

Title: Random unitaries in extremely low depth

Speakers: Thomas Schuster

Collection/Series: Quantum Information

Subject: Quantum Information

Date: November 06, 2024 - 11:00 AM

URL: <https://pirsa.org/24110051>

Abstract:

Random unitaries form the backbone of numerous components of quantum technologies, and serve as indispensable toy models for complex processes in quantum many-body physics. In all of these applications, a crucial consideration is in what circuit depth a random unitary can be generated. I will present recent work, in which we show that local quantum circuits can form random unitaries in exponentially lower circuit depths than previously thought. We prove that random quantum circuits on any geometry, including a 1D line, can form approximate unitary designs over n qubits in $\log n$ depth. In a similar manner, we construct pseudorandom unitaries (PRUs) in 1D circuits in $\text{poly log } n$ depth, and in all-to-all-connected circuits in $\text{poly log log } n$ depth. These shallow quantum circuits have low complexity and create only short-range entanglement, yet are indistinguishable from unitaries with exponential complexity. Applications of our results include proving that classical shadows with 1D log-depth Clifford circuits are as powerful as those with deep circuits, demonstrating superpolynomial quantum advantage in learning low-complexity physical systems, and establishing quantum hardness for recognizing phases of matter with topological order.

Random unitaries in extremely low depth

Thomas Schuster

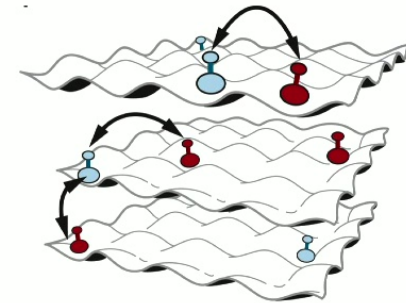
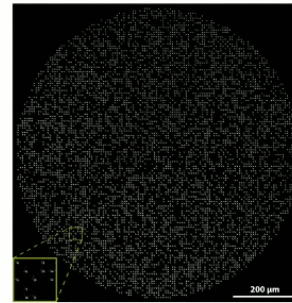
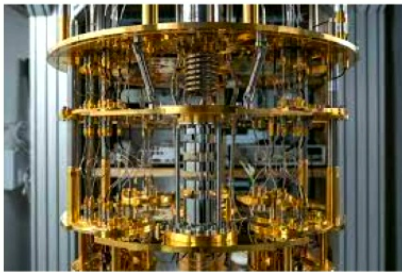
TS, Haferkamp, Huang arxiv: 2407:07754 (2024)

Caltech



Large-scale quantum science

Modern experiments reach beyond the traditional regimes of quantum physics, information, and computation



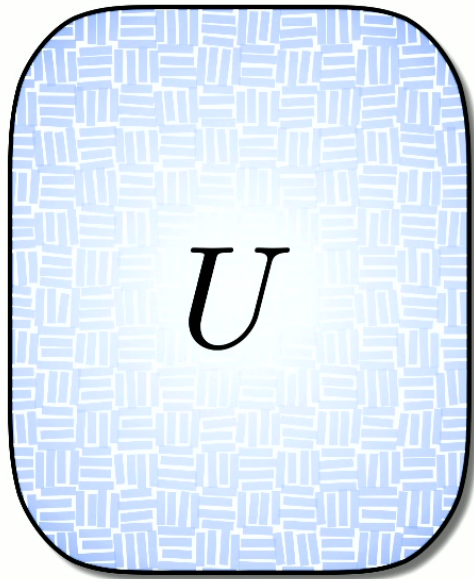
How do we benchmark large quantum devices?

How do large quantum circuits and Hamiltonians behave?

How can we find quantum advantages, esp in near-term experiments?

What properties are easy to measure in qu expts, and what are hard?

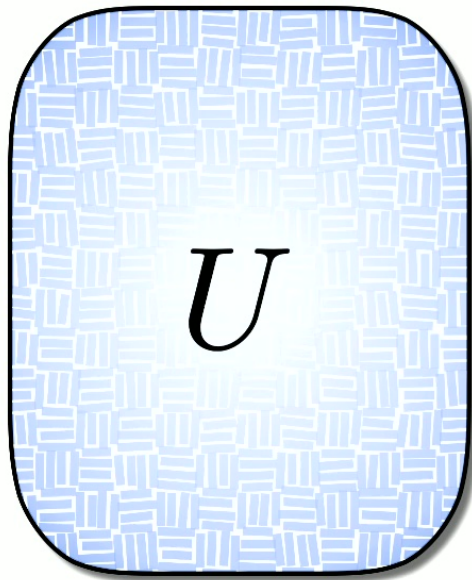
A surprisingly helpful tool



Haar-random unitary

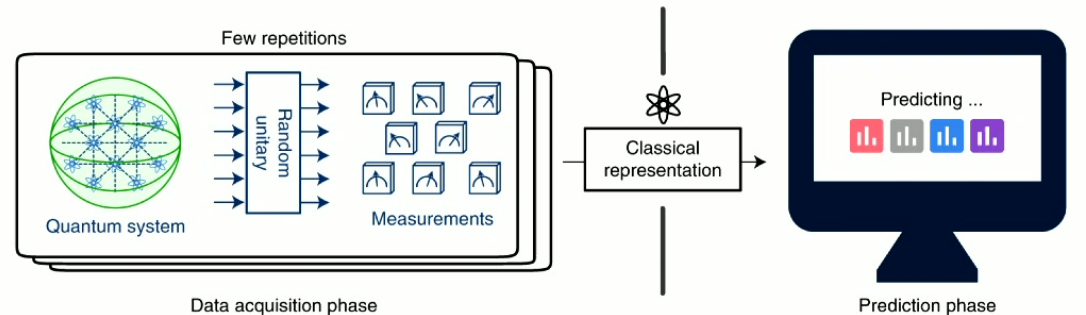
A Haar-random unitary on n qubits is a random $2^n \times 2^n$ unitary matrix

A surprisingly helpful tool



Haar-random unitary

As an application:

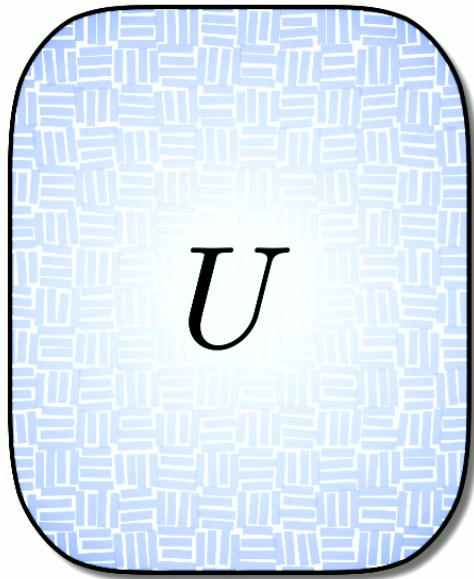


Huang, Kueng, Preskill (2020)

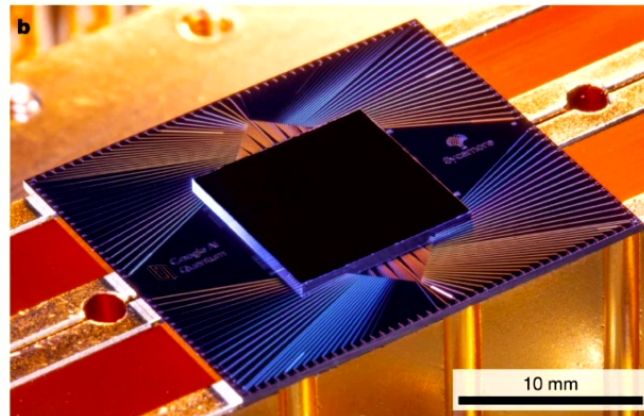
Fidelity estimation and
classical shadow tomography

A surprisingly helpful tool

As an application:



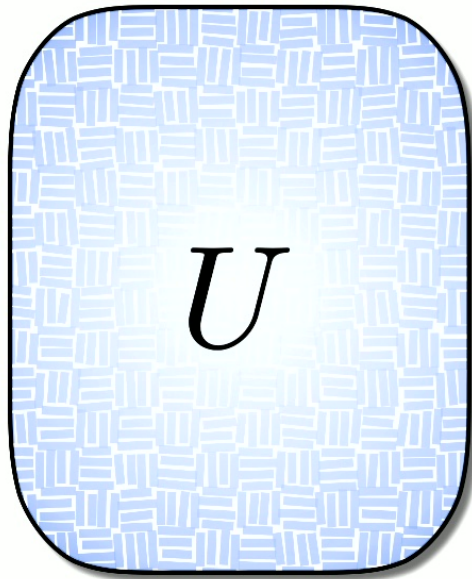
Haar-random unitary



Google Quantum AI (2019)

Quantum supremacy experiments

A surprisingly helpful tool



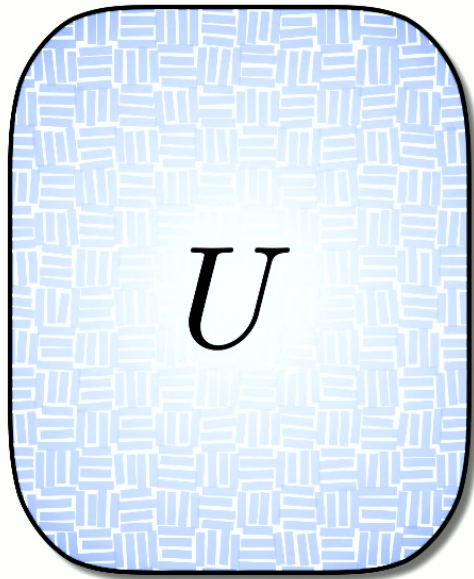
Haar-random unitary

As an application:



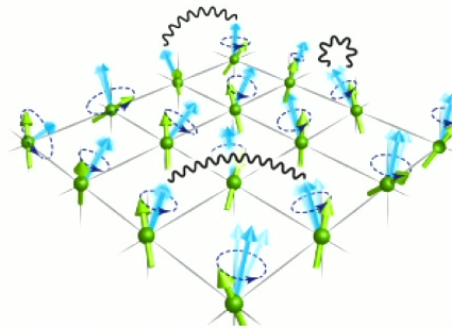
Quantum cryptography?

A surprisingly helpful tool

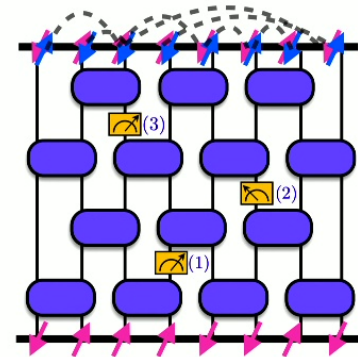


Haar-random unitary

As a toy model:



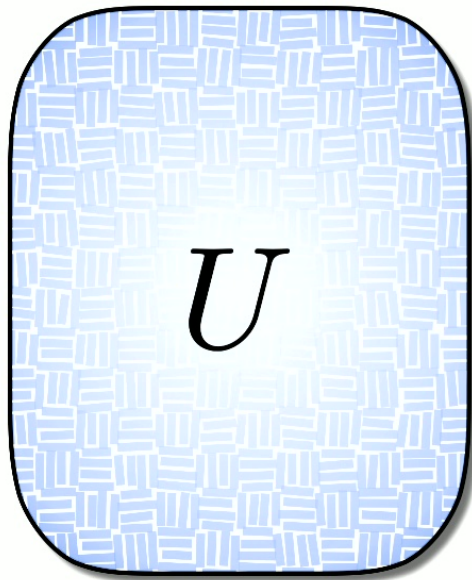
Michael Knap



Fisher, Khemani, Nahum, Vijay

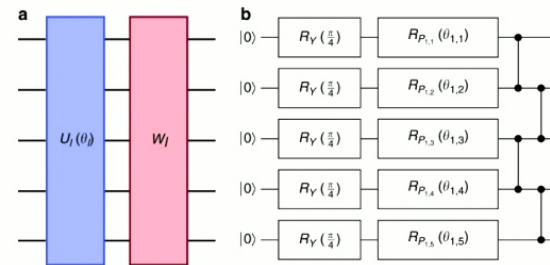
Quantum many-body dynamics

A surprisingly helpful tool

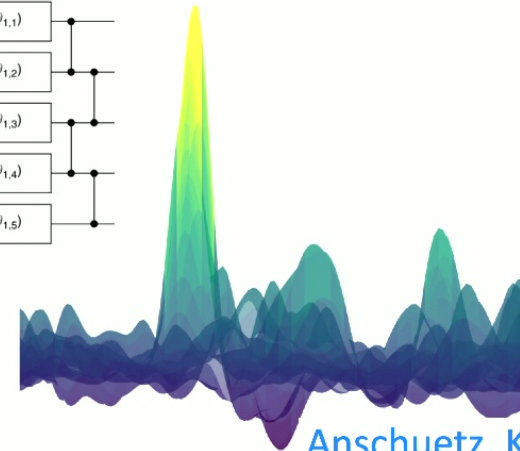


Haar-random unitary

As a toy model:



McClean et al (2018)

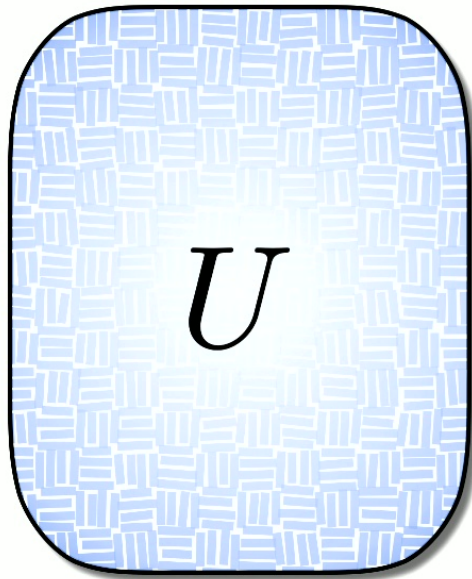


Anschuetz, Kiani (2022)

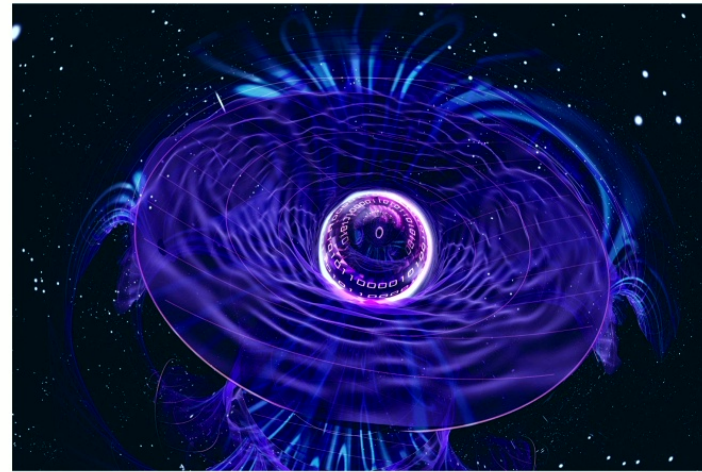
Quantum machine learning

A surprisingly helpful tool

As a toy model:

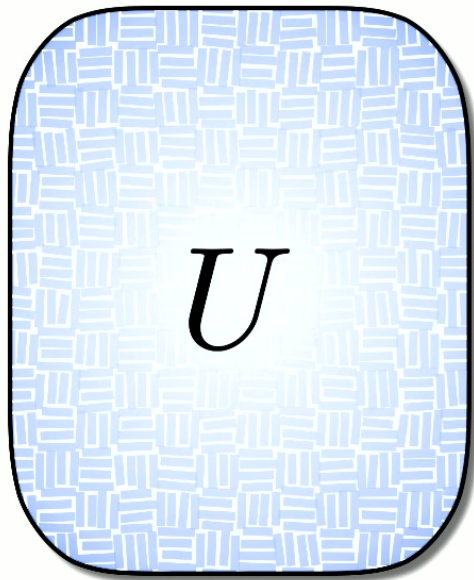


Haar-random unitary



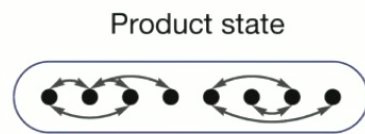
Quantum gravity & the AdS/CFT
correspondence

A surprisingly helpful tool

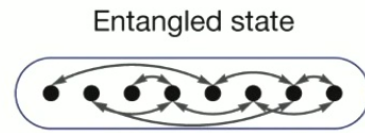


Haar-random unitary

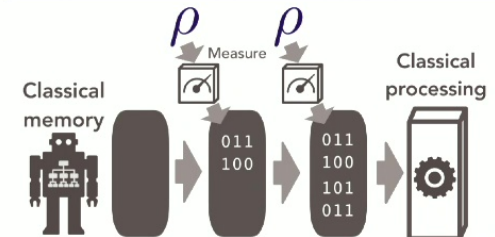
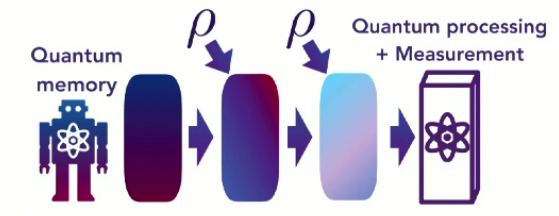
As a counter-example:



vs.



Islam,...,Greiner (2015)

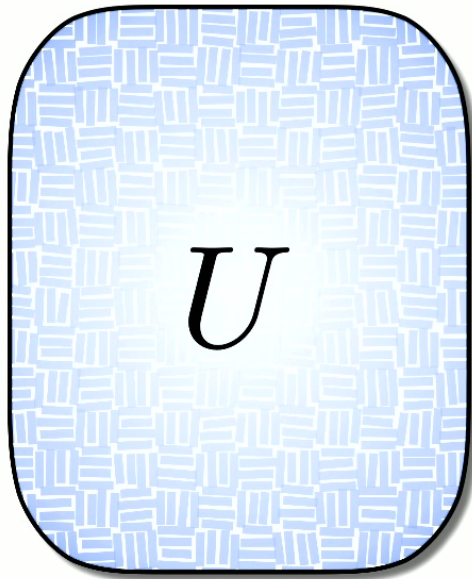


Huang,...,McClean (2022)

Challenges and advantages in quantum learning

A central question

In what *depth* can a local quantum circuit look like a Haar-random unitary?

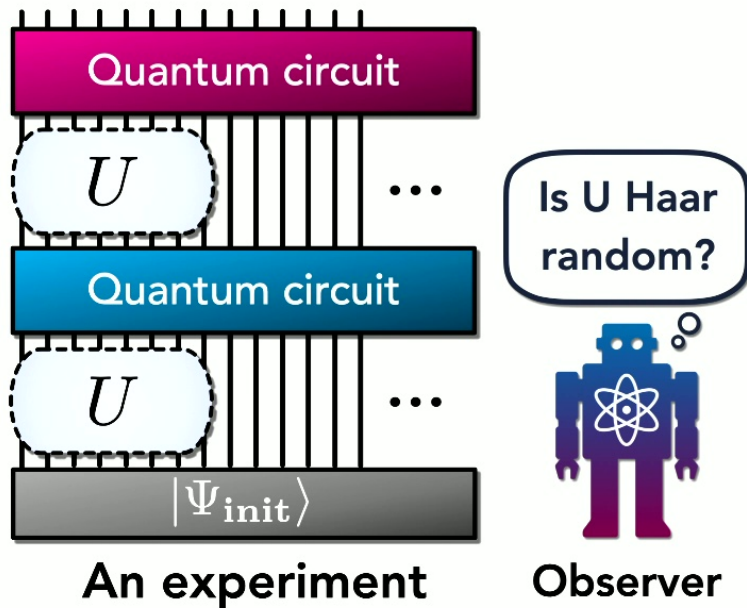



A true Haar-random unitary has
exponential depth

So any useful answer requires a notion
of approximation

A central question

In what *depth* can a local quantum circuit look like a Haar-random unitary?



-  **Unitary k-design:**
any k-query experiments
-  **Pseudorandom unitaries:**
any efficient experiments

What is known so far

In what *depth* can a local quantum circuit look like a Haar-random unitary?

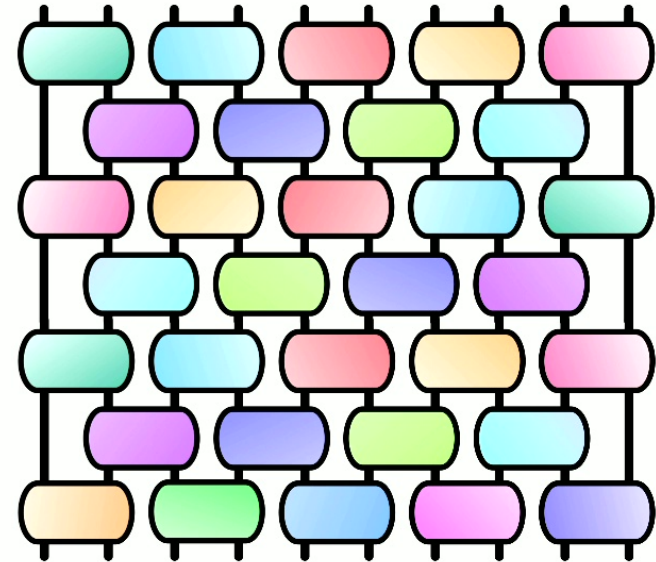
- Local random circuits form **unitary k -designs** in depth $k * n$, on any circuit geometry

[Brandao, Harrow, Horedecki \(2012\)](#)

[Haferkamp \(2022\)](#)

[Chen, Haah, Haferkamp, Liu, Metger, Tan \(2024\)](#)

see also: [Haah, Liu, Tan \(2024\)](#), [Chen et al \(2024\)](#), [Metger et al \(2024\)](#)

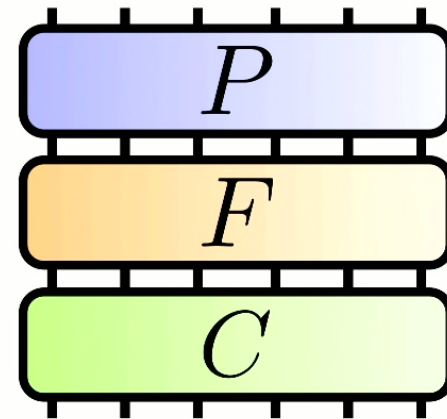


What is known so far

In what *depth* can a local quantum circuit look like a Haar-random unitary?

- Local circuits can form **pseudorandom unitaries** in depth **poly n** , in 1D circuits
polylog n , in all-to-all circuits

Ji, Liu, Song (2018), Metger, Poremba, Sinha, Yuen (2024)
Ma, Huang (2024)

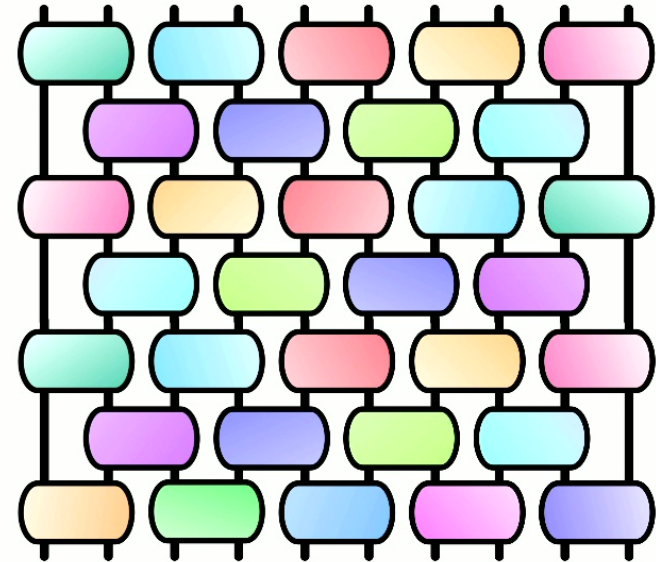


What is known so far

In what *depth* can a local quantum circuit look like a Haar-random unitary?

- Local circuits can form **pseudorandom unitaries** in depth **poly n** , in 1D circuits
polylog n , in all-to-all circuits

Ji, Liu, Song (2018), Metger, Poremba, Sinha, Yuen (2024)
Ma, Huang (2024)

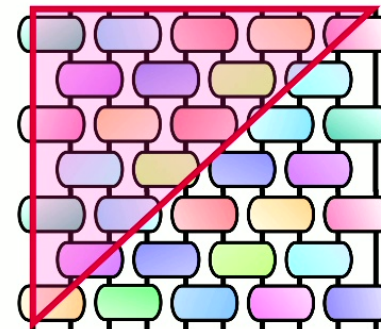
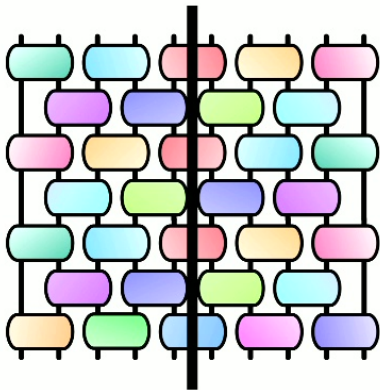


What is known so far

These circuit depths seem very reasonable!

For example, 1D circuits require linear depth to...

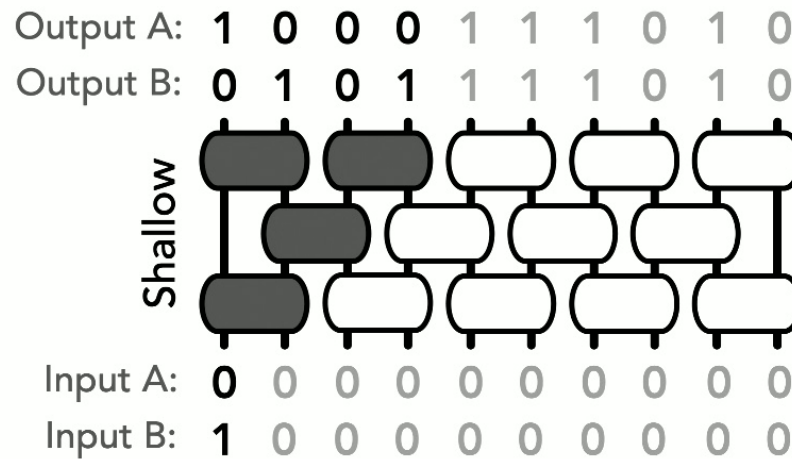
- Generate high entanglement
- Have extensive light-cones



What is known so far

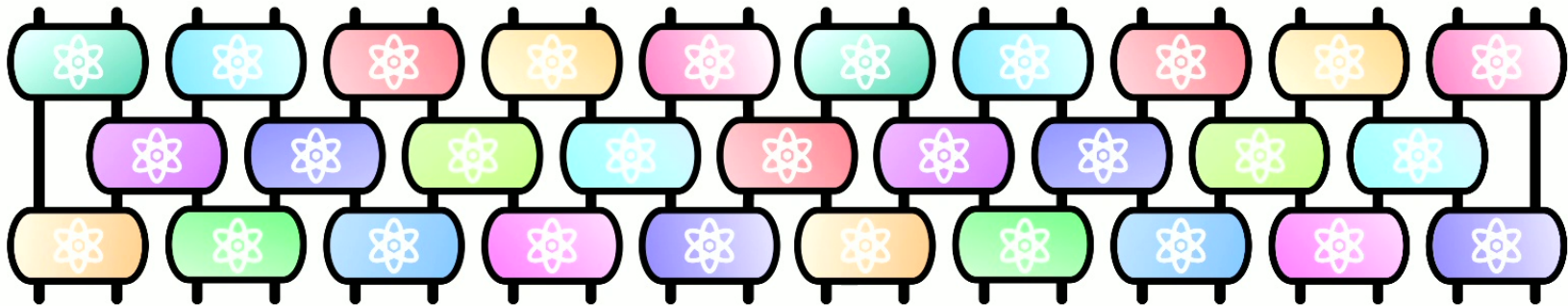
These circuit depths seem very reasonable!

Classical circuits *require* linear depth in 1D to form pseudorandom permutations or designs



Random unitaries in extremely low depth

Theorem 2: Quantum circuits can form **pseudorandom unitaries** in depth **$\text{polylog } n$** , in 1D circuits
 $\text{polyloglog } n$, in all-to-all connected circuits

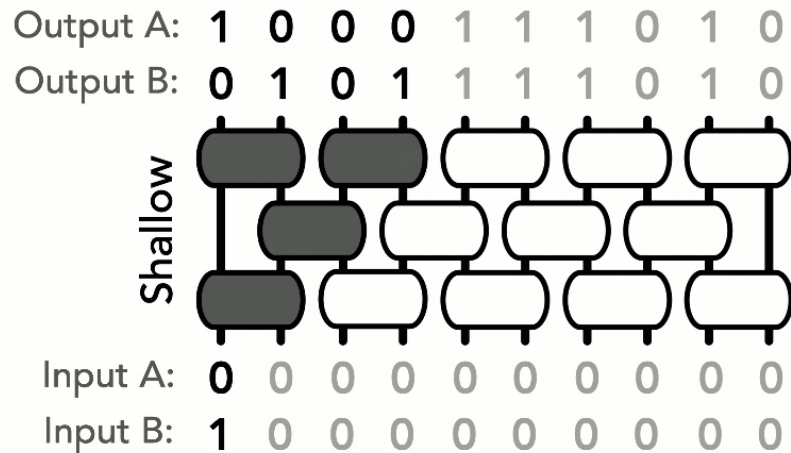


TS, Haferkamp, Huang arxiv: 2407:07754 (2024)

Intuition

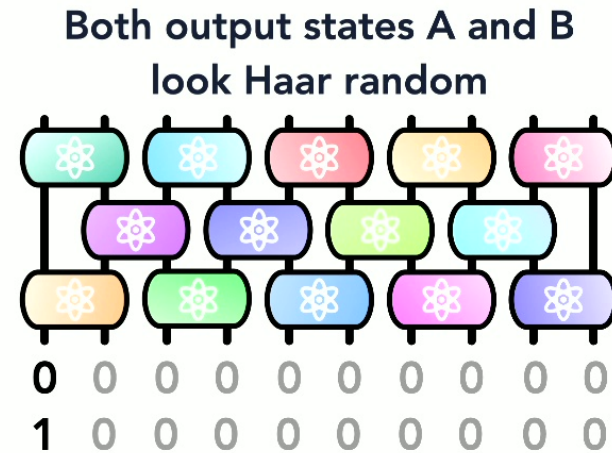
Quantum circuits can **locally hide** information into **non-commuting** observables

Classical



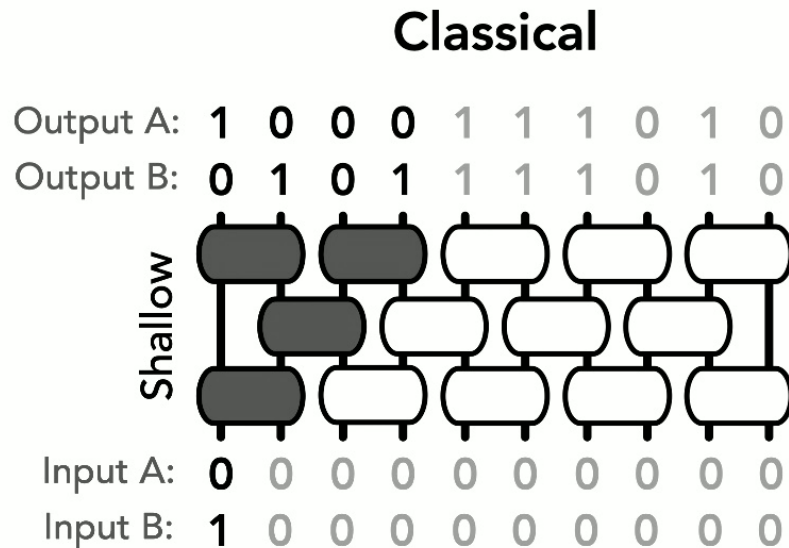
vs

Quantum



Intuition

Quantum circuits can **locally hide** information into **non-commuting** observables



Classical experiment:

1. Prepare local information
2. Evolve under **classical** circuit
(info is spread into ξ -bit observables)
3. Measure in Z -basis

Intuition

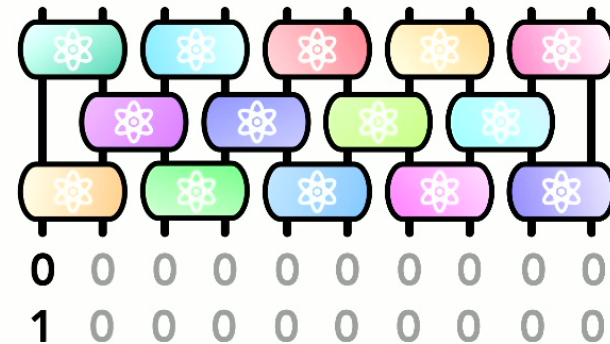
Quantum circuits can **locally hide** information into **non-commuting** observables

Quantum experiment:

1. Prepare local information
2. Evolve under **quantum** circuit
(info is spread into ξ -**qubit** observables)
3. Measure in some choice of basis

Quantum

Both output states A and B
look Haar random



Intuition

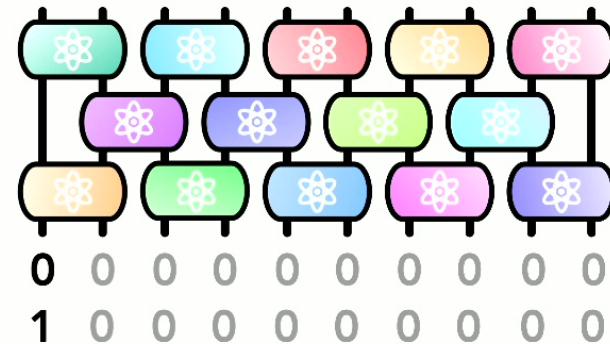
Key point: Any fixed measurement basis is highly unlikely to commute with a random ξ -qubit observable

Quantum experiment:

1. Prepare local information
2. Evolve under **quantum** circuit
(info is spread into ξ -**qubit** observables)
3. Measure in some choice of basis

Quantum

Both output states A and B
look Haar random

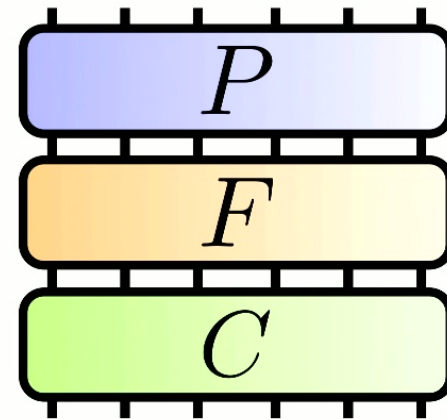


What is known so far

In what *depth* can a local quantum circuit look like a Haar-random unitary?

- Local circuits can form **pseudorandom unitaries** in depth **poly n** , in 1D circuits
polylog n , in all-to-all circuits

Ji, Liu, Song (2018), Metger, Poremba, Sinha, Yuen (2024)
Ma, Huang (2024)

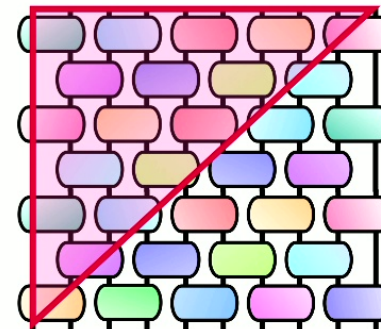
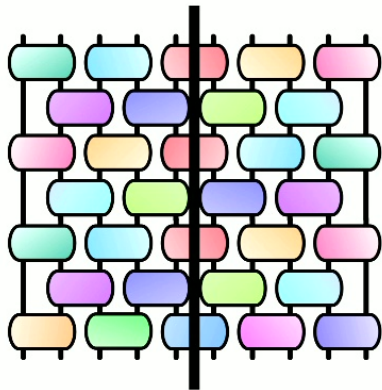


What is known so far

These circuit depths seem very reasonable!

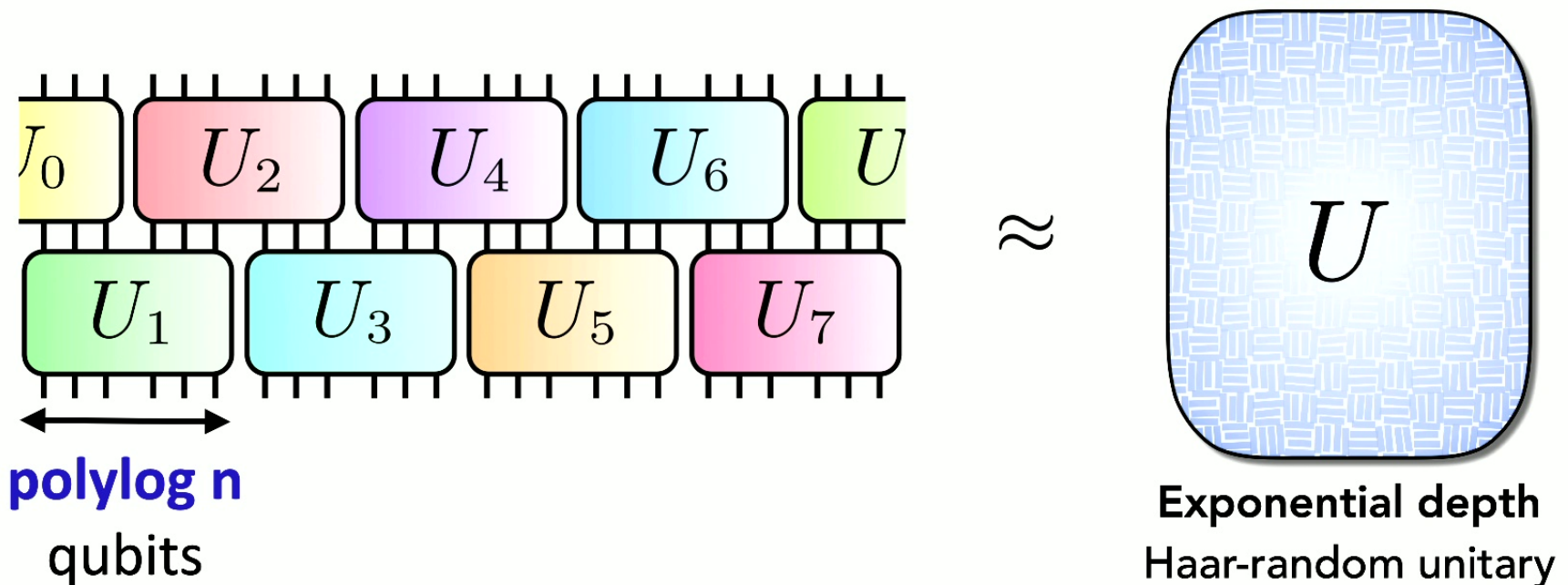
For example, 1D circuits require linear depth to...

- Generate high entanglement
- Have extensive light-cones



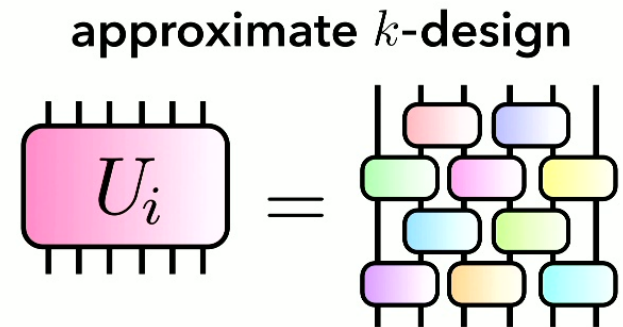
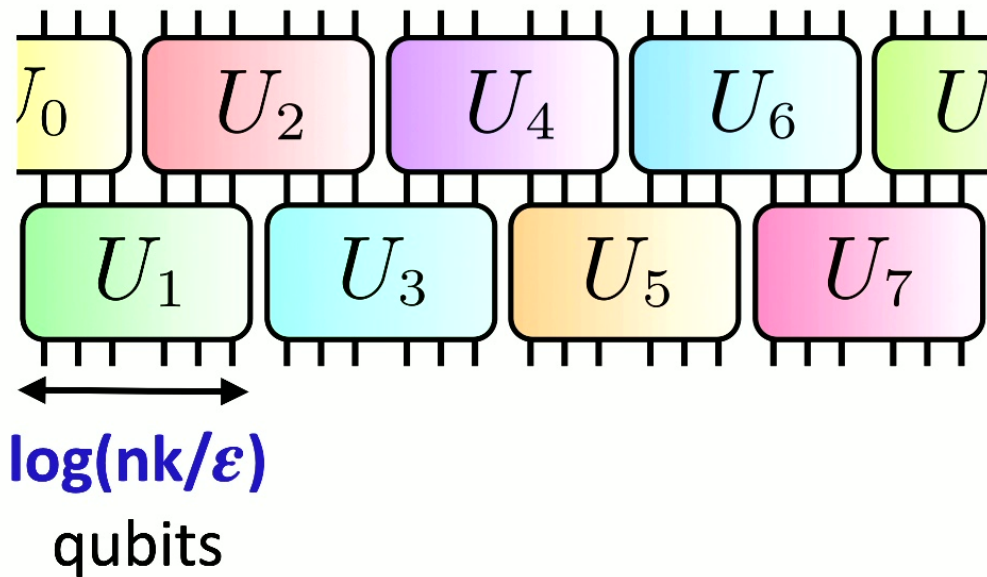
Building random unitaries brick-by-brick

A general approach to exponentially reduce the depth of a random unitary



Building random unitaries brick-by-brick

Theorem 1: If each small unitary is drawn from an ε/n -approx k -design on $\log n$ qubits, the circuit forms an ε -approx k -design on n qubits



Building random unitaries brick-by-brick

Theorem 1: If each small unitary is drawn from an ε/n -approx k -design on $\log n$ qubits, the circuit forms an ε -approx k -design on n qubits

For the experts: Our k -designs are close to Haar in relative error

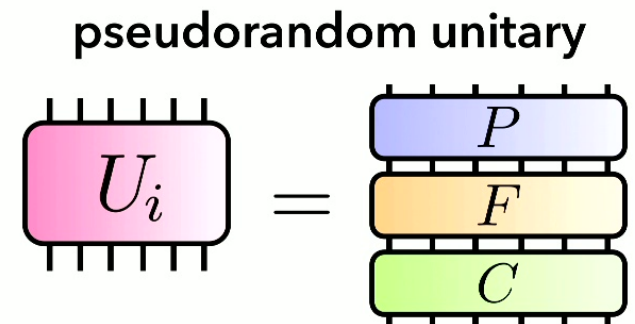
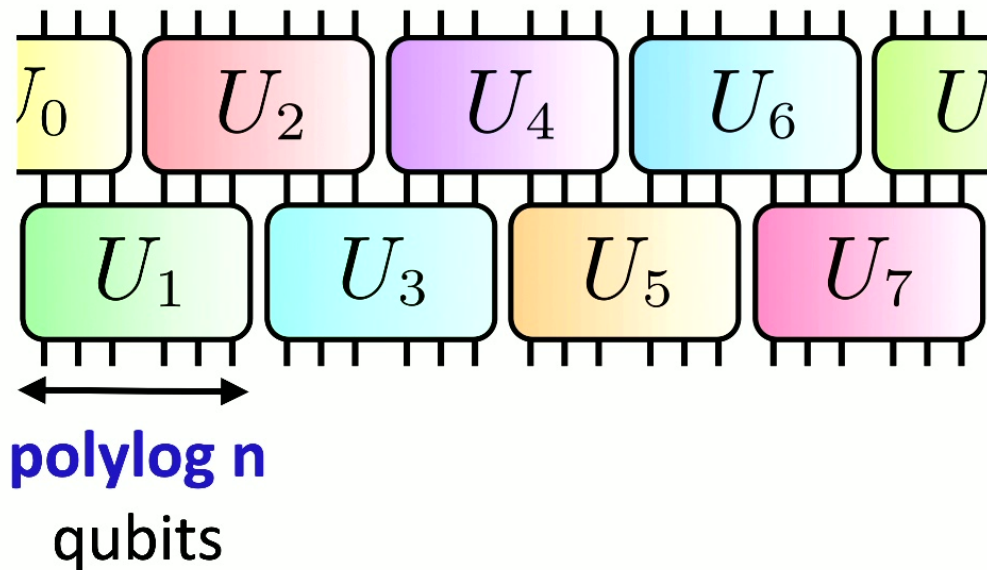
$$(1 - \varepsilon)\Phi_H \preceq \Phi_\varepsilon \preceq (1 + \varepsilon)\Phi_H$$

$$\text{w/ } \Phi_\varepsilon = \mathbb{E}_{U \sim \mathcal{E}} [U^{\otimes k} \rho U^{\dagger, \otimes k}]$$

This is strictly stronger than other notions of error (diamond norm, etc.)

Building random unitaries brick-by-brick

Theorem 2: If each small unitary is drawn from a PRU on $\text{polylog } n$ qubits, the circuit forms a PRU on n qubits



Building random unitaries brick-by-brick

Theorem 1: If each small unitary is drawn from an ε/n -approx k -design on $\log n$ qubits, the circuit forms an ε -approx k -design on n qubits

For the experts: Our k -designs are close to Haar in relative error

$$(1 - \varepsilon)\Phi_H \preceq \Phi_\varepsilon \preceq (1 + \varepsilon)\Phi_H$$

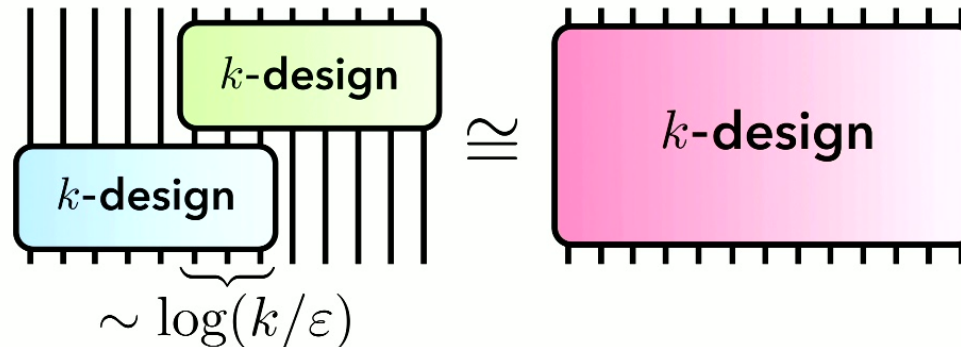
$$\text{w/ } \Phi_\varepsilon = \mathbb{E}_{U \sim \mathcal{E}} [U^{\otimes k} \rho U^{\dagger, \otimes k}]$$

This is strictly stronger than other notions of error (diamond norm, etc.)

Gluing random unitaries

Our proof is built upon a simple lemma

Lemma: Let $V_{ABC} = U_{AB} U_{BC}$, where U_{AB} and U_{BC} are drawn from $\varepsilon/4$ -approx unitary k -designs. V_{ABC} is an ε -approx k -design if $n_B > \log(k/\varepsilon)$.

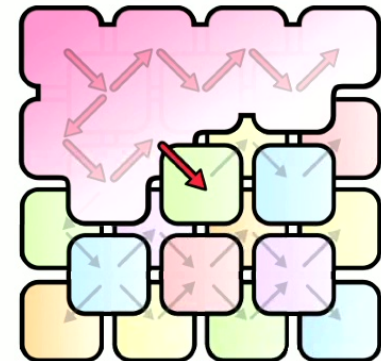
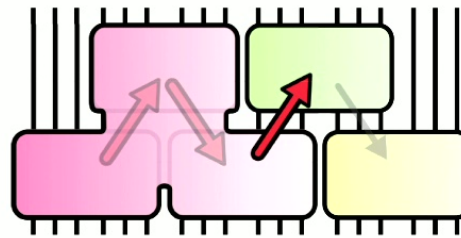


Gluing random unitaries

Our proof is built upon a simple lemma

Lemma: Let $V_{ABC} = U_{AB} U_{BC}$, where U_{AB} and U_{BC} are drawn from $\varepsilon/4$ -approx unitary k -designs. V_{ABC} is an ε -approx k -design if $n_B > \log(k/\varepsilon)$.

Applying the lemma n times
yields Theorems 1 and 2

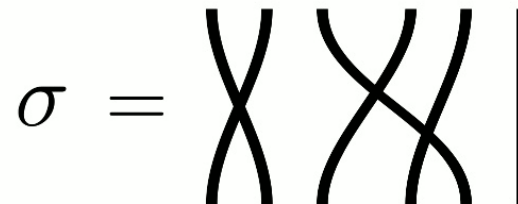


Proof of the gluing lemma

Background: The *twirl* over k copies of a Haar-random unitary is

$$\mathbb{E}_U [U^{\otimes k} \rho U^{\dagger, \otimes k}] = \sum_{\sigma, \tau} \text{tr}(\rho \sigma^{-1}) \cdot \text{Wg}_{\sigma, \tau} \cdot \tau$$

Here, σ and τ are permutations of the k copies:



Weingarten matrix $\text{Wg}_{\sigma, \tau}$ = inverse of Gram matrix, $G_{\sigma, \tau} = \text{tr}(\sigma \tau^{-1})$

Proof of the gluing lemma

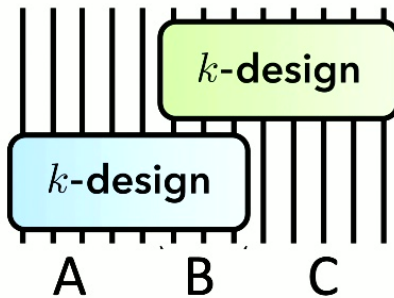
Key fact: Permutations are approximately orthogonal for $k^2 \ll 2^n$

Harrow (2023)

$$G_{\sigma,\tau}/2^{nk} \approx 2^{nk} Wg_{\sigma,\tau} \approx 1_{\sigma,\tau}$$

This implies that $\mathbb{E}_U [U^{\otimes k} \rho U^{\dagger, \otimes k}] \approx \frac{1}{2^{nk}} \sum_{\sigma} \text{tr}(\rho \sigma^{-1}) \cdot \sigma$

And



$$\approx \frac{1}{2^{(n+n_B)k}} \sum_{\sigma, \tilde{\sigma}} \text{tr}(\rho \sigma_A^{-1} \sigma_B^{-1} \tilde{\sigma}_C^{-1}) \cdot \text{tr}(\sigma_B \tilde{\sigma}_B^{-1}) \cdot \sigma_A \tilde{\sigma}_B \tilde{\sigma}_C$$

* \approx denotes approximation to within relative error $O(k^2/2^n)$ or $O(k^2/2^{n_B})$

Proof of the gluing lemma

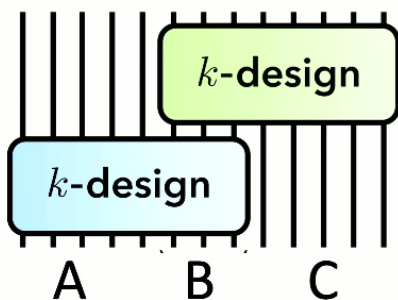
Key fact: Permutations are approximately orthogonal for $k^2 \ll 2^n$

Harrow (2023)

$$G_{\sigma,\tau}/2^{nk} \approx 2^{nk} Wg_{\sigma,\tau} \approx 1_{\sigma,\tau}$$

This implies that $\mathbb{E}_U [U^{\otimes k} \rho U^{\dagger, \otimes k}] \approx \frac{1}{2^{nk}} \sum_{\sigma} \text{tr}(\rho \sigma^{-1}) \cdot \sigma$

And



$$\approx \frac{1}{2^{(n+n_B)k}} \sum_{\sigma, \tilde{\sigma}} \text{tr}(\rho \sigma_A^{-1} \sigma_B^{-1} \tilde{\sigma}_C^{-1}) \cdot \text{tr}(\sigma_B \tilde{\sigma}_B^{-1}) \cdot \sigma_A \tilde{\sigma}_B \tilde{\sigma}_C$$

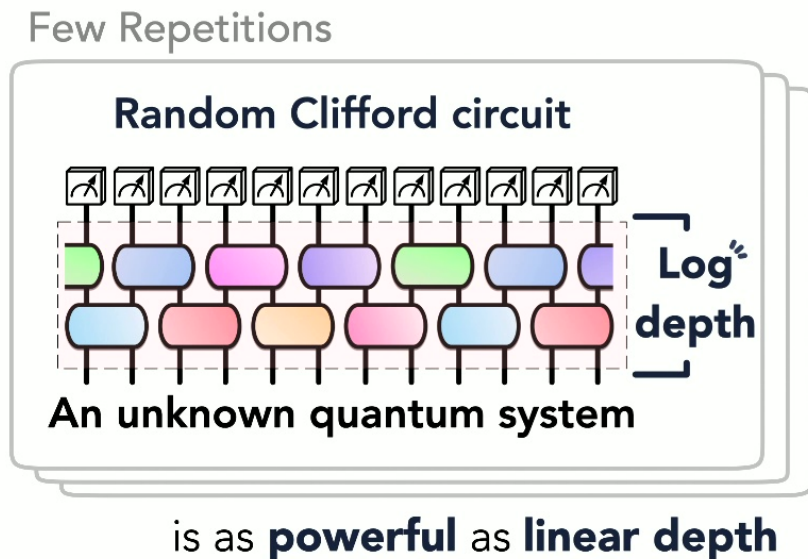
$$\approx \frac{1}{2^{nk}} \sum_{\sigma} \text{tr}(\rho \sigma^{-1}) \cdot \sigma \approx \text{[Pink box labeled } k\text{-design]}$$

* \approx denotes approximation to within relative error $O(k^2/2^n)$ or $O(k^2/2^{n_B})$



Provably-efficient shallow classical shadows

Classical shadows one to estimate the fidelity of an unknown quantum state with exponentially many target states, from a small number of experiments

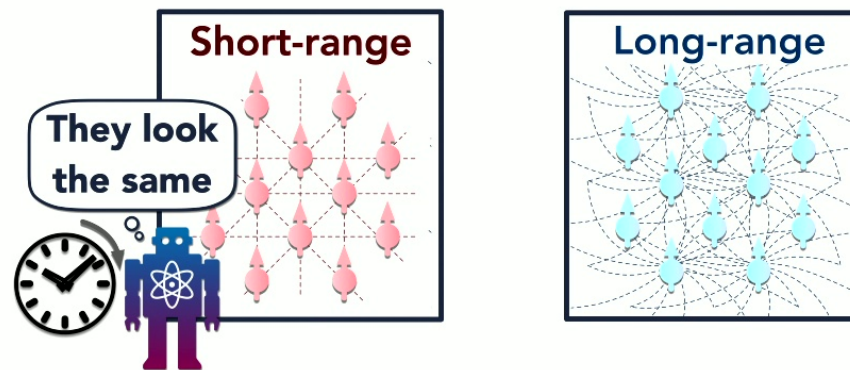


Original protocol requires a **deep** random Clifford unitary

Our results show that **log depth** random Clifford circuits are just as good

Opens door to classical shadows on many (~ 40-50) qubits at current noise rates

Our results immediately extend many existing separations in quantum learning to low complexity systems

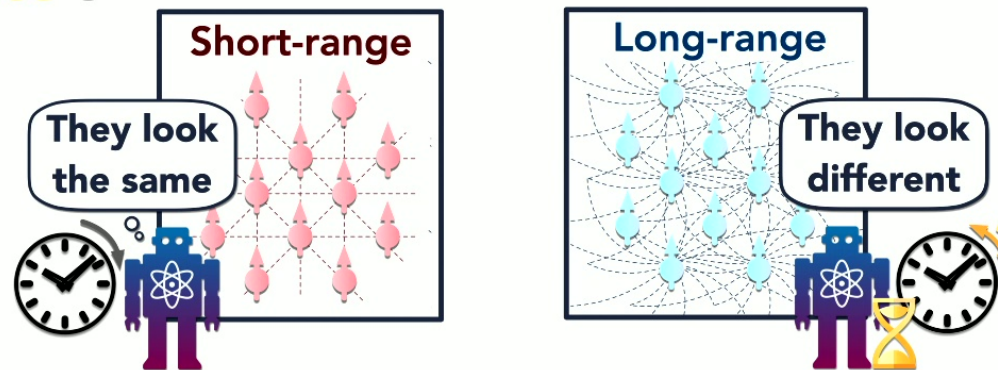


see also: [TS + Google Quantum \(2023\)](#), [Cotler, TS, Mohseni \(2023\)](#)

Power of time-reversal in quantum learning

Our results immediately extend many existing separations in quantum learning to low complexity systems

Intriguingly, many such tasks **can be solved** when given access to both a unitary U and its **time-reverse** U^\dagger



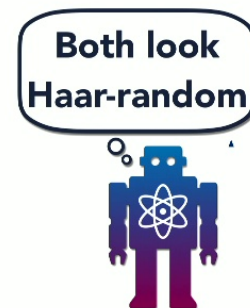
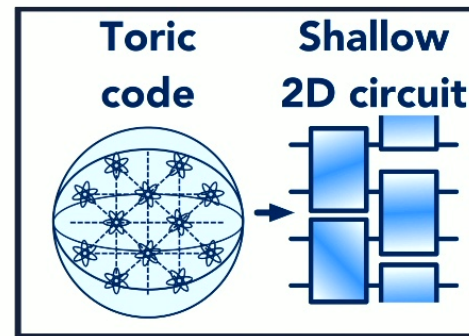
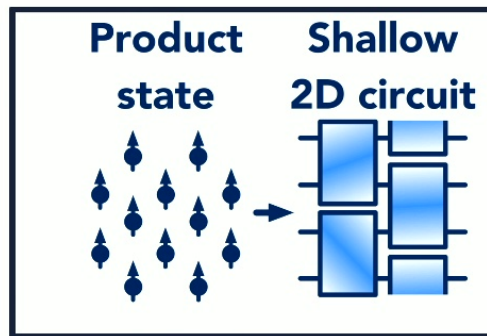
Corollary: Quantum expts with time-reversal can feature **exponential advantages** over any quantum expt without time-reversal

see also: [TS + Google Quantum \(2023\)](#), [Cotler, TS, Mohseni \(2023\)](#)

Hardness of recognizing topological order

Verifying topological order is a notorious challenge in atomic and materials expts

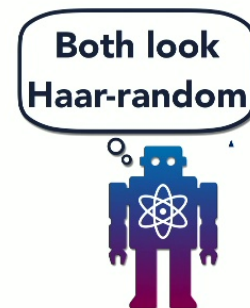
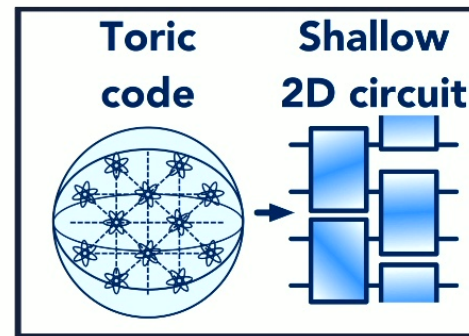
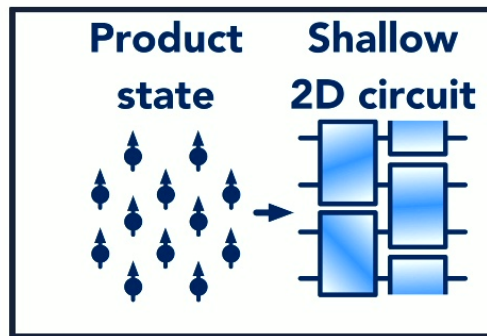
Corollary: Recognizing whether an unknown quantum state has **topological vs. trivial** order is **quantum computationally hard** (for corr. len. \sim polylog n).



Hardness of recognizing topological order

Verifying topological order is a notorious challenge in atomic and materials expts

Corollary: Recognizing whether an unknown quantum state has **topological vs. trivial** order is **quantum computationally hard** (for corr. len. \sim polylog n).



A worst-case statement! **Open Q:** Does this extend to states in real world settings?

Summary

Shallow quantum dynamics can rapidly become **indistinguishable** from deep **Haar-random** unitaries

Fundamentally, this is enabled by the abundance of **non-commuting observables** in large quantum systems

Some open questions

- Several smaller mathematical questions remain open:
 - Our designs have depth $k \times \log(n/\varepsilon)$; lower bounds give $k + \log(n/\varepsilon)$
 - Can we achieve the same depths with random 2-qubit brickwork circuits?
- A new definition of unitary designs to capture scrambling dynamics?
[Brandao, Huang, Ma, TS \(forthcoming\)](#)
- Farther afield: Quantum advantages in far-from-Haar random dynamics?
 - Constant-depth random circuit sampling, sparse random Hamiltonians, out-of-time-order correlators, ...
[Napp et al. \(2019\)](#), [Bao, Block, Altman \(2021\)](#), [McGinley et al. \(2024\)](#); [Chen et al. \(2023\)](#); [Google Quantum \(2021\)](#)