *minimal* 3-design: except for $n = 2$, $\nexists H < \mathcal{C}(n) : H \text{ is a 3-design}$
- Analysis fully generalized to qudits (only a 2-design!)

$$F_t(\mathcal{C}(n)) = \begin{cases} 2 & t = 2 \\ 5 & t = 3, n = 1 \\ 6 & t = 3, n \geq 2 \\ 15 & t = 4, n = 1 \\ 29 & t = 4, n = 2 \\ 30 & t = 4, n \geq 3 \end{cases}$$

c.f. $$\|\zeta_\Psi\|^2 = \begin{cases} 2 & t = 2 \\ \frac{(2\times 3)!}{3!(3+1)!} = 5 & t = 3, n = 1 \\ 3! = 6 & t = 3, n \geq 2 \\ \frac{(2\times 4)!}{4!(4+1)!} = 14 & t = 4, n = 1 \\ 4! = 24 & t = 4, n \geq 2 \end{cases}$$

Some generalizations to briefly mention

Approximate designs: $\|\mathcal{T}_\Phi - \mathcal{T}_{\mathrm{Haar}}\|_\diamond \leq \epsilon$

- Take random circuits of length $\mathrm{poly}(t, \log \epsilon^{-1})$ [1208.0692]

Designs over nonuniform distributions

$$\sum_{k=1}^{K} p_k U_k^{\otimes t}(\,\cdot\,)(U_k^\dagger)^{\otimes t}$$

Designs for arbitrary compact groups

- Match the irreducible components of $g \mapsto g^{\otimes t}$

Connecting circuit complexity with quantum chaos

Designs are useful for practicality – can we learn something **fundamental** from them?

Roberts & Yoshida, Chaos and complexity by design [1610.04903]

Designs are directly motivated by notions of **circuit complexity**

Designs are also defined through **random unitaries**

Chaos is understood through **models of random unitary evolution**

Quantum circuit complexity ↔ Quantum chaos?

↑

Unitary designs

Some motivation

Consider the Heisenberg evolution of some local observable W:

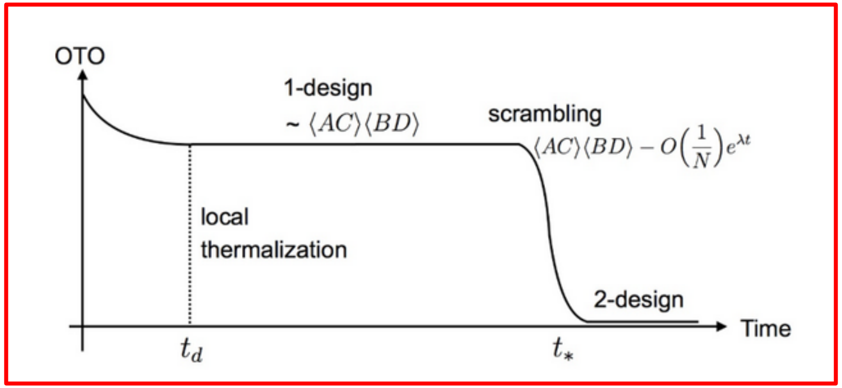
$$W(t) = e^{iHt} W e^{-iHt}$$

A common measure for quantum chaos is the OTOC:

$$\langle W(t)^\dagger V^\dagger W(t) V \rangle, \quad V \text{ some other local operator}$$

If sufficiently chaotic, the OTOC decays to $\sim\langle \tilde{W}^\dagger V^\dagger \tilde{W} V \rangle, \text{ where } \tilde{W} = U^\dagger W U$,

U a random unitary



Does *U* really have to be sampled from the Haar measure? Can we already diagnose quantum chaos with a simpler ensemble?

Chaos and designs

Consider the 2*k*-point correlator

$$\langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle = \frac{1}{2^n} \operatorname{tr}(A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k)$$

where the average is evaluated on the maximally mixed state, $A_j, B_j \in \mathcal{P}(n)/\langle i \rangle$, and $\tilde{B} = U^\dagger B U$ for *U* drawn from some ensemble $\mathcal{E}$ of unitaries

Roberts & Yoshida show that:

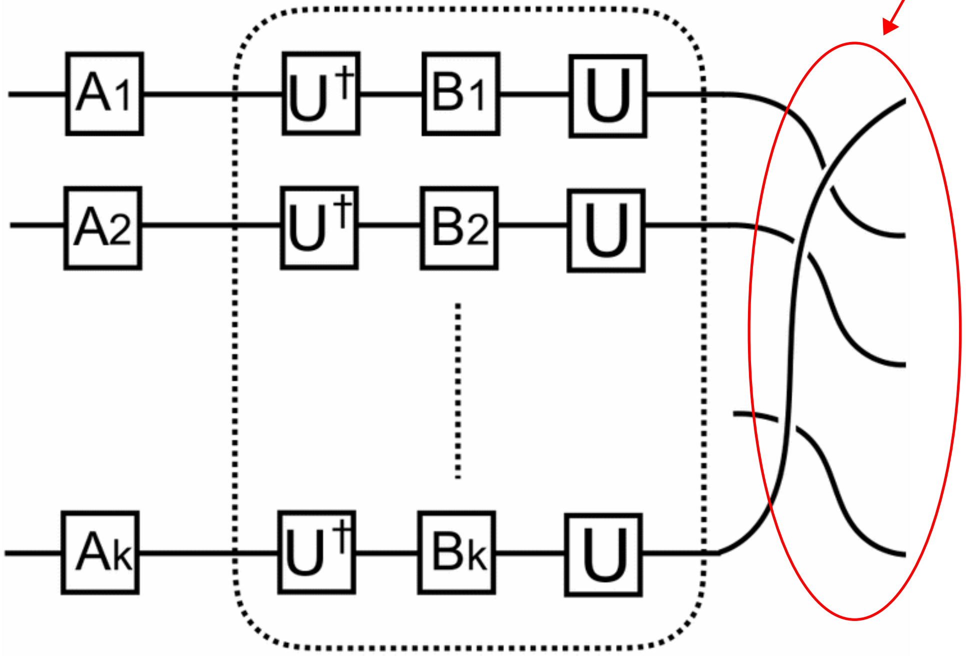
$$1. \quad \int_{\mathcal{E}} dU \, \langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle \overset{\text{one-to-one}}{\leftrightarrow} \int_{\mathcal{E}} dU \, U^{\otimes k} (\,\cdot\,)(U^\dagger)^{\otimes k} \equiv \mathcal{T}_{\mathcal{E}}^{(k)}(\,\cdot\,)$$

$$2. \quad \mathbb{E}_{A_j, B_j} \left| \int_{\mathcal{E}} dU \, \langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle \right|^2 \propto \int_{\mathcal{E} \times \mathcal{E}} dU \, dV |\operatorname{tr}(U^\dagger V)|^{2k} \equiv F_k(\mathcal{E})$$

1. OTOCs specify twirls

$$\langle A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k \rangle = \frac{1}{2^n} \mathrm{tr}(A_1 \tilde{B}_1 \cdots A_k \tilde{B}_k)$$

$$= \frac{1}{2^n} \mathrm{tr}\Big[(A_1 \otimes \cdots \otimes A_k)(\tilde{B}_1 \otimes \cdots \otimes \tilde{B}_k) W_\pi\Big]$$



$\mathcal{T}_\mathcal{E}^{(k)}(B_1 \otimes \cdots \otimes B_k)$

$B_1 \otimes \cdots \otimes B_k$ and $A_1 \otimes \cdots \otimes A_k$:

(Pauli) basis for $\mathcal{L}(\mathcal{H}^{\otimes k})$

$2k$-OTOC defines the matrix elements:

$\langle\langle A_{\pi(1)} \otimes \cdots \otimes A_{\pi(k)} | \mathcal{T}_\mathcal{E}^{(k)} | B_1 \otimes \cdots \otimes B_k \rangle\rangle$

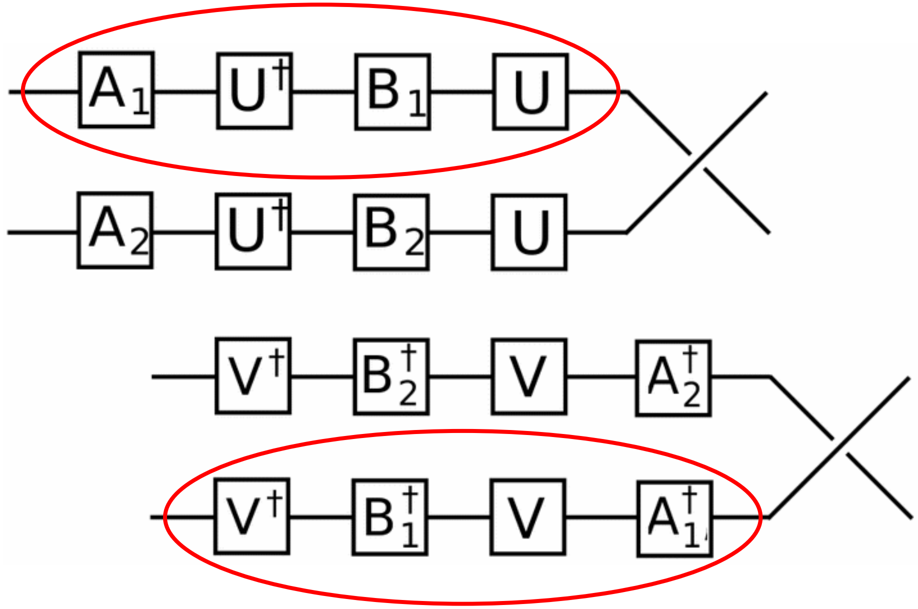
Some linear algebra shows this is unique

2. OTOCs are frame potentials

$$\mathbb{E}_{A_j,B_j}\left|\int_{\mathcal{E}} dU\,\langle A_1\tilde{B}_1\cdots A_k\tilde{B}_k\rangle\right|^2 \stackrel{!}{=} \frac{1}{(4^n)^{k+1}}F_k(\mathcal{E})$$

$$\propto \sum_{U,V\in\mathcal{E}}\sum_{A_j,B_j} \mathrm{tr}(A_1U^\dagger B_1U\cdots A_kU^\dagger B_kU)\,\mathrm{tr}(V^\dagger B_k^\dagger VA_k^\dagger\cdots V^\dagger B_1^\dagger VA_1^\dagger)$$

$k=2:$



Use SWAP $=\dfrac{1}{2^n}\sum_P P\otimes P^\dagger$

to connect wires

$\mathrm{tr}(VU^\dagger)\,\mathrm{tr}(V^\dagger U)=|\mathrm{tr}(VU^\dagger)|^2$

Implications

The notions of quantum chaos and pseudorandomness are **equivalent** to those of unitary designs

Decay of OTOCs is directly connected to how uniformly random the ensemble is

"evenly distributed"

Recall: $F_k(\mathcal{E}) \geq F_k(\mathrm{Haar})$

Hence: smaller average OTOC → closer to a *k*-design → system more random/chaotic

Designs and complexity

Designs are clearly related to quantum circuit complexity

Loose lower bound:

$$\text{Complexity of } \mathcal{E} \geq \frac{2kn \log 2 - \log F_k(\mathcal{E})}{\log(\#\text{choices})}$$

# of elementary gates to prepare any circuit in $\mathcal{E}$

# of gates we can choose from, per step in the circuit

Designs and complexity

Counting argument: allotted complexity C, $\#\text{circuits} \leq (\#\text{choices})^C$

To generate all elements of $\mathcal{E}$, we need at least $(\#\text{choices})^C \geq |\mathcal{E}|$

$$\implies C \geq \frac{\log|\mathcal{E}|}{\log(\#\text{choices})}$$

Finally, the frame potential bounds $|\mathcal{E}|$: $F_k(\mathcal{E}) \geq \frac{1}{|\mathcal{E}|^2}\sum_{U=V}|\mathrm{tr}(UV^\dagger)|^{2k} = \frac{1}{|\mathcal{E}|}(2^n)^{2k}$

$$\implies C(\mathcal{E}) \geq \frac{2kn\log 2 - \log F_k(\mathcal{E})}{\log(\#\text{choices})}$$

Chaos and complexity via designs

The closer $\mathcal{E}$ is to a *k*-design, the smaller $F_k(\mathcal{E})$ is:

$$C(\mathcal{E}) \geq \frac{2kn\log 2 - \log F_k(\mathcal{E})}{\log(\#\text{choices})}$$

$\implies$ **Minimal complexity of an ensemble increases with its chaoticity**

Recall: *k*-design has $F_k(\mathcal{E}) = k!$

$$\implies C(\mathcal{E}) \geq \tilde{\Omega}(kn)$$

Also naturally relates to entropy:

$$S \geq 2kn - \log_2 F_k(\mathcal{E})$$

(von Neumann entropy of the probability distribution associated with $\mathcal{E}$)

Some other results

If $\mathcal{E}$ is continuous, then we can only generate elements with ϵ-close circuits:

$$C_\epsilon \geq \frac{2kn\log 2 - k\epsilon^2 - \log F_k(\mathcal{E})}{\log(\#\text{choices})}$$

If generated by an ensemble of Hamiltonians, then $C_\epsilon \sim t^2$ for $t \lesssim 1/\sqrt{n}$

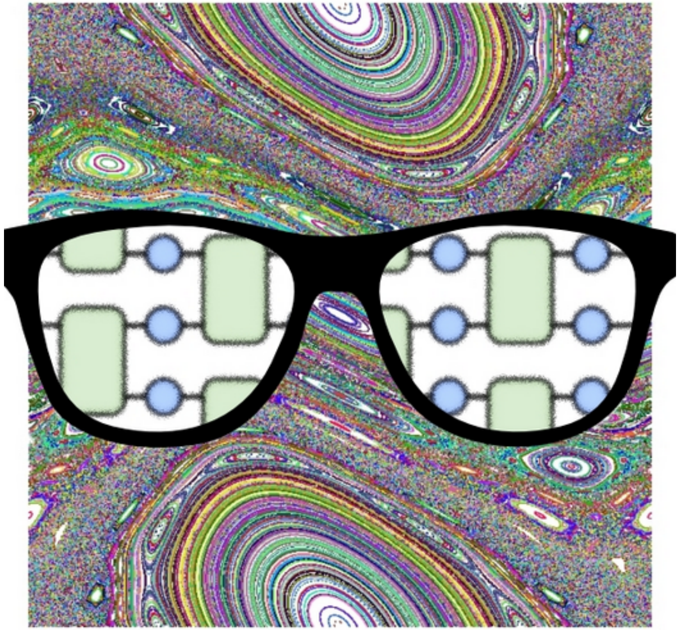
Explicit calculation with 8-point OTOC:

$$\mathbb{E}_{\text{Haar}}\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger\rangle \sim \frac{1}{(2^n)^4}; \quad \mathbb{E}_{\text{Clifford}}\langle A\tilde{B}C\tilde{D}A^\dagger\tilde{D}^\dagger C^\dagger\tilde{B}^\dagger\rangle \sim \frac{1}{(2^n)^2}$$

Closing remarks

1. Continuous groups can be approximated by finite groups, up to an order *t*
   - This approximation is sufficient for most purposes

2. Finite groups are easier to study theoretically and implement practically
   - **Clifford group!!!**



3. Representation theory offers an elegant mathematical framework

4. Chaos ↔ Designs ↔ Complexity