# Refuting XQUATH at Sublinear Depth

CMSC 39100: Physics of Computation

Aditya Bhardwaj

May 2023

# Where we left off

- Sampling from the output distribution of a randomly generated quantum circuit $C$

**Question: Why did we think this was classically hard?**

- Quantum Approximate Counting vs. Classical Approximate Counting
- Proved that $\mathtt{sampBPP} = \mathtt{sampBQP} \implies \mathtt{PH}$ collapses

# Some intuition for PH

- Consider 3-SAT.
$$(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6)$$
Is there $n$-bit string $x = x_1 x_2 \cdots x_n$ that satisfies all the clauses?
- Input $c$ and $n$-bit string $x$
$$\mathrm{Check}(c, w) = \begin{cases} 1 & x \text{ satisfies } c \\ 0 & x \text{ doesn't satisfy } c \end{cases}$$
- Problem in $\mathtt{NP}$: Given $c$, decide if there exists $x$ such that $\mathrm{Check}(c, x) = 1$?

# Some intuition for $\texttt{PH}$

- Level 0: $\texttt{P}$
- Level 1: $\texttt{NP}$
  - True? There exists $x$ such that $\text{Check}(c, x) = 1$
- Level 2: $\texttt{NP}^{\texttt{NP}}$
  - clauses acting on two $n$-bit strings $x^{(1)}$ and $x^{(2)}$
  - $\text{Check}\left(c, x^{(1)}, x^{(2)}\right) = \begin{cases} 1 & x^{(1)}, x^{(2)} \text{ satisfies } c \\ 0 & x^{(1)}, x^{(2)} \text{ doesn't satisfy } c \end{cases}$
  - True? For all $x^{(1)}$, there exists $x^{(2)}$ such that $\text{Check}\left(c, x^{(1)}, x^{(2)}\right) = 1$
- Level 3: $\texttt{NP}^{\texttt{NP}^{\texttt{NP}}}$
  - True? There exists $x^{(1)}$ such that for all $x^{(2)}$ there exists $x^{(3)}$ such that $\text{Check}\left(c, x^{(1)}, x^{(2)}, x^{(3)}\right) = 1$

$$\vdots$$

$$\subseteq \texttt{PSPACE}$$

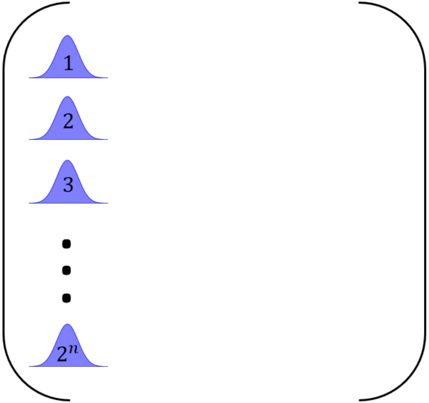
# What does the distribution look like?

Circuit roughly implements a Haar random unitary on $n$ qubits.

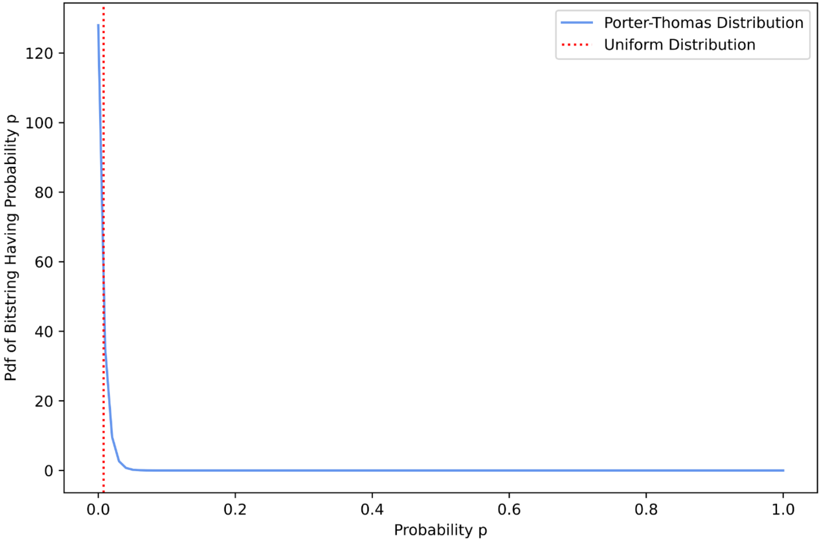
Output probabilities follow Porter-Thomas distribution $|\langle x|C|0^n\rangle|^2 = p(x) \sim 2^n e^{-2^n p}$

But there is noise! $\implies$ $0.998U + 0.002D$

arxiv: quant-ph/2007.07872



# Porter-Thomas Distribution



# How do we check?

Sears Tower view:

1. Generate random quantum circuit $C$
2. Get $k$ samples from the distribution induced by $C|0^n\rangle$
3. Perform some statistical test on the samples
   - fidelity, KL-divergence, total variation distance, etc. not good
4. Claim it is hard for a classical algorithm to pass the test.

# Consider easier problem [Aaronson & Chen '17]

**Definition**

Given $C$, the $n$-bit string outcome $x$ is *heavy* if $p(x) = |\langle x|C|0^n\rangle|^2$ is greater than the median probability in the output distribution of $C$

**Problem: Heavy Output Generation (HOG)**

Given random quantum circuit $C$, generate output $n$-bit strings $x_1, x_2, \ldots, x_k$ such that at least $2/3$ of them are heavy.

$p_z$

Heavy $p_y$

$\vdots$

Median

$\vdots$

Light $p_b$

$p_a$

# HOG

**Problem: Heavy Output Generation (HOG)**

Given random quantum circuit $C$, generate output $n$-bit strings $x_1, x_2, \ldots, x_k$ such that at least $2/3$ of them are heavy.

- Easy to solve HOG quantumly. Why?
    1. sum of probabilities above median is $\geq 0.7$ whp over $C$.
        - relies on Porter-Thomas
    2. then can use Chernoff bound to show $> 2/3$
    3. Rigorous statement: Quantum algorithm succeeds at HOG with probability $1 - \exp(-\Omega(k))$.
- What about classically?

# QUATH

**Quantum Threshold Assumption (QUATH)**

No poly-time classical algorithm that takes as input a random quantum circuit $C$ with $m \gg n$ gates and decides whether $0^n$ is heavy with success probability $1/2 + \Omega\left(\frac{1}{2^n}\right)$.

- Why $\Omega\left(\frac{1}{2^n}\right)$?
  1. can already get $\Omega\left(\frac{1}{2^m}\right)$ with a Feynman type algorithm
  2. How would we solve QUATH quantumly?
     - Just repeatedly run $C$ and measure to get a list of strings $2/3$ of which are heavy. If $0^n$ is on the list, then say its heavy.

# QUATH $\implies$ HOG is hard

**Proof Idea:** Prove contrapositive. Suppose there exists classical algorithm $\mathcal{A}$ that can solve HOG. Use intuition of how we solved QUATH quantumly.

**Details:**

1. Let's not treat $0^n$ like its special.
   - Instead draw a uniform random string $z \in \{0,1\}^n$.
   - At end of $C$, apply $X$ gate for each $i$ where $z_i = 1$. Call this $C'$.
   - $\langle z|C'|0^n\rangle = \langle 0^n|C|0^n\rangle$
2. Use $\mathcal{A}$ on $C'$ to get $z_1, \ldots, z_k$, 2/3 of which are heavy
3. Pick $z_{i^*}$ uniformly at random from $z_1, \ldots, z_k$.
   3.1 If $z = z_{i^*} \rightarrow$ output heavy
   3.2 Else, coin toss to output heavy or light
4. Then we correctly decide if $z$ is heavy for $C'$ with probability

$$\Pr[z = z_{i^*}] \cdot \frac{2}{3} + \Pr[z \neq z_{i^*}] \cdot \frac{1}{2} = 2^{-n} \cdot \frac{2}{3} + (1 - 2^{-n}) \cdot \frac{1}{2} = \frac{1}{2} + \Omega(2^{-n})$$

# Linear Cross-Entropy Benchmark (XEB)

**Notation:** $p_C(x)$ = ideal distribution and $q_C(x)$ = experimental distribution

**KL-divergence** $D_{KL}(q \parallel p) = \sum_x q(x) \log\left(\frac{q(x)}{p(x)}\right) = H(q,p) - H(q)$

**cross-entropy** $H(q,p) = -\sum_x q(x) \log(p(x))$

**linear cross-entropy** $\chi_C(q) = 2^n \sum_x q_C(x) p_C(x) - 1 = 2^n \sum_x \langle p_C(x) \rangle_{q_C} - 1$

- sample efficient: $\frac{2^n}{k} \sum_{i=1}^{k} p_C(x_i) - 1$
- lowest variance
- average XEB $\langle \chi_C(q) \rangle_C$ over $C_1, C_2, \ldots, C_K$
  - Google experiment: $K = 10$, $k = 7 \times 10^6$

# XHOG [Aaronson & Gunn '19]

**Problem: XHOG, or Linear Cross-Entropy Heavy Output Generation**

Given circuit $C$, generate $k$ distinct samples $x_1, \ldots, x_k$ such that

$$\mathbb{E}_i[|\langle x_i|C|0^n\rangle|^2] \geq \frac{b}{2^n}.$$

- $1 < b \leq 2$
- $b = 2$ with noiseless $C$
- e.g. Google noisy experiment $b = 1.002$
- generate outputs that have high probabilities

# XQUATH [Aaronson and Gunn '19]

**Assumption: XQUATH, or Linear Cross-Entropy Quantum Threshold Assumption**

No poly-time classical algorithm that that given random $C$ produces an estimate $\tilde{p}$ to $p_0 \equiv |\langle 0^n|C|0^n\rangle|^2$ such that

$$\text{XScore} = 2^{2n} \cdot \mathbb{E}_C\left[\left(p_0 - \frac{1}{2^n}\right)^2 - (p_0 - \tilde{p})^2\right] = \Omega(2^{-n})$$

- can't do slightly better in **mean squared error** than trivial algorithm
- Feynman algorithm cannot refute XQUATH if $m \gg 3n$ like in Google experiment

# XQUATH $\implies$ XHOG is hard

**Assumption: XQUATH, or Linear Cross-Entropy Quantum Threshold Assumption**

No poly-time classical algorithm that given random $C$ produces an estimate $\tilde{p}$ to $p_0 \equiv |\langle 0^n|C|0^n\rangle|^2$ such that

$$\text{XScore} = 2^{2n} \cdot \mathbb{E}_C\left[\left(p_0 - \frac{1}{2^n}\right)^2 - (p_0 - \tilde{p})^2\right] = \Omega(2^{-n})$$

XHOG is hard assuming XQUATH by similar proof as HOG and QUATH

- Proof sketch:
    1. Assume there is classical algorithm that solves XHOG so that you can get samples $x_1, \ldots, x_k$ so that $\mathbb{E}_i[|\langle x_i|C|0^n\rangle|^2] \geq \frac{b}{2^n}$.
    2. Then output $\frac{b}{2^n}$ if $0^n$ on the list and $\frac{1}{2^n}$ otherwise.

# Refuting XQUATH [Gao et. al '21] [Aharonov et. al '22]

**Recall:** Intuition for XQUATH (advantage scales like $2^{-n}$) came from path integral. Let $C = U_d U_{d-1} \cdots U_1$, then

$$\langle 0^n | C | 0^n \rangle = \sum_{x_1,\ldots,x_{d-1} \in \{0,1\}^n} \langle 0^n | U_d | x_{d-1} \rangle \langle x_{d-1} | U_{d-1} | x_{d-2} \rangle \cdots \langle x_2 | U_2 | x_1 \rangle \langle x_1 | U_1 | 0^n \rangle.$$

Roughly $2^{nd}$ paths of equal weight on average, so seems like advantage can only be $\mathrm{poly}(nd) 2^{-nd}$.

**Idea:** We can do better by using a different basis!

# Pauli Basis Path Integral

Instead of kets use density matrices.

$$P_n = \left\{ \frac{I}{\sqrt{2}}, \frac{X}{\sqrt{2}}, \frac{Y}{\sqrt{2}}, \frac{Z}{\sqrt{2}} \right\}^{\otimes n}$$

| | (a) Vector basis | (b) Operator basis |
|---|---|---|
| State | $\lvert\psi\rangle = \sum_{x\in\{0,1\}^n} \langle x\vert\psi\rangle \lvert x\rangle$ | $\rho = \sum_{s\in\mathsf{P}_n} \mathrm{Tr}(s\rho)s$ |
| Evolution | $\lvert\psi\rangle \mapsto U\lvert\psi\rangle$ | $\rho \mapsto U\rho U^\dagger$ |
| Path integral | $\langle x\vert U\vert\psi\rangle$ $= \sum_{y\in\{0,1\}^n} \langle x\vert U\vert y\rangle \langle y\vert\psi\rangle$ | $\mathrm{Tr}\left(sU\rho U^\dagger\right)$ $= \sum_{t\in\mathsf{P}_n} \mathrm{Tr}\left(sUtU^\dagger\right)\mathrm{Tr}(t\rho)$ |

Aharonov et. al '22

Natural when you are looking at depolarizing noise.

# Probabilities with Pauli

Let $C = U_d U_{d-1} \cdots U_1$. Then

$$
\begin{aligned}
p_x &= |\langle x| C |0^n\rangle|^2 \\
&= \mathrm{Tr}\left( |x\rangle\langle x| C |0^n\rangle\langle 0^n| C^\dagger \right) \\
&= \sum_{s \in P_n^{d+1}} \mathrm{Tr}\left( |x\rangle\langle x| s_d \right) \mathrm{Tr}\left( s_d U_d s_{d-1} U_d^\dagger \right) \cdots \mathrm{Tr}\left( s_1 U_1 s_0 C_1^\dagger \right) \mathrm{Tr}\left( s_0 |0^n\rangle\langle 0^n| \right) \\
&= \sum_{s \in P_n^{d+1}} f(C, s, x)
\end{aligned}
$$

# Refuting XQUATH: A First Lemma

**Lemma 1: Orthogonality of Pauli paths**

If $C$ is a random circuit and $s \neq s' \in P_n^{d+1}$ then

$$\mathbb{E}_C \left[ f(C, s, x) f(C, s', x) \right] = 0$$

for any $x \in \{0, 1\}^n$

**Corollary**

$\mathbb{E}_C \left[ f(C, s, x) \right] = 0$ for any $s \neq I_n^{\otimes d+1}$

Proof of Corollary: $\mathbb{E}_C \left[ f(C, s, x) f(C, I_n^{\otimes d+1}, x) \right] = \frac{1}{2^n} \mathbb{E}_C [f(C, s, x)] = 0$

# Refuting XQUATH: Part 1

## Claim

For a random quantum circuit $C$, outputting $\tilde{p} = \frac{1}{2^n} + f(C, s, 0^n)$ gets you XSCORE $\frac{1}{15^d}$ where $s = \left(\frac{1}{\sqrt{2^n}} Z \otimes I^{\otimes n-1}\right)^{\otimes d+1}$.

**Proof** (Part 1):

$$
\begin{aligned}
\text{XScore} &= 2^{2n} \cdot \mathbb{E}_C \left[ \left( p_0 - \frac{1}{2^n} \right)^2 - (p_0 - \tilde{p})^2 \right] = 2^{2n} \cdot \mathbb{E}_C \left[ \frac{1}{2^{2n}} - \frac{2}{2^n} p_0 - \tilde{p}^2 + 2\tilde{p} \cdot p_0 \right] \\
&= 2^{2n} \cdot \mathbb{E}_C \left[ -\frac{1}{2^{2n}} - \tilde{p}^2 + 2\tilde{p} \cdot p_0 \right] \\
&= 2^{2n} \cdot \mathbb{E}_C \left[ -\frac{2}{2^{2n}} - f(C, s, 0^n)^2 + 2\tilde{p} \cdot p_0 \right] \\
&= 2^{2n} \cdot \mathbb{E}_C \left[ -\frac{2}{2^{2n}} - f(C, s, 0^n)^2 + 2\frac{p_0}{2^n} + 2f(C, s, 0^n)^2 \right] \\
&= 2^{2n} \cdot \mathbb{E}_C \left[ -f(C, s, 0^n)^2 + 2f(C, s, 0^n)^2 \right] = 2^{2n} \cdot \mathbb{E}_C \left[ f(C, s, 0^n)^2 \right]
\end{aligned}
$$

# Refuting XQUATH: Lemma 2

**Lemma 2: Harrow & Low '09**

For Haar random 2 qubit gate and $p, q \in P_2$

$$\mathbb{E}_C \left[ \mathrm{Tr} \left( pUqU^\dagger \right)^2 \right] = \begin{cases} 1 & \text{if } p = q = \frac{I \otimes I}{2} \\ 0 & \text{if} p = \frac{I \otimes I}{2} \text{ and } q \neq \frac{I \otimes I}{2} \text{ or vice versa} \\ \frac{1}{15} & \text{otherwise} \end{cases}$$

# Refuting XQUATH: Part 2

**Proof** (Part 2):

- Each layer $U_i$ of $C$ consists of two qubit gates $U_i^{(1)}, U_i^{(2)}, \ldots, U_i^{(n/2)}$ and $s = \left(\frac{1}{\sqrt{2^n}} Z \otimes I^{\otimes n-1}\right)^{\otimes d+1}$.

$$\text{Had XScore } = 2^{2n} \cdot \mathbb{E}_C \left[ f\left(C, s, 0^n\right)^2 \right]$$

$$= 2^{2n} \cdot \mathbb{E}_C \left[ \mathrm{Tr}\left(|x\rangle\langle x| s_d\right)^2 \cdot \mathrm{Tr}\left(s_d U_d s_{d-1} U_d^\dagger\right)^2 \cdots \mathrm{Tr}\left(s_1 U_1 s_0 U_1^\dagger\right)^2 \cdot \mathrm{Tr}\left(s_0 |0^n\rangle\langle 0^n|\right)^2 \right]$$

First and last terms cancel the $2^{2n}$ up front. Left with product of $d$ terms of the form

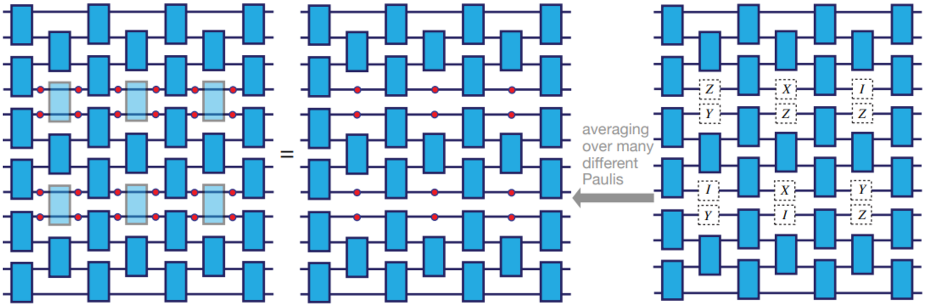
$$\mathbb{E}_{U_i} \left[ \mathrm{Tr}\left( \frac{1}{2^n} \left(Z \otimes I^{\otimes n-1}\right) U_i \left(Z \otimes I^{\otimes n-1}\right) U_i^\dagger \right)^2 \right]$$

which looks like

$$\mathbb{E}_{U_i^{(1)}} \left[ \mathrm{Tr}\left( \frac{1}{4} (Z \otimes I) U_i^{(1)} (Z \otimes I) U_i^{(1)\dagger} \right) \right] \cdot \mathbb{E}_{U_i^{(2)}} \left[ \mathrm{Tr}\left( \frac{1}{4} (I \otimes I) U_i^{(2)} (I \otimes I) U_i^{(2)\dagger} \right) \right] \cdots$$

First term gives $\frac{1}{15}$ and the rest give 1, so $\boxed{\text{XScore} = \frac{1}{15^d}}$

# Spoofing XEB [Gao et. al '21]




Spoofs XEB for 1D circuits. Scales like $\frac{2^{O(\ell)}}{\ell} nd$.

# So where do we go now?

- Is there a reduction from XQUATH to QUATH?
- Still think HOG and XHOG are hard problems. Is there some other assumption ($\frac{1}{\text{poly}}$) under which we can prove their hardness?
- Or better yet, can we let them rest on the gold standard?
- Where is the Goldilocks zone?
- Better algorithms for spoofing XEB?
- What if HOG and XHOG are actually easy?

# Other cool things to learn more about

- Understand mapping of XEB to stat mech models (diffusion reaction, Ising)
- Relationship between XEB and fidelity
- Hardness of BosonSampling

# Notes

https://arxiv.org/pdf/2007.07872.pdf
https://arxiv.org/pdf/1612.05903.pdf
https://arxiv.org/pdf/2111.03011.pdf
https://arxiv.org/pdf/2211.03999.pdf
https://arxiv.org/pdf/2111.03011.pdf