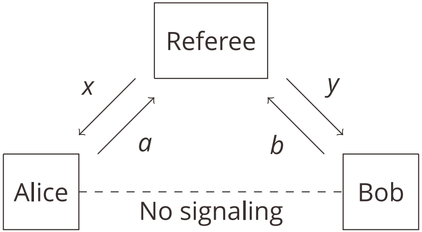
The Quantum Supremacy Tsirelson Inequality

QIP 2021

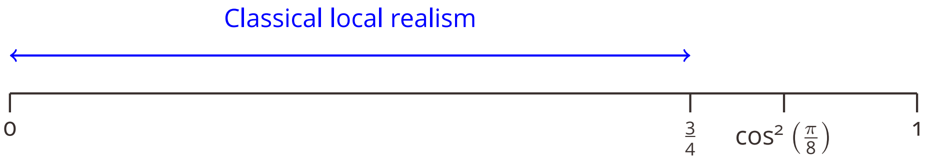
William Kretschmer

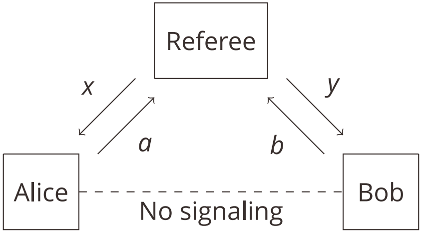
arXiv:2008.08721



CHSH game: output a, b such that $a \oplus b = xy$.

Bell inequality: $\Pr[a \oplus b = xy] \leq \frac{3}{4}$

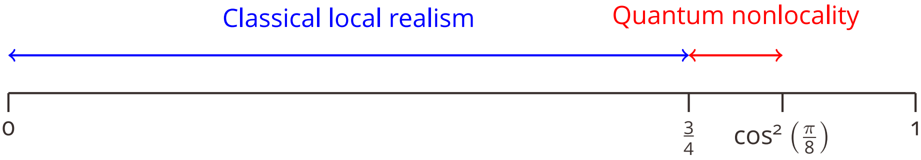


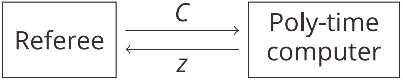


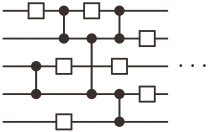
CHSH game: output a, b such that $a \oplus b = xy$.

Bell inequality: $\Pr[a \oplus b = xy] \leq \frac{3}{4}$

Tsirelson inequality: $\Pr[a \oplus b = xy] \leq \cos^2\left(\frac{\pi}{8}\right)$

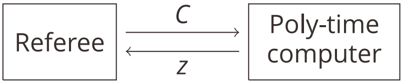


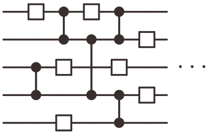


$C =$ 

XHOG task: output $z \in \{0,1\}^n$ such that $|\langle z|C|0^n\rangle|^2$ is large.

“Bell” inequality: $\mathbb{E}\left[|\langle z|C|0^n\rangle|^2\right] \leq \frac{1}{2^n}$

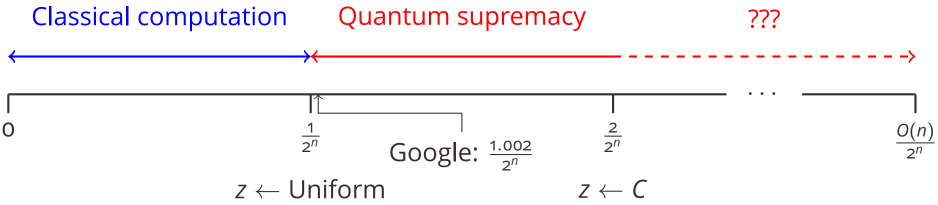


$C =$ 

XHOG task: output $z \in \{0,1\}^n$ such that $|\langle z|C|0^n\rangle|^2$ is large.

"Bell" inequality: $\mathbb{E}\left[|\langle z|C|0^n\rangle|^2\right] \leq \frac{1}{2^n}$

"Tsirelson" inequality: $\mathbb{E}\left[|\langle z|C|0^n\rangle|^2\right] \overset{?}{\leq} \frac{b}{2^n}$



Theorem (This work)

Let C be a Haar-random n-qubit unitary. Let $\varepsilon \geq \frac{1}{\mathrm{poly}(n)}$. *Then any quantum algorithm that outputs a string z such that* $\mathrm{E}\left[|\langle z|C|0^n\rangle|^2\right] \geq \frac{2+\varepsilon}{2^n}$ *requires* $\Omega\left(\frac{2^{n/4}}{\mathrm{poly}(n)}\right)$ *queries to C.*

Theorem (This work)

Let C be a Haar-random n-qubit unitary. Let $\varepsilon \geq \frac{1}{\mathrm{poly}(n)}$. *Then any quantum algorithm that outputs a string z such that* $\mathrm{E}\left[|\langle z|C|0^n\rangle|^2\right] \geq \frac{2+\varepsilon}{2^n}$ *requires* $\Omega\left(\frac{2^{n/4}}{\mathrm{poly}(n)}\right)$ *queries to C.*

+ Similar results for other oracles.

Theorem (This work)

Let C be a Haar-random n-qubit unitary. Let $\varepsilon \geq \frac{1}{\mathrm{poly}(n)}$. *Then any quantum algorithm that outputs a string z such that* $\mathrm{E}\left[|\langle z|C|0^n\rangle|^2\right] \geq \frac{2+\varepsilon}{2^n}$ *requires* $\Omega\left(\frac{2^{n/4}}{\mathrm{poly}(n)}\right)$ *queries to C.*

+ Similar results for other oracles.
+ $O\left(2^{n/3}\right)$ upper bound, by collision finding.

- Real-world relevance

- Real-world relevance
- Random unitary oracles

- Real-world relevance
- Random unitary oracles
- Not a decision problem

- Real-world relevance
- Random unitary oracles
- Not a decision problem
- Needs new tools

Canonical

$$\mathcal{U}|\bot\rangle = |\psi\rangle$$
$$\mathcal{U}|\psi\rangle = |\bot\rangle$$
$$\mathcal{U}|\varphi\rangle = |\varphi\rangle$$

Random

$$\mathcal{V} = \begin{bmatrix} | & ? & ? \\ |\psi\rangle & ? & ? \\ | & ? & ? \end{bmatrix}$$

Canonical **Random**

$$\mathcal{U}|\bot\rangle = |\psi\rangle$$
$$\mathcal{U}|\psi\rangle = |\bot\rangle \iff \mathcal{V} = \begin{bmatrix} | & ? & ? \\ |\psi\rangle & ? & ? \\ | & ? & ? \end{bmatrix}$$
$$\mathcal{U}|\varphi\rangle = |\varphi\rangle$$

Theorem (Ambainis-Rosmanis-Unruh 2014)

T queries to $\mathcal{U}$ can be simulated with a "resource state":

$$|R\rangle := \bigotimes_{j=1}^{k} \alpha_j|\psi\rangle + \beta_j|\perp\rangle$$

where $k \sim T^2$.

$\implies$ Consider algorithms that just have copies of $|\psi\rangle$

$\implies$ Easy lower bound, by symmetry

Tighter bounds? Between $2^{n/4}$ and $2^{n/3}$

Tighter bounds? Between $2^{n/4}$ and $2^{n/3}$

Stronger evidence of **real-world** hardness?

Tighter bounds? Between $2^{n/4}$ and $2^{n/3}$

Stronger evidence of **real-world** hardness?

Computational **pseudorandomness** of random quantum circuits?

William Kretschmer
https://www.cs.utexas.edu/~kretsch/
kretsch@cs.utexas.edu

The University of Texas at Austin
Computer Science