Random unitaries from random quantum circuits

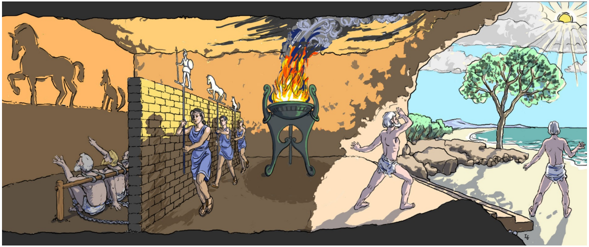
Jonas Haferkamp

Based on work with:

Chi-Fang (Anthony) Chen, Jeongwan Haah, Hsin-Yuan (Robert) Huang, Yunchao Liu, Tony Metger, Thomas Schuster, and Xinyu (Norah) Tan

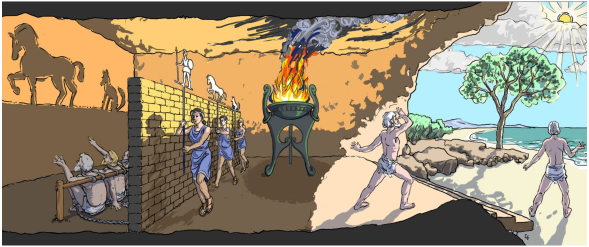
Part I: Why random unitaries? A positive outlook.

A quantum state's shadow



- Prediction of observables $\langle O \rangle$ from classical snapshots of state.

A quantum state's shadow



- Prediction of observables $\langle O \rangle$ from classical snapshots of state.
- Rotate state by random quantum operation (unitary) and measure.

Aaronson, STOC 2018;
Huang, Kueng, Preskill, Nat. Phys 2021

Build-A-Shadow

- Average measurement channel:

$$\mathcal{M}(|\psi\rangle) := \underbrace{\mathbb{E}_U}_{\text{classical randomness}} \left(\underbrace{\sum_{b\in\{0,1\}^n} |\langle\psi|U|b\rangle|^2}_{\text{quantum randomness}} U|b\rangle\langle b|U^\dagger \right).$$

Build-A-Shadow

- Average measurement channel:

$$\mathrm{M}(|\psi\rangle) := \underbrace{\mathbb{E}_U}_{\text{classical randomness}} \left(\underbrace{\sum_{b\in\{0,1\}^n} |\langle\psi|U|b\rangle|^2}_{\text{quantum randomness}} U|b\rangle\langle b|U^\dagger \right).$$

- Classical shadow from samples and inverting M:

$$\hat{\rho} := \mathrm{M}^{-1}\left(\frac{1}{N}\sum_{i=1}^{N} U_i|b_i\rangle\langle b_i|U_i^\dagger\right).$$

- Estimate $\langle O\rangle_\psi$ by $\mathrm{Tr}[\hat{\rho}O]$.
- Guarantees from $\mathrm{Var}(\mathrm{Tr}[\hat{\rho}O])$.
- 3rd moments of Haar measure suffice!

Chapters

1. Why random unitaries? A positive outlook.
2. Unitary designs and pseudorandom unitaries
3. Random quantum circuits converge to designs.
4. Random unitaries in extremely low depth.
5. Outlook

Part II: Unitary designs and pseudorandom unitaries

Quantum pseudoranomness

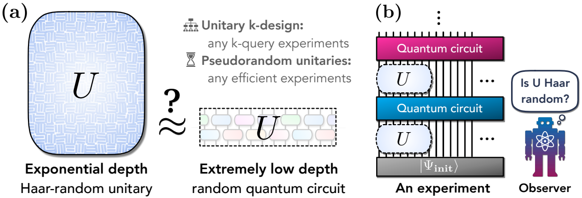
- Haar random unitaries require exponentially deep circuits.

Quantum pseudoranomness

- Haar random unitaries require exponentially deep circuits.
- Haar random unitaries are hard to learn from counting arguments. 

Quantum pseudoranomness

- Haar random unitaries require exponentially deep circuits.
- Haar random unitaries are hard to learn from counting arguments. 



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

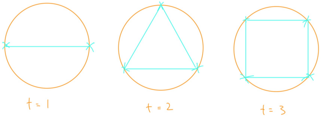
Unitary designs

Unitary k-design ν matches the kth moments of Haar measure

$$\Phi_{\mu_H}^{(k)} = \Phi_{\nu}^{(k)}$$

for

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



- Example: Moments of $U(1)$ $\mathbb{E}_{\phi} e^{\mathrm{i}t\phi} = 0$, but $e^{\mathrm{i}2\times 0} + e^{\mathrm{i}2\times\pi} \neq 0$.

Additive vs. multiplicative error approximate designs

Moment operator:

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

Additive error approximate designs:

$$||\Phi_{\mu_H} - \Phi_\nu||_\diamond \le \varepsilon.$$

Multiplicative error approximte designs:

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

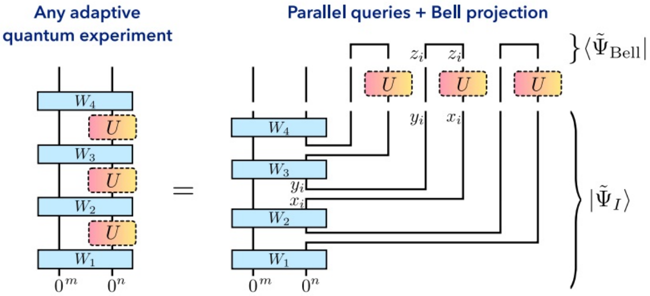
- CP ordering: $A \preceq B$ if $B - A$ is completely positive.

Information theoretical quantum pseudorandomness

- Approximate designs look Haar in any experiment that queries k-copies.

Information theoretical quantum pseudorandomness

- Approximate designs look Haar in any experiment that queries k-copies.
- Additive error $1/\mathrm{superpoly}(n)$-approximate designs property imply non-adaptive security.
- Multiplicative error $1/\mathrm{superpoly}(n)$-approximate designs property implies adaptive security.

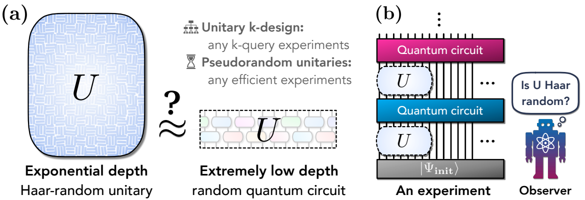


PRU's

Definition (Pseudorandom unitaries)

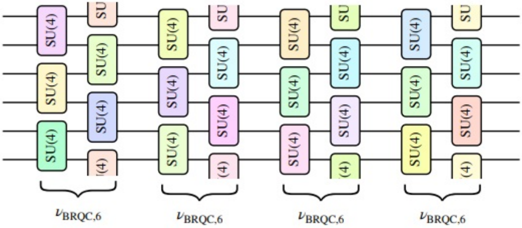
A family of quantum circuits $\{U_l\}^m_{l\in\{0,1\}}$ with $m = \mathrm{poly}(n)$ that can be efficiently prepared. For any poly-time algorithm $A^U(1^n)$ that queries U any number of times, satisfies

$$\Pr_l[A^U(1^n) = 1] \approx \Pr_{U\sim\mu_H}[A^U(1^n) = 1].$$



Part II: Random quantum circuits converge to designs

Random quantum circuits



- Typically refers to circuits with gates drawn iid.
- Example: Brickwork circuits with gates drawn from Haar measure.
- Depth d corresponds to d-fold convolution: $\nu_{\mathrm{BRQC},6}^{*4}$.
- Random walk on unitary group.

Unitary designs from spectral gaps

Gap of k-th moment operator:

$$\Delta_k(\nu) := 1 - \underbrace{\left\| \mathop{\mathbb{E}}_{U\sim\nu} U^{\otimes k} \otimes \overline{U}^{\otimes k} - \mathop{\mathbb{E}}_{U\sim\mu_H} U^{\otimes k} \otimes \overline{U}^{\otimes k} \right\|_\infty}_{=:g(\nu,k)} .$$

- Submultiplicative $g(\nu^{*d}, k) \leq g(\nu, k)^d$.
- ν is $g(\nu, k)2^{2nk}$-approximate designs. Brandão, Harrow, Horodecki, Comm. Math. Phys 2016

Lemma

ν^{*d} is ε-approximate k-design in depth

$$d \geq \frac{1}{\Delta_k}(2nk + \log(1/\varepsilon))$$

History of spectral gap estimates

Random reversible circuits (3-local all-to-all):

- Gowers 1996: $\Delta_k = \mathrm{poly}^{-1}(nk) \implies$ Approximate permutation designs in depth $\mathrm{poly}(nk)(2nk + \log(1/\varepsilon))$.
- Hoory, Magen, Myers, Rackoff: $\Delta_k = \Omega(n^{-3}k^{-3})$
- Brodsky, Hoory : $\Delta_k = \Omega(n^{-2}k^{-1})$
- He and O'Donnell: $\Delta_k = \tilde{\Omega}(n^{-1}k^{-1})$

History of spectral gap estimates

Random reversible circuits (3-local all-to-all):

- Gowers 1996: $\Delta_k = \mathrm{poly}^{-1}(nk) \implies$ Approximate permutation designs in depth $\mathrm{poly}(nk)(2nk + \log(1/\varepsilon))$.
- Hoory, Magen, Myers, Rackoff: $\Delta_k = \Omega(n^{-3}k^{-3})$
- Brodsky, Hoory : $\Delta_k = \Omega(n^{-2}k^{-1})$
- He and O'Donnell: $\Delta_k = \tilde{\Omega}(n^{-1}k^{-1})$

Random quantum circuits (2-local all-to-all):

- Brown and Viola: First order expansion of the gap, $\Delta_k = \mathrm{const.}/n + O_k(1/n^2)$.
- Harrow and Low/Brandao, Horodecki: $\Delta_{2/3} = \Omega(1/n)$.
- Brandão, Harrow, and Horodecki: $\Delta_k = \Omega(n^{-1}k^{-10.5})$
- **H**: $\Delta_k = \Omega(n^{-1}k^{-5-o(1)})$

Other constructions of approximate designs at FOCS 2024

All presented in session 2C, 1:30-2:30pm on Monday!!!

- Haah, Liu, and Tan: $\Delta_k(\text{Pauli rotations}) = \Omega(k^{-1})$. $\implies$ multiplicative error approximate designs in (1D) depth $O(n^2 k)$.
- Chen, Docter, Xu, Bouland, Brandão, Hayden: Construction of additive error designs in depth $O(k\,\mathrm{poly}(n))$.
- Metger, Poremba, Sinha, Yuen, Additive error designs in depth $O(k\,\mathrm{poly}(n))$.

Main result: k-independent gaps

Theorem (k-independent gap)

For 3-local all-to-all random reversible and 2-local all-to-all random quantum circuits $\Delta_k = \Omega(n^{-3})$ *for all* $k \leq 2^{n/2}$.

Main result: k-independent gaps

Theorem (k-independent gap)

For 3-local all-to-all random reversible and 2-local all-to-all random quantum circuits $\Delta_k = \Omega(n^{-3})$ *for all* $k \leq 2^{n/2}$.

Theorem (Quasi-optimal gap)

For all $k \leq 2^{n/6.1}$, *we have* $\Delta_k = \tilde{\Omega}(n^{-1})$, *which is optimal (up to polylog factors) for random reversible and quantum circuits.*

Main result: k-independent gaps

Theorem (k-independent gap)

For 3-local all-to-all random reversible and 2-local all-to-all random quantum circuits $\Delta_k = \Omega(n^{-3})$ for all $k \leq 2^{n/2}$.

Theorem (Quasi-optimal gap)

For all $k \leq 2^{n/6.1}$, we have $\Delta_k = \tilde{\Omega}(n^{-1})$, which is optimal (up to polylog factors) for random reversible and quantum circuits.

Corollary (Designs in linear depth)

Random brickwork circuits form ε-approximate designs in depth $\mathrm{polylog}(k)(2nk + \log(1/\varepsilon))$.

Elements of the proof

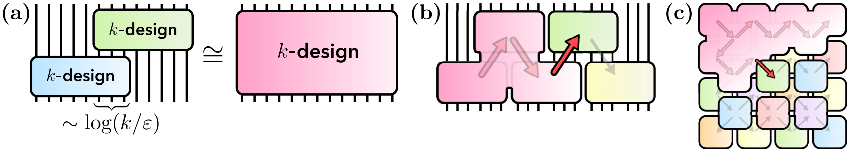
- Gap of random reversible circuits from expanding Cayley graph of symmetric group Kassabov, Inventionae 2010.
- Relate to gap of random reversible circuits via "PFC" ensemble Metger, Poremba, Sinha, Yuen, FOCS 2024:

$$\mathrm{PFC} \stackrel{\sim}{=} \underbrace{\sum_{x\in\{0,1\}^n} |\pi(x)\rangle\langle x|}_{\text{random permutation}, \pi\in S_{2^n}} \times \underbrace{\sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle\langle x|}_{\text{random phase}, f:\{0,1\}^n\to\{0,1\}} \times \underbrace{C}_{\text{random Clifford}}$$

- Approximate components by random walks in subgroups.
- Universality theorem for random quantum circuits H, Quantum 2022
- Techniques developed for frustration-free Hamiltonians: Detectability lemma and quantum union bound.

Part IV. Random unitaries in extremely low depth
(What the spectral gap can't see)

Random unitaries from gluing



Theorem

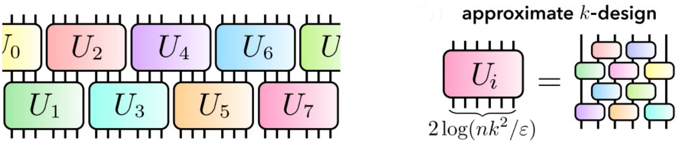
The product of two k-designs overlapping on $\xi \geq \log_2(nk/\varepsilon)$ qubits form ε-approximate unitary design on the full space.

Approximate designs from gluing

- Use random quantum circuits in the blocks.
- Plug in $\mathrm{polylog}(k)(2nk + \log(1/\varepsilon))$

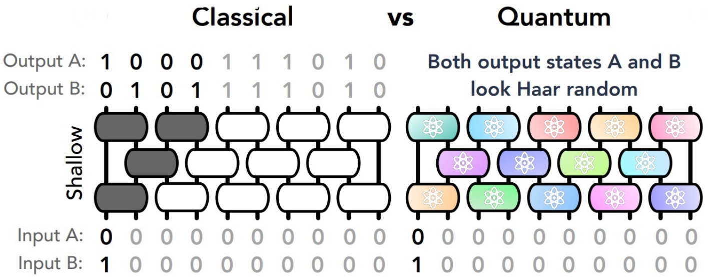
Theorem

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



Chen, Haah, H, Liu, Metger, Tan, preprint 2024

How about classical circuits



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

Optimality of our results

Theorem

$\frac{1}{2}$-approximate 2-designs require $\Omega(\log(n))$ depth.

- Lower bound on anticoncentration in any basis.

Theorem

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

- 1D quantum circuits of depth $O(\log(n))$ can be efficiently learned. Huang, Liu, Broughton, Kim, Anshu, Landau, McClean, STOC 2023

PRUs from gluing

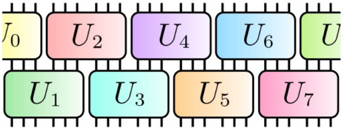
Use "PFC" in the blocks:

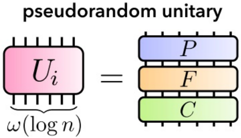
Theorem

If quantum secure one-way functions exist, PFC is a PRU. The depth of PFC is $\mathrm{poly}(n)$.

Theorem

PRU's can be generated in depth $\mathrm{polylog}(n)$ *on any geometry, including a 1D line.*





How to prove the gluing lemma?

Lemma (Unitary designs from EPR states)

A random unitary ensemble $\mathcal{E}$ forms an ε-approximate unitary k-design with error

$$\varepsilon = \frac{4^{nk}}{k!} \cdot \left(1 + \frac{k^2}{2^{n+1}}\right) \cdot \left\| \left[(\Phi_{\mathcal{E}} - \Phi_H) \otimes \mathbb{1}\right](P^{\mathrm{EPR}}) \right\|_\infty .$$

How to prove the gluing lemma?

Lemma (Unitary designs from EPR states)

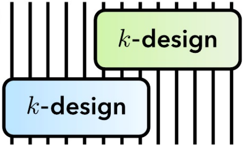
A random unitary ensemble $\mathcal{E}$ forms an ε-approximate unitary k-design with error

$$\varepsilon = \frac{4^{nk}}{k!} \cdot \left(1 + \frac{k^2}{2^{n+1}}\right) \cdot \left\| \left[(\Phi_{\mathcal{E}} - \Phi_H) \otimes \mathbb{1}\right](P^{\mathrm{EPR}}) \right\|_{\infty}.$$

- CP ordering $A \preceq B$ iff $A \otimes \mathbb{1}(P^{\mathrm{EPR}}) \leq B \otimes \mathbb{1}(P^{\mathrm{EPR}})$.
- Analyse spectrum of Choi states.

Brandão, Harrow, Horodecki, Comm. Math. Phys. 2016

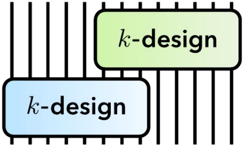
Weingarten and permutations



- Expand blocks in permutations:

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

Weingarten and permutations



- 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

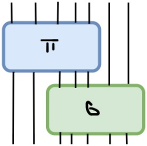
Proof sketch

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

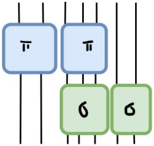
Proof sketch

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

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



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

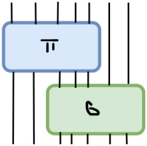


.

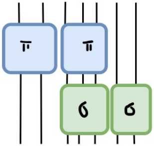
Proof sketch

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

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



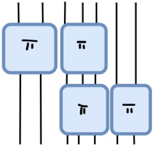
$$= \sum_{\pi,\sigma\in S_k}$$



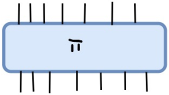
.

- Use approximate orthogonality again:

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



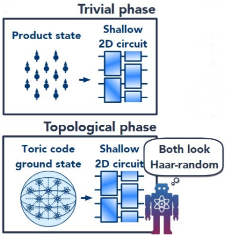
$$= \sum_{\pi\in S_k}$$



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

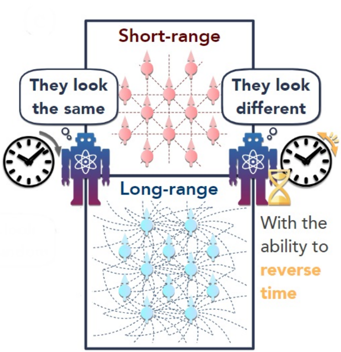
V. Applications

Hardness of quantum learning



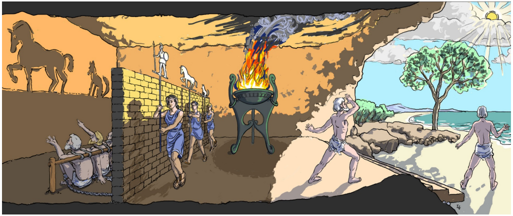
- Hard to distinguish trivial order and toric code after appyling PRU.
- Topological order up to circuits of subextensive depth.
- Distinguishing random pure states from maximally mixed using single copy measurements. Chen, Cotler, Huang, and Li, FOCS 2022

Power of time-reversal in quantum learning



- Distinguish 2D local circuit U_{2D} from U'_{2D} augmented with a long range interaction $e^{i\phi Z_i Z_j}$.
- Time-reversal allows to "see lightcones".

Shallow shadows

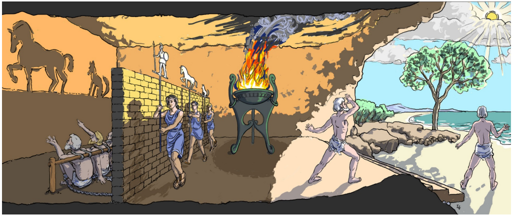


Corollary

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

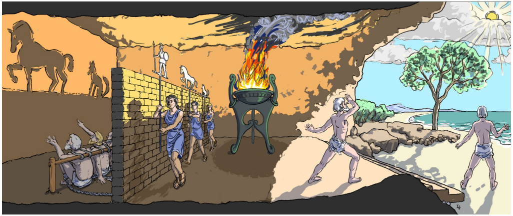


Corollary

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.*

Shallow shadows



Corollary

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.*
- *Sufficient for fidelity estimation.*

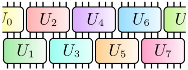
Outlook

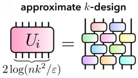
Summary

- Optimal k-dependence for random reversible and random quantum circuits: resolved conjectures from 1996 and 2009.
- Also resolved robust Brown-Susskind conjecture.
- Log-depth convergence for random quantum circuits.
- Plenty of hardness results for learning.

Open problems

- Log-depth random quantum circuits with iid gates!
- Is the optimal scaling $\log(n) + k$ for approximate designs?
- Are random quantum circuits with iid gates PRU's?





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 $\frac{1}{2} + \mathrm{Tr}[\mathrm{Tr}_A(|\psi\rangle\langle\psi|)^2]$.