Quantum Pseudorandomness and Classical Complexity

July 15, 2021

William Kretschmer

arXiv:2103.09320

Introduction

Pseudorandom States (PRSs):

“Computational approx. to Haar measure”

Pseudorandom States (PRSs):

"Computational approx. to Haar measure"

Question

Where do PRSs fit in the complexity landscape?

- Cryptography

- Cryptography
- Physical simulation

- Cryptography
- Physical simulation
- AdS/CFT

Definition (Ji, Liu, Song 2018)

$\{|\varphi_k\rangle\}_{k\in\{0,1\}^n}$ is *pseudorandom* if:

- Efficient generation of $|\varphi_k\rangle$ given $k \in \{0,1\}^n$
- For all poly-time $\mathcal{A}$ and any $T = \text{poly}(n)$:

$$\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{A}\left(|\varphi_k\rangle^{\otimes T}\right) = 1\right] - \Pr_{|\psi\rangle\leftarrow\mu_{\text{Haar}}}\left[\mathcal{A}\left(|\psi\rangle^{\otimes T}\right) = 1\right] \leq \text{negl}(n)$$

Theorem (Ji, Liu, Song 2018)

If quantum-secure OWFs exist, then pseudorandom states exist.

Theorem (Ji, Liu, Song 2018)

If quantum-secure OWFs exist, then pseudorandom states exist.

$$\text{PRSs} \Rightarrow \text{???}$$

"QMA" protocol to break PRSs

Suppose Arthur has $|\psi\rangle^{\otimes T}$

- Merlin: send quantum circuit C
- Arthur: check that $C|0^n\rangle \approx |\psi\rangle$ using swap test

"QMA" protocol to break PRSs

Suppose Arthur has $|\psi\rangle^{\otimes T}$

- Merlin: send quantum circuit C
- Arthur: check that $C|0^n\rangle \approx |\psi\rangle$ using swap test

PROBLEM

Not a QMA ***language***! Input $|\psi\rangle^{\otimes T}$ a quantum state, not a string in $\{0,1\}^n$.

Results

Theorem (This work)

There exists a quantum oracle $\mathcal{O}$ such that:

1. $\mathsf{BQP}^{\mathcal{O}} = \mathsf{QMA}^{\mathcal{O}}$, *and*
2. *PRSs exist relative to $\mathcal{O}$.*

Theorem (This work)

There exists a quantum oracle $\mathcal{O}$ such that:

1. $\mathsf{BQP}^{\mathcal{O}} = \mathsf{QMA}^{\mathcal{O}}$, *and*
2. *PRSs exist relative to* $\mathcal{O}$.

Theorem (This work)

If $\mathsf{BQP} = \mathsf{PP}$, *then PRSs do not exist.*

Shadow Tomography [Aaronson 2018]

Given:

- Binary observables $O_1, \dots, O_M$
- Copies of n-qubit state ρ

Goal: estimate $\mathrm{Tr}(O_i \rho)$ up to $\pm\varepsilon$ for all $i \in [M]$.

Shadow Tomography [Aaronson 2018]

Given:

- Binary observables $O_1, \ldots, O_M$
- Copies of n-qubit state ρ

Goal: estimate $\mathrm{Tr}(O_i \rho)$ up to $\pm\varepsilon$ for all $i \in [M]$.

Sample efficient: poly$(n, \log M, \varepsilon)$

Shadow Tomography [Aaronson 2018]

Given:

- Binary observables $O_1, \ldots, O_M$
- Copies of n-qubit state ρ

Goal: estimate $\mathrm{Tr}(O_i \rho)$ up to $\pm\varepsilon$ for all $i \in [M]$.

Sample efficient: poly$(n, \log M, \varepsilon)$

Time efficient?

Hyperefficient Shadow Tomography

Given:

- Oracle that takes $i \in [M]$ and measures O_i
- Copies of n-qubit state ρ

Goal: output C s.t. $C(i) = \mathrm{Tr}(O_i \rho) \pm \varepsilon$ for all $i \in [M]$.

Hyperefficient Shadow Tomography

Given:

- Oracle that takes $i \in [M]$ and measures O_i
- Copies of n-qubit state ρ

Goal: output C s.t. $C(i) = \mathrm{Tr}(O_i \rho) \pm \varepsilon$ for all $i \in [M]$.

Impossible efficiently

(in time $\mathrm{poly}(n, \log M, \varepsilon)$)

H.S.T. *with State Preparation*

Given:

- Oracle that takes $i \in [M]$ and produces $|\psi_i\rangle$
- Copies of n-qubit state ρ

Goal: output C s.t. $C(i) = \langle\psi_i|\rho|\psi_i\rangle \pm \varepsilon$ for all $i \in [M]$.

H.S.T. *with State Preparation*

Given:

- Oracle that takes $i \in [M]$ and produces $|\psi_i\rangle$
- Copies of n-qubit state ρ

Goal: output C s.t. $C(i) = \langle\psi_i|\rho|\psi_i\rangle \pm \varepsilon$ for all $i \in [M]$.

Still impossible efficiently

H.S.T. *with State Preparation*

Given:

- Oracle that takes $i \in [M]$ and produces $|\psi_i\rangle$
- Copies of n-qubit state ρ

Goal: output C s.t. $C(i) = \langle\psi_i|\rho|\psi_i\rangle \pm \varepsilon$ for all $i \in [M]$.

***Still* impossible efficiently**

Proof: otherwise, we would have a black box QMA reduction for breaking PRSs! □

Haar-random oracle:

$$\mathcal{U} = \{\mathcal{U}_x \leftarrow \mathbb{U}(2^{|x|})\}_{x \in \{0,1\}^*}$$

Haar-random oracle:

$$\mathcal{U} = \{\mathcal{U}_x \leftarrow \mathbb{U}(2^{|x|})\}_{x \in \{0,1\}^*}$$

Theorem (This work)

If $\mathsf{BQP}^{\mathcal{U}} \neq \mathsf{QMA}^{\mathcal{U}}$, *then* $\mathsf{BQP} \neq \mathsf{QMA}$

Proof Techniques

$$\mathcal{O} = (\mathcal{U}, \mathcal{P})$$

- $\mathcal{U}$: collection of Haar-random unitaries
- $\mathcal{P}$: PSPACE-complete language

$$\mathcal{O} = (\mathcal{U}, \mathcal{P})$$

- $\mathcal{U}$: collection of Haar-random unitaries
- $\mathcal{P}$: PSPACE-complete language

Proof idea: QMA algorithm can't learn any nontrivial property of $\mathcal{U}$, by concentration of Haar measure

$$\mathcal{O} = (\mathcal{U}, \mathcal{P})$$

- $\mathcal{U}$: collection of Haar-random unitaries
- $\mathcal{P}$: PSPACE-complete language

Proof idea: QMA algorithm can't learn any nontrivial property of $\mathcal{U}$, by concentration of Haar measure

PRSs exist relative to $\mathcal{U}$ by BBBV, and $\mathcal{P}$ doesn't help

Classical shadows

[Huang, Kueng, Preskill 2020]

$+$

Postselection

[Aaronson 2005]

Open Problems

Classical oracles?

Classical oracles?

Other evidence for PRSs?

Classical oracles?

Other evidence for PRSs?

Quantum **meta-complexity?**

William Kretschmer

https://www.cs.utexas.edu/~kretsch/

kretsch@cs.utexas.edu

The University of Texas at Austin
Computer Science

Lemma

Suppose that $f : \mathbb{U}(N)^{\oplus k} \to \mathbb{R}$ is T-Lipschitz in the Frobenius norm. Then for every $x > 0$:

$$\Pr_{U \leftarrow \mu_{\text{Haar}}}\left[f(U) \geq \mathop{\mathrm{E}}_{V \leftarrow \mu_{\text{Haar}}}[f(V)] + x\right] \leq \exp\left(-\frac{(N-2)x^2}{24T^2}\right).$$

Lemma

Suppose that $f : \mathbb{U}(N)^{\oplus k} \to \mathbb{R}$ *is* T*-Lipschitz in the Frobenius norm. Then for every* $x > 0$*:*

$$\Pr_{U \leftarrow \mu_{\text{Haar}}}\left[f(U) \geq \mathop{\mathrm{E}}_{V \leftarrow \mu_{\text{Haar}}}[f(V)] + x\right] \leq \exp\left(-\frac{(N-2)x^2}{24T^2}\right).$$

$N = 2^n$, where $n =$ # qubits

Lemma

Suppose that $f : \mathbb{U}(N)^{\oplus k} \to \mathbb{R}$ is T-Lipschitz in the Frobenius norm. Then for every $x > 0$:

$$\Pr_{U \leftarrow \mu_{\mathrm{Haar}}}\left[f(U) \geq \mathop{\mathrm{E}}_{V \leftarrow \mu_{\mathrm{Haar}}}[f(V)] + x\right] \leq \exp\left(-\frac{(N-2)x^2}{24T^2}\right).$$

$$N = 2^n, \text{ where } n = \# \text{ qubits}$$

$$f(U) = \max_{|\psi\rangle}\left\{\Pr\left[\mathcal{A}^U(|\psi\rangle)\right] = 1\right\}$$

Lemma

Suppose that $f : \mathbb{U}(N)^{\oplus k} \to \mathbb{R}$ *is* T*-Lipschitz in the Frobenius norm. Then for every* $x > 0$*:*

$$\Pr_{U \leftarrow \mu_{\text{Haar}}} \left[f(U) \geq \mathop{\mathrm{E}}_{V \leftarrow \mu_{\text{Haar}}} [f(V)] + x \right] \leq \exp\left(-\frac{(N-2)x^2}{24T^2} \right).$$

$$\begin{aligned} N &= 2^n, \text{ where } n = \#\,\text{qubits} \\ f(U) &= \max_{|\psi\rangle} \left\{ \Pr\left[\mathcal{A}^U(|\psi\rangle) \right] = 1 \right\} \\ T &= \#\,\text{queries to } U \end{aligned}$$