Old and New School Quantum Advantage

Angus Lowe

Background

- Quantum theory is different from classical randomness
  - Bell Non-locality ['66]
  - Superdense coding ['92]
  - Separations in communication complexity ['99]

} Proven

- In '94, Shor showed we might be able to speed up algorithms too

} Not proven

- Can we prove computational quantum advantage?

Overview

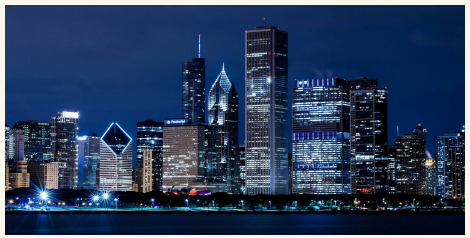
→ the chronological account

I. Paleo-advantage ['90s]

- Oracles, query complexity
- Simon's Problem
- Recent results

II. Sampling advantage ['00s]

- Complexity theory
- Hardness of exact sampling



III. Modern Advantage [Now]

- Average-case hardness, approx. sampling
- Circuit-depth separations

Quantum Theory 101

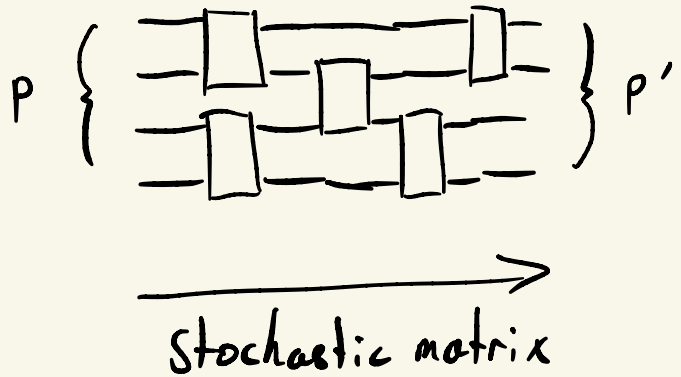
Probability

Sample space : $\Omega = \{1, \dots, d\}$.

Distribution : $p \in \mathbb{R}^d$, $p \geq 0$, $\sum_j p_j = 1$

Events : $W \subset \Omega$, $\Pr_p[W] = \sum_{j \in W} p_j$

Measurement : $\Omega = W_1 \sqcup W_2 \sqcup \dots \sqcup W_m$.

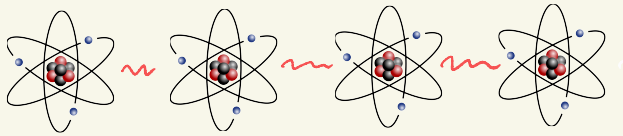


Quantum Theory 101

Quantum

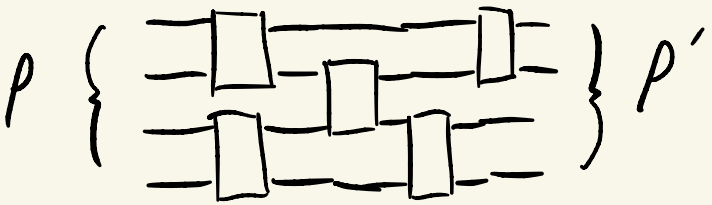
"Sample space": $\Omega = \{1, \ldots, d\}$ ← "labels for the preferred basis"

"Distribution" / "state": $\rho \in \mathbb{C}^{d \times d}, \rho \geq 0, \operatorname{tr}\rho = 1$



"Events": $W \subset \mathbb{C}^d, \Pr_\rho[W] = \operatorname{tr}\Pi_W \rho$ $(\Pi_W = \text{proj}_W)$

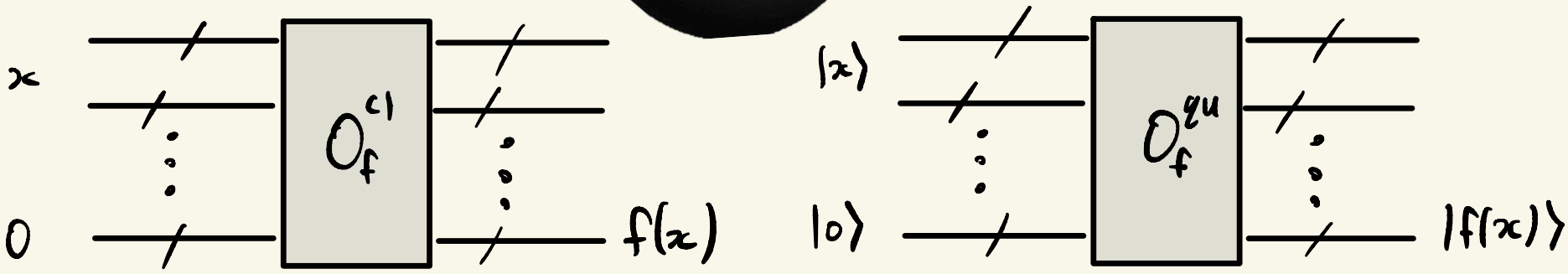
Measurement: $\mathbb{C}^d = W_1 \oplus W_2 \oplus \ldots \oplus W_m$



Unitary channel

I. Paleo-Advantage

Oracles



- Query complexity := # calls to oracle to solve problem

e.g., f is either:

Case 1. $f(x) = 0^n \quad \forall\ x \in \{0,1\}^n$

Case 2. $f(x) = 1^n \quad \forall\ x \in \{0,1\}^n$

→ decide which.

Simon's Problem

Given: Promise that $f: \{0,1\}^n \to \{0,1\}^n$, $\forall x \neq y \quad f(x) = f(y)$ iff $x = y \oplus s$ for some fixed $s \in \{0,1\}^n$.

Goal: Find s.

e.g.,

x	$f(x)$
00	11
01	01
10	11
11	01

$(s = 10)$

→ classical algorithm: i) query $f(x_1), f(x_2), \ldots, f(x_T)$.

ii) if $f(x_j) = f(x_k)$, $x_j \neq x_k$, then $s = x_j \oplus x_k$.

→ "birthday paradox" => $T \approx \sqrt{2^{n+1}}$ is enough

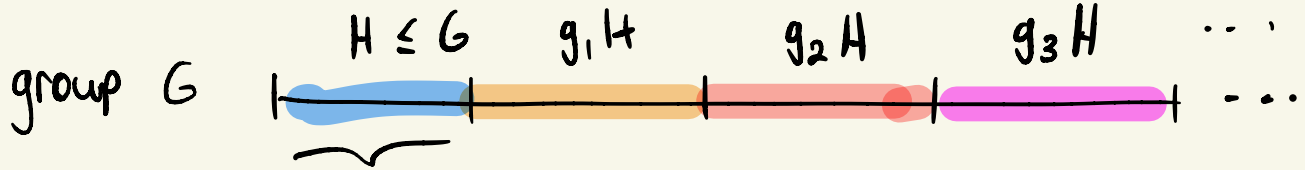
→ $T = \Omega(\sqrt{2^n})$ required, information-theoretically

Simon's Problem

Given: Promise that $f: \{0,1\}^n \to \{0,1\}^n$, $\forall x \neq y \quad f(x) = f(y)$ iff $x = y \oplus s$ for some fixed $s \in \{0,1\}^n$.

Goal: Find s.

Quantumly: Helpful to note f labels cosets.



e.g., $\{00, 10\}$ in previous slide

→ find $H \leq G$.

→ Quantum oracle gives us

$$\rho_H = \frac{1}{|G|} \sum_{h \in H} R(h)$$

reg. rep.

Reminder: trying to find $H \leq G$, e.g., $\{00, 10\}$

$$\rho_H = \frac{1}{|G|} \sum_{h \in H} R(h)$$ → reg. rep.

$$\rho_H \cong \frac{1}{|G|} \bigoplus_{\lambda \in \hat{G}} I_{d_\lambda} \otimes \sum_{h \in H} r_\lambda(h)^*$$

Rep. theory facts

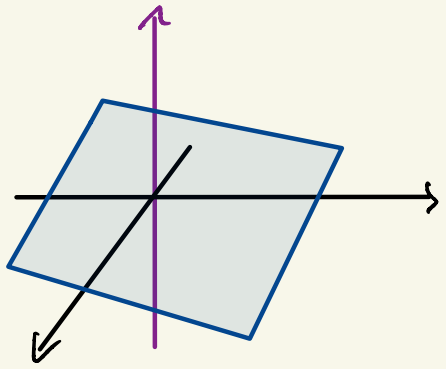
$$R(h) e_g = e_{gh^{-1}}$$

$$R(h) \cong \bigoplus_{\lambda \in \hat{G}} I_{d_\lambda} \otimes r_\lambda(h)^*$$

↳ Can I meas. in this basis?

→ $\Pr[\lambda] \propto \sum_{h \in H} \chi_\lambda(h)$

For Simon's Problem, $\lambda \in \{0,1\}^n$, $\chi_\lambda(x) = (-1)^{\lambda \cdot x}$



$\therefore$ $T = O(\log |G|) = O(\log 2^n) = O(n)$ suffices.

Other Results in Query Complexity

* • [BV '93] Quantum 1 vs. Classical $> n$

Note: '94 Shor is also! ← • [Simon '94] Quantum n vs. Classical $> 2^{n/2}$

→ How far can we push this gap?

- "t-fold forrelation problem" [AA '18],

  Quantum t vs. Classical $> 2^{n(1-\frac{1}{2t})}$

  ↳ [BS '20, SSW '20]

- Conjecture: this is optimal, i.e., classical can solve <u>any</u> t-query quantum problem using $\lesssim 2^{n(1-\frac{1}{2t})}$.

- Proven [BGGS '21].

- Non-Abelian HSP: dihedral HSP breaks lattice-based cryptography [Regev '03]

Query Complexity Advantage

Pros

- Unconditional!
- Super-exponential separations

Cons

- Oracles do not exist
- Query complexity ≠ time complexity

II. Sampling Advantage

Overview of Approach

- Proving things about time complexity is hard: can't even show $P \neq NP$

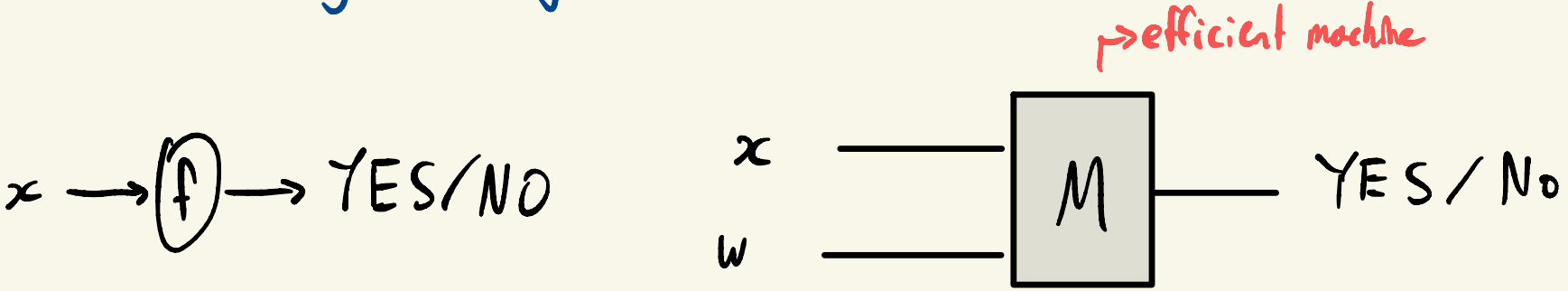
Note: does not follow from Shor, factoring not NP-hard.

- Idea: can we show quantum advantage assuming $P \neq NP$?

- Ans: not quite. But almost.

- How? Look at hardness of sampling.

Complexity Theory 101



$\Sigma_0 = P :=$ set of all f s.t. $\exists\ M_f$ computing f i.e.,

$$M_f(x) = f(x) \quad \forall x.$$

$\Sigma_1 = NP :=$ set of all f s.t. $\exists\ M_f$ verifying f i.e.,

1. if $f(x) = YES$, $M(x, w) = YES$ for some w.
2. if $f(x) = NO$, $M(x, w) = NO$ $\forall\ w$.

oracle notation ↑

$\Sigma_2 = NP^{NP} :=$ set of all f s.t. $\exists\ M_f$ verifying f given the power to ask an oracle for the values of any $g \in NP$.

Complexity Theory 101

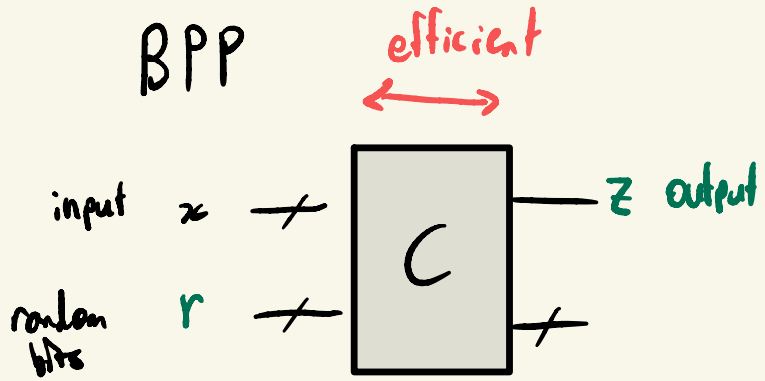
$\Sigma_k := NP^{\Sigma_{k-1}}$. "$k^{th}$ level of the polynomial hierarchy"

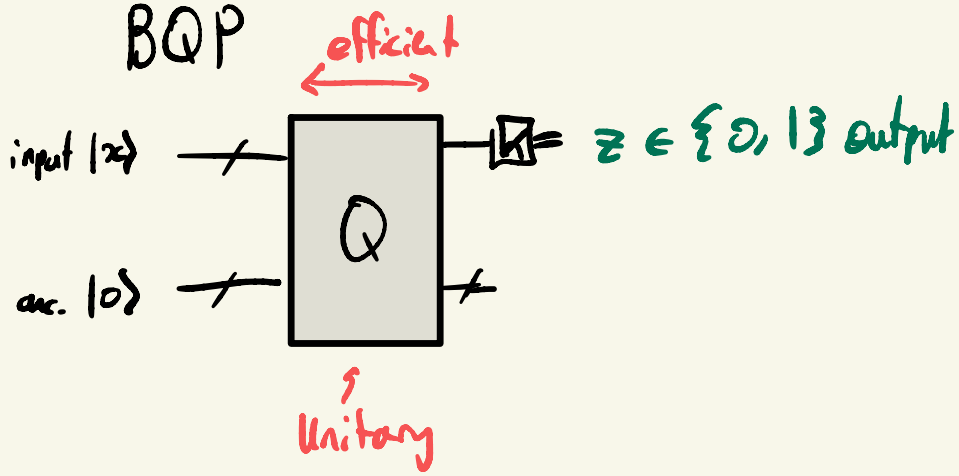
$PH := \bigcup_{k \in \mathbb{Z}_{\geq 0}} \Sigma_k$.

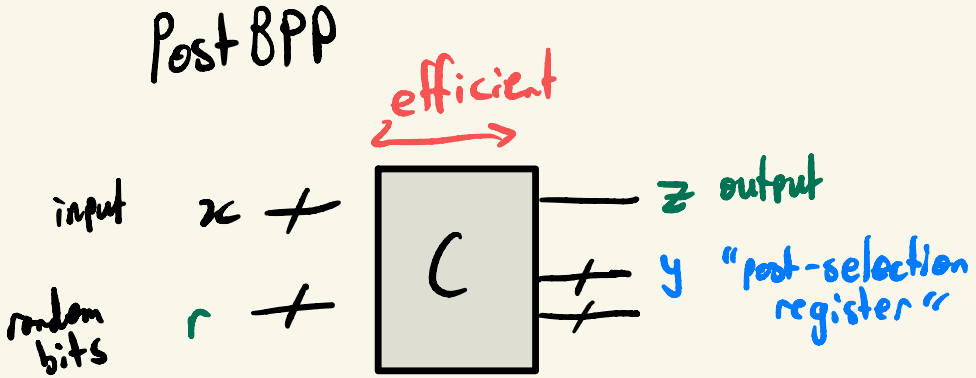
Note: if $\Sigma_j = \Sigma_{j+1}$ for some j, $PH = \Sigma_j$.

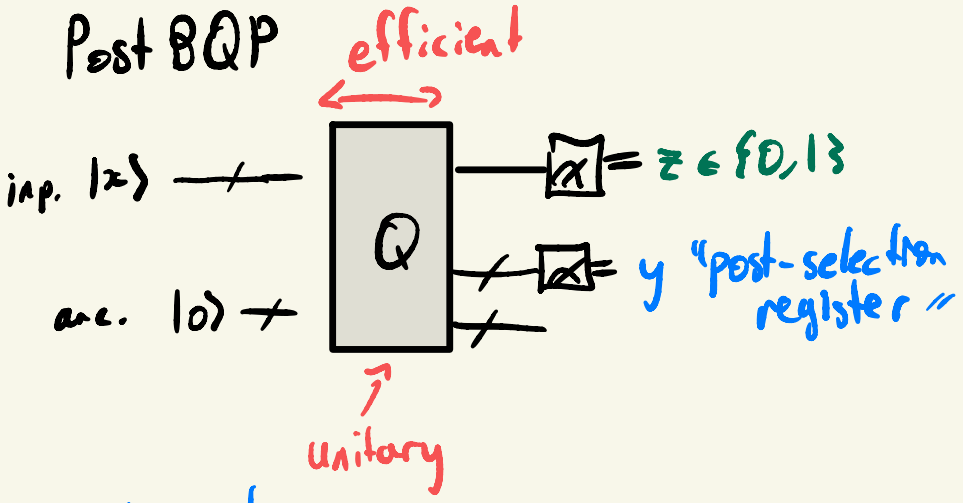
This is thought to be <u>very</u> unlikely.

Circuits







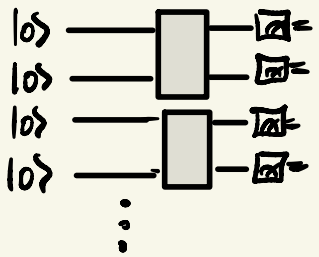


= Post-Select

How Hard is it to Simulate a Quantum Circuit?

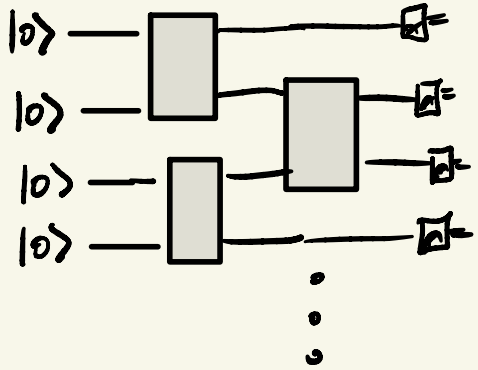
- What does it mean to simulate? One version: sample exactly from output of quantum circuit.

Depth-1:



→ easy. $|x_{12}\rangle \otimes |x_{34}\rangle \otimes \dots$

Depth-2:



→ also easy. [TD '02]

↪ super-poly. time

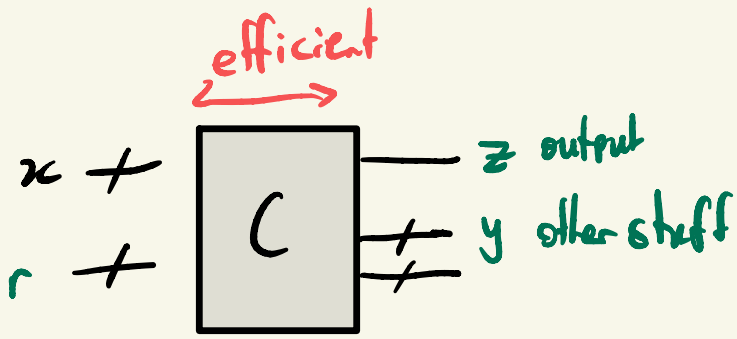
Thm [TD'02]: Depth-3 quantum circuits are hard to sample from exactly unless the PH collapses.

Pf: 1) Facts from complexity theory: PostBQP is much more powerful than PostBPP.

$$P^{\text{PostBPP}} \subseteq \Sigma_3 \qquad \text{[HHT '97]}$$

But. $$P^{\text{PostBQP}} \supseteq \text{PH}. \qquad \text{[Aaronson '05]}$$

2) If $\exists$ efficient classical circuit to sample exactly from depth-3 circuit, this means



$$P_C(y,z) = P_Q(y,z)$$

↑ depth-3 output

$\Rightarrow$ If we give Q the power to post-select, can simulate that too by post-selecting on y. $\therefore$ PostBPP $\geq$ PostDepth-3

3) $\mathrm{PostBQP} = \mathrm{PostDepth}\,3$.

1) + 2) + 3) $\Rightarrow$ $\mathrm{PostBQP} = \mathrm{PostDepth}\text{-}3 \subseteq \mathrm{PostBPP}$

$\Rightarrow \Sigma_3 \supseteq \mathrm{P}^{\mathrm{PostBPP}} \supseteq \mathrm{P}^{\mathrm{PostBQP}} \supseteq \mathrm{PH}$

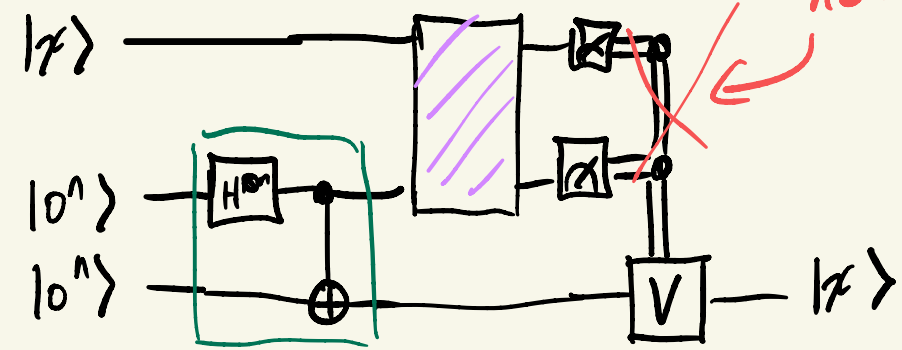
$\Rightarrow$ PH collapses at third level. ▨

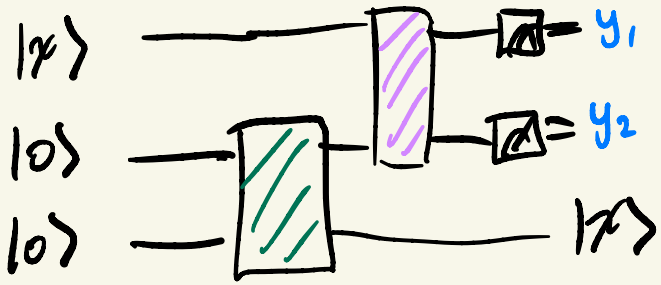
PostBQP = PostDepth-3

[Fenner, Green, Homer, Zhang '03]
[Gosset Lecture Notes]

- Proof: use quantum teleportation.

Teleportation:

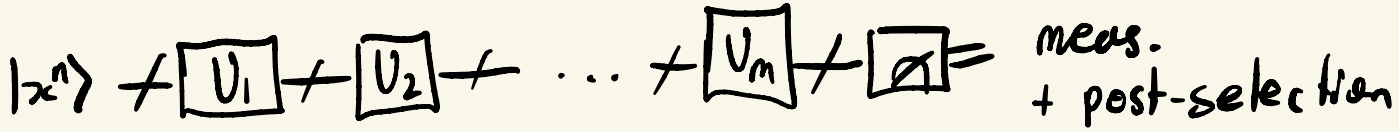




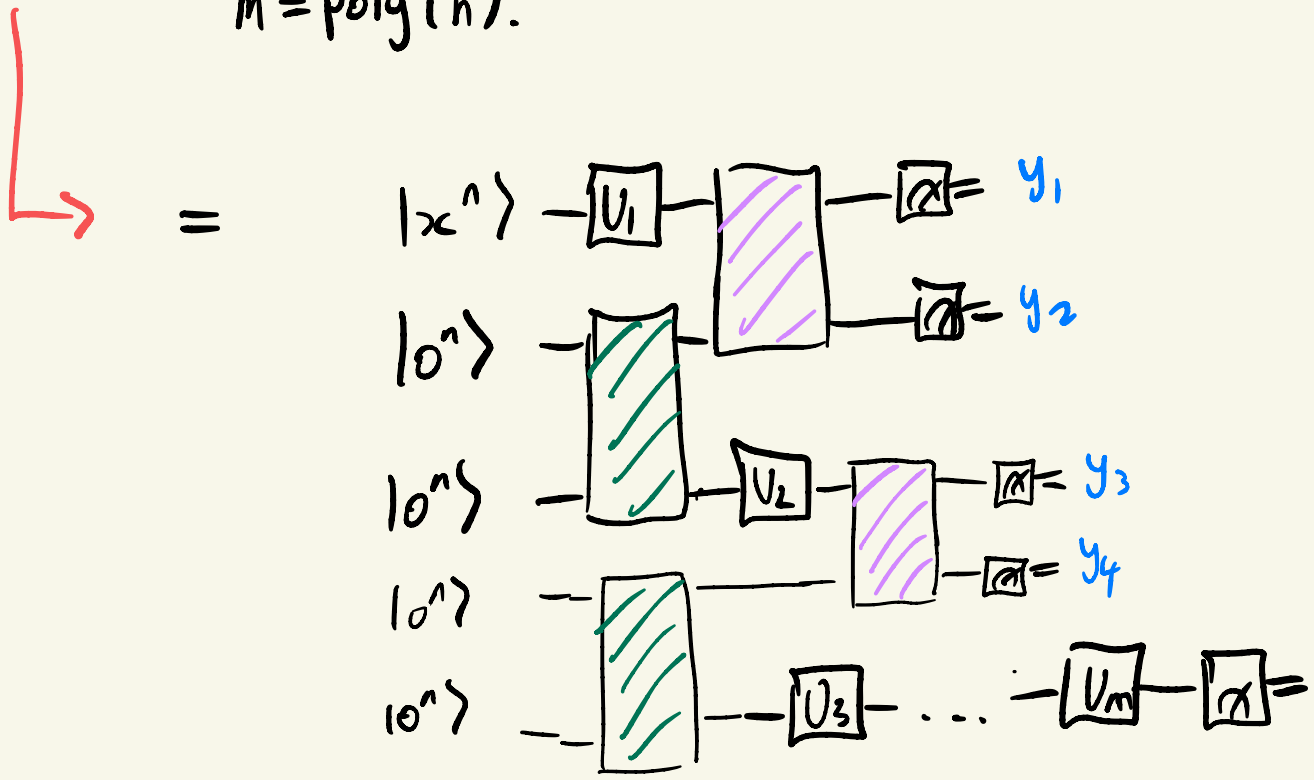
(Blackboard ?)

PostBQP = PostDepth-3

- Suppose we have a PostBQP circuit



$m = \text{poly}(n)$.



Exact Sampling

* super-poly.

Pros

- Computational task, no oracles
- "PH non-collapse" $\approx$ "$P \neq NP$"
  - ↳ fair assumption
- poly-time vs. "exp*-time separation
- Works for other models too

Cons

- Quantum computers cannot exactly sample either

...

Exact Sampling

* super-poly.

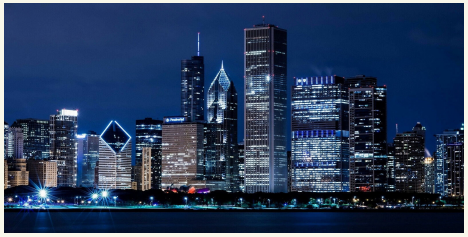
Pros

- Computational task, no oracles
- "PH non-collapse" $\approx$ "$P \neq NP$"
  - ↳ fair assumption
- poly-time vs. "exp*-time separation
- Works for other models too

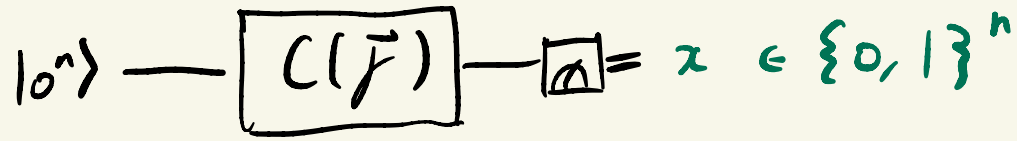
Cons

- Quantum computers cannot exactly sample either
  - ↳ 2 reasons: fault-tolerance, change of gate set
- Requires some complexity-theoretic assumptions

III. Modern Advantage



Approximate Sampling



Task: Given n, $\vec{f}$, output $x \in \{0,1\}^n$ sampled from $\tilde{p}$ s.t.

angles in circuit

$$\|p - \tilde{p}\|_1 \leq \frac{1}{n^{10}} .$$

- Before used post-selection. Now use estimation.
  - $P^{\text{Q. Est.}} \supseteq \text{PH}$ [GG '14]
  - $P^{\text{Cl. Est.}} \subseteq \Sigma_3$ [Stockmeyer '83]

Thm [BMS '15]: Suppose $P^{\text{Q. Est.}} \supseteq \text{PH}$ even if Q. Est. task defined in average-case setting. Then unless PH collapses, approximate sampling is classically hard.

Approximate Sampling

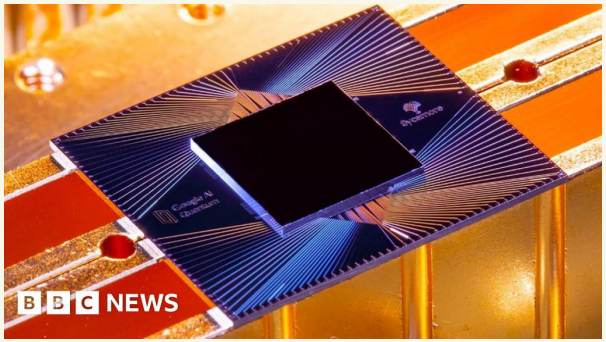
super-poly.

Pros

- Quantum computers can do this!
- Noisy quantum computers can do this!
- Poly vs. exp-time separation
- PH collapse very unlikely
- Works for other models too

Cons

- Average-case hardness conjectures remain unproven
- "Sampling" not a traditional computational task



Circuit-Depth Separations

* bounded fan-in, improved to unbounded by [WKST '19]

- Using quantum circuits inspired by nonlocal games, can show [BGKT'19]:

  i) there is a relation problem * solved w/ certainty by a constant-depth, 1D quantum circuit.

  ii) any classical circuit* requires depth at least $\Omega(\log n)$.

Pros

- Unconditional
  → no oracles, no conjectures
- Can be made robust to noise [BGKT '19]

Cons

- $\log n$ is pretty easy classically...
- Unclear why this is a fair comparison
  ↳ opinion

Summary

- Ongoing work to prove average-case hardness conjectures, give new circuit-depth separations, give new "hard" circuits e.g., dual unitaries.
- Query complexity, sampling, approximate sampling, and circuit-depth separations all point to a quantum advantage.
- No smoking gun...
- Alternative is just faith in hardness of factoring
- Is that good enough?