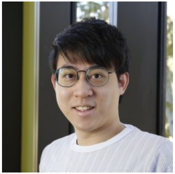
Random unitaries in extremely low depth

Jonas Haferkamp

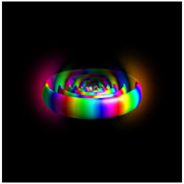
Based on work with:

Thomas Schuster, Hsin-Yuan Huang



A quantum revolution!

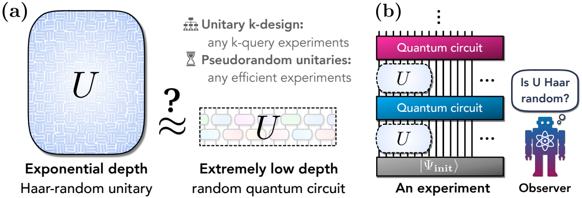
- Progress in the control of quantum many-body systems!
- Characterize/benchmark properties of quantum systems.

Random unitaries

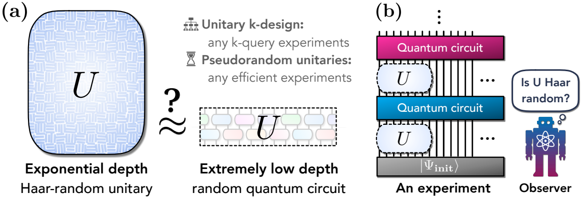
Designs and pseudorandom unitaries

- Random unitaries are too expensive!



Designs and pseudorandom unitaries

- Random unitaries are too expensive!



- Unitary k-design: Indistinguishable from k copies of U.
- PRU's: Indistinguishable in polynomial time.

Approximate unitary k-designs

$$(1-\varepsilon)\,\Phi_H \preceq \Phi_{\mathcal{E}} \preceq (1+\varepsilon)\,\Phi_H,$$

where

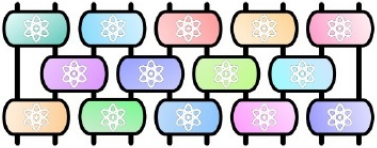
$$\Phi_{\mathcal{E}}(A) := \mathbb{E}_{U\sim\mathcal{E}}\left[U^{\otimes k} A U^{\dagger,\otimes k}\right].$$

- CP ordering: $A \preceq B$ if $B - A$ is completely positive.

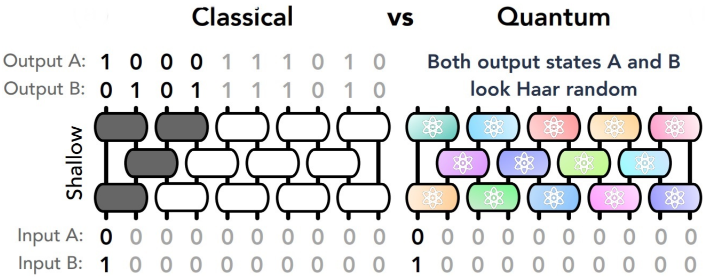
Approximate designs in extremely low depth

Theorem

Approximate unitary designs can be generated in $O(k \log(n))$ *depth on any geometry, including 1D lines. For* $k = 3$*, the gates can be chosen to be Cliffords.*



How about classical circuits?

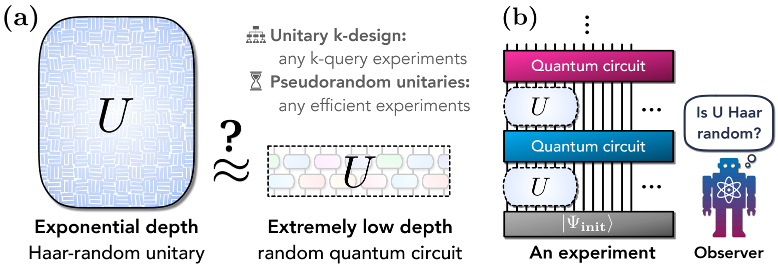


- Classical circuits require linear depth to be approximate 2-wise independent.

PRU's in extremely low depth

Theorem

PRU's can be generated in depth $\omega(\log(n))$ on any geometry, including a 1D line.



Optimality of our results

Theorem

Approximate 2-designs require $\Omega(\log(n))$ *depth.*

- Lower bound on anticoncentration in any basis.

Theorem

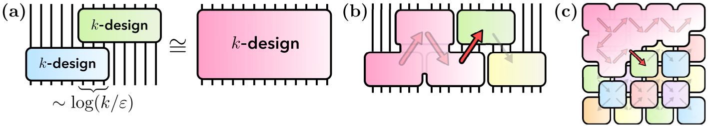
PRU's require $\omega(\log(n))$ *depth.*

- Learning is efficient in depth $O(\log(n))$.

Huang, Liu, Broughton, Kim, Anshu, Landau, McClean, STOC 2023

Proof sketch

Random unitaries from gluing



Theorem

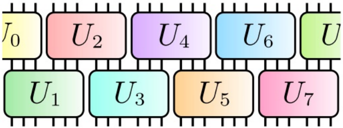
Local patches with $\xi \geq \log_2(nk)$ *qubits form an approximate design.*

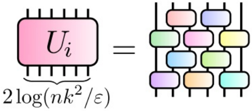
Approximate designs from gluing

Use random quantum circuits in the blocks:

Theorem

Coarse-grained random quantum circuits generate ε-approximate designs in depth $O(\mathrm{polylog}(k)(nk + \log(1/\varepsilon)))$.





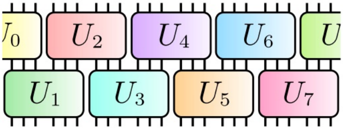
Chen, Haah, Haferkamp, Liu, Metger, Tan, FOCS 2025

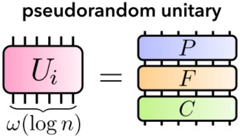
PRUs from gluing

Use "PFC" in the blocks:

Theorem

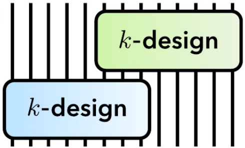
For P a pseudorandom permutation on the computational basis, F a pseudorandom diagonal unitary and C a uniformly random Clifford unitary, PFC is a PRU. The depth of PFC is $\mathrm{poly}(n)$.





Metger, Poremba, Sinha, Yuen, STOC 2024; Huang, Ma, FOCS 2024

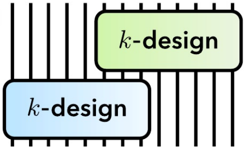
Proving the gluing lemma



- Expand blocks in permutations:

$$\Phi_H(A) \equiv \mathbb{E}_{U\sim\mathcal{E}_H}[U^{\otimes k} A\,(U^\dagger)^{\otimes k}] = \sum_{\sigma,\tau\in S_k} \mathrm{Tr}(A\,\sigma^{-1})\,\mathrm{Wg}(\sigma\tau^{-1}; 2^{\xi/2})\,\tau\,.$$

Proving the gluing lemma



- Expand blocks in permutations:

$$\Phi_H(A) \equiv \mathbb{E}_{U\sim\mathcal{E}_H}[U^{\otimes k} A (U^\dagger)^{\otimes k}] = \sum_{\sigma,\tau\in S_k} \mathrm{Tr}(A\,\sigma^{-1})\,\mathrm{Wg}(\sigma\tau^{-1}; 2^{\xi/2})\,\tau.$$

- Exploit approximate orthogonality of permutations:

$$||G - \mathbb{1}_{k!\times k!}||_\infty \leq \frac{k^2}{2^{\xi/2}}, \qquad G_{\pi,\sigma} \equiv \frac{1}{2^{\xi/2}}\mathrm{Tr}[\pi\sigma].$$

Harrow, Lett. in Math. Phys. 2024

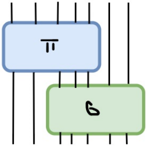
Proving the gluing lemma

$$\Phi_H \approx \sum_{\pi \in S_k} |\pi\rangle\langle\pi|, \qquad \langle\pi| \equiv \frac{1}{2^{\xi/4}} \mathrm{Tr}[\pi \bullet]$$

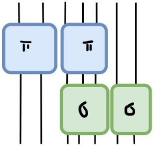
Proving the gluing lemma

$$\Phi_H \approx \sum_{\pi \in S_k} |\pi\rangle\langle\pi|, \qquad \langle\pi| \equiv \frac{1}{2^{\xi/4}} \mathrm{Tr}[\pi \bullet]$$

$$\Phi_{H,1,2} \circ \Phi_{H,2,3} = \sum_{\pi,\sigma \in S_k}$$



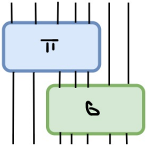
$$= \sum_{\pi,\sigma \in S_k}$$

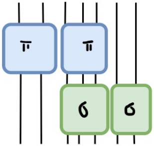


.

Proving the gluing lemma

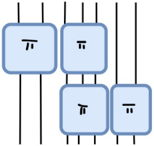
$$\Phi_H \approx \sum_{\pi \in S_k} |\pi\rangle\langle\pi|, \qquad \langle\pi| \equiv \frac{1}{2^{\xi/4}} \mathrm{Tr}[\pi \bullet]$$

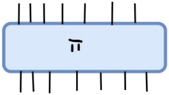
$$\Phi_{H,1,2} \circ \Phi_{H,2,3} = \sum_{\pi,\sigma \in S_k}$$ 

$$= \sum_{\pi,\sigma \in S_k}$$ 

.

- Use approximate orthogonality again:

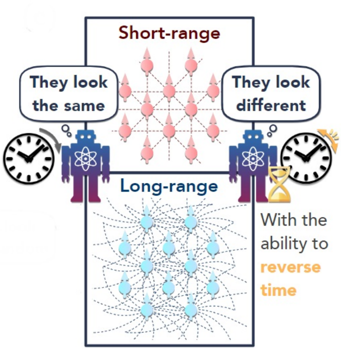
$$\Phi_{H,1,2} \circ \Phi_{H,2,3} \approx \sum_{\pi \in S_k}$$ 

$$= \sum_{\pi \in S_k}$$ 

$$\approx \Phi_{H,1,2,3}.$$

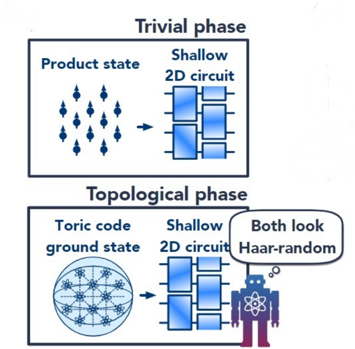
Applications

Power of time-reversal in quantum learning



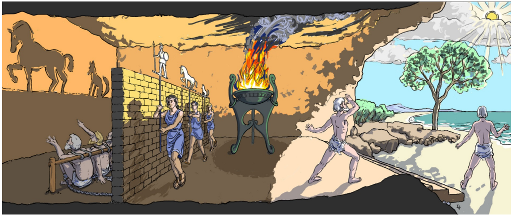
- Distinguish 2D local circuit U_{2D} from U'_{2D} augmented with a long range interaction $e^{i\phi Z_i Z_j}$.
- Shallow PRU's break under time-reversal.

Hardness of recognising topological phases



- Hard to distinguish trivial order and toric code after appyling PRU.
- Topological order up to circuits of subextensive depth.

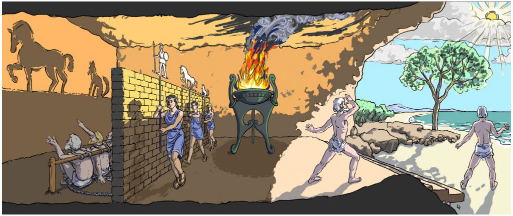
Shallow shadows



Classical shadows can be obtained with $\log(n)$-depth circuits:

- Use the same inversion map as for Haar random measurement-channel.
- Learn M observables O with $O(\max_O ||O||_1 \log(M))$ samples.

Shallow shadows



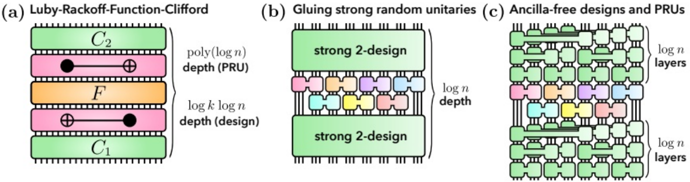
Classical shadows can be obtained with $\log(n)$-depth circuits:

- Use the same inversion map as for Haar random measurement-channel.
- Learn M observables O with $O(\max_O ||O||_1 \log(M))$ samples.
- $|| \bullet ||_1$ scaling is bias from wrong inversion map.

Updates

Sophisticated constructions

- Inverse robust (strong) designs and PRUs with log-depth circuits.
- Near optimal depth with ancillae!
- Designs in quantum constant time, i.e. in QAC_f^0.



Schuster, Ma, Lombardi, Brandao, and Huang, arXiv preprint
Cui, Schuster, Brandao, and Huang, arXiv preprint
Foxman, Parham, Vasconcelos, Yuen, arXiv preprint

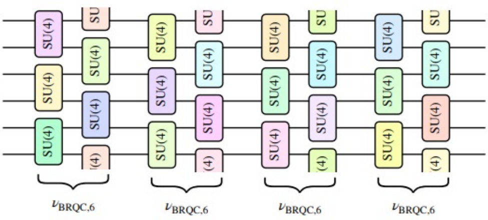
Will it glue?

Notion of randomness	Group U(2^n)	O(2^n)	USp(2^n)	Cl(n)	M(n)
additive-error group designs	$\mathcal{O}(\log(\frac{n}{\epsilon}))$ [21,22]	Ω(L)	Ω(L)	$k \geq 4$ $\Omega(L)$	$\Omega(n)$
relative-error state designs	$\Theta(\log(\frac{n}{\epsilon}))$ [21,22]	$\Omega(\mathrm{R})^*, \Omega(n)^\dagger$	Ω(L)	$k \geq 4$ $\Omega(\mathrm{R})^*, \Omega(n)^\dagger$	$\Omega(n)$
relative-error group designs	$\Theta(\log(\frac{n}{\epsilon}))$ [21,22]	all above	all above, $\Omega(n)^\dagger$	$k \geq 4$ all above	$\Omega(n)$
additive-error state designs	$\mathcal{O}(\log(\frac{n}{\epsilon}))$ [21,22]	$\mathcal{O}(\log(\frac{n}{\epsilon}))$	$\mathcal{O}(\log(\frac{n}{\epsilon}))$	$k < 6$: $\mathcal{O}(\log(\frac{n}{\epsilon}))$	$\Omega(n)$
anti-concentration	$\Theta(\log(n))$ [25,26]	$\mathcal{O}(\log(n))$ [27]	$\mathcal{O}(\log(n))$	$\Theta(\log(n))$ [28,29]	$\Omega\left(\frac{n^{1/3}}{\log(n)}\right)$

- L = minimal depth for lightcone to touch constant fraction of qubits.
- R = diameter of underlying architecture.

L. Grevink, J. Haferkamp, M. Heinrich, J. Helsen, M. Hinsche, T. Schuster, and Z. Zimboás, arXiv preprint
M. West, D. Garcie-Martin, N.L. Diaz, M. Cerezo, M. Larocca, arXiv preprint

Unstructured random quantum circuits

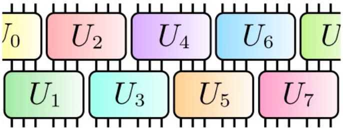


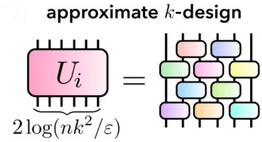
- Approximate state 2-designs in log-depth!
- Exploiting old stat-mech approaches to expectation values of random circuits.

J. Haferkamp, M. Heinrich, J. Helsen, I. Roth, upcoming

Outlook

- Random quantum circuits with iid gates are PRU and k-designs?
- Optimal scaling of $\log(n) + k$ for designs?
- More applications!





Bonus slides

Why is the purity not a counterexample?

- Unitary 2-design have maximal entanglement but shallow circuits do not!
- $\mathbb{E}\mathrm{Tr}[\mathrm{Tr}_A(|\psi\rangle\langle\psi|)^2] \leq (1+\varepsilon)2^{-\Omega(n)}$?

Why is the purity not a counterexample?

- Unitary 2-design have maximal entanglement but shallow circuits do not!
- $\mathbb{E}\mathrm{Tr}[\mathrm{Tr}_A(|\psi\rangle\langle\psi|)^2] \leq (1+\varepsilon)2^{-\Omega(n)}$?
- Relative errors only for psd observables. But

$$\mathbb{E}\mathrm{Tr}\left[\mathrm{Tr}_A(|\psi\rangle\langle\psi|)^2\right] = \mathbb{E}\mathrm{Tr}\left[(|\psi\rangle\langle\psi|)^{\otimes 2}\mathbb{1}_A \otimes \mathbb{F}_B\right].$$

Why is the purity not a counterexample?

- Unitary 2-design have maximal entanglement but shallow circuits do not!
- $\mathbb{E}\mathrm{Tr}[\mathrm{Tr}_A(|\psi\rangle\langle\psi|)^2] \leq (1+\varepsilon)2^{-\Omega(n)}$?
- Relative errors only for psd observables. But

$$\mathbb{E}\mathrm{Tr}\left[\mathrm{Tr}_A(|\psi\rangle\langle\psi|)^2\right] = \mathbb{E}\mathrm{Tr}\left[(|\psi\rangle\langle\psi|)^{\otimes 2}\mathbb{1}_A \otimes \mathbb{F}_B\right].$$

- Relative errors only in the SWAP-test probability $\frac{1}{2} + \mathrm{Tr}[\mathrm{Tr}_A(|\psi\rangle\langle\psi|)^2]$.