Complexity-theoretic evidence for Random Circuit Sampling

Adam Bouland
UC Berkeley

Bill Fefferman
UC Berkeley, U. Maryland/NIST

Umesh Vazirani
UC Berkeley

Chinmay Nirkhe

UC Berkeley Visit Days 2018

Quantum Supremacy and the Complexity of Random Circuit Sampling
A. Bouland, B. Fefferman, C. Nirkhe, U. Vazirani
[arXiv version soon]

The Extended Church Turing Thesis

Any "reasonable" method of computation can be *efficiently* simulated on a standard model (i.e. Turing Machine, uniform circuits, etc.)

Quantum Computing!

$\exists \mathcal{O}$ s.t. $\mathsf{BPP}^{\mathcal{O}} \subsetneq \mathsf{BQP}^{\mathcal{O}}$ [BV93,Sim94]

$\exists \mathcal{O}$ s.t. $\mathsf{BPP}^{\mathcal{O}} \subsetneq \mathsf{BQP}^{\mathcal{O}}$ [BV93,Sim94]

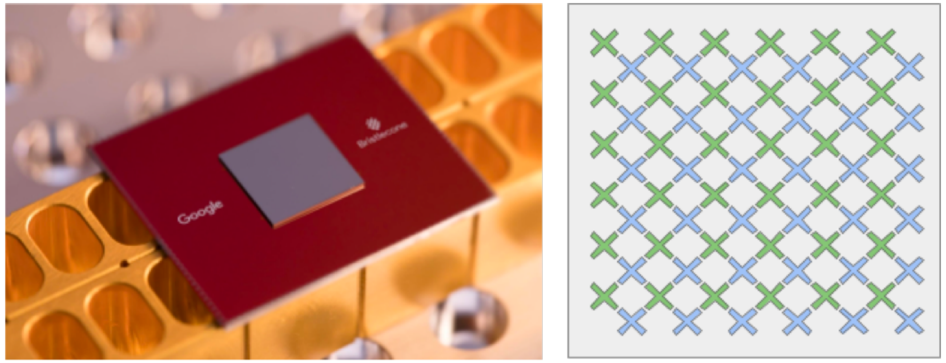
$\mathrm{FACTORING} \in \mathsf{BQP}$ [Sho94]

BQP = the set of languages decidable by a polynomial time quantum algorithm

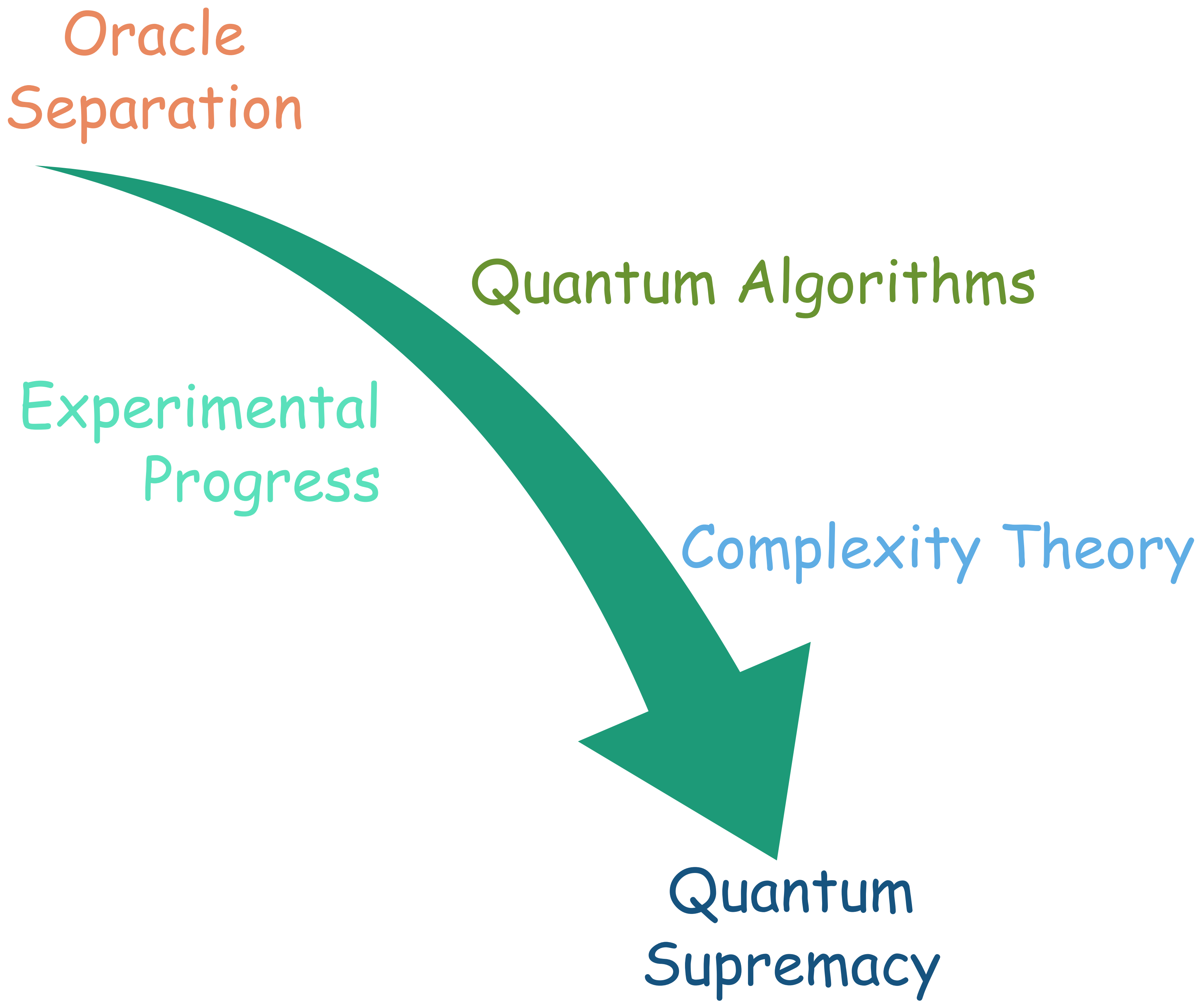
Experimental Progress

Joint Center for Quantum Information and Computer Science

TU Delft Delft University of Technology



Google 72-qubit Bristlecone chip


Oracle
Separation
Quantum Algorithms
Experimental
Progress
Complexity Theory
Quantum
Supremacy

Complexity-Theory inspired supremacy proposals

Problems for which no efficient classical algorithms exist (perhaps under complexity-theoretic conjectures)

Example: Boson Sampling [AA11]

Proves efficient classical algorithms cannot exist unless PH-collapses

Experimentally inspired supremacy proposals

Problems which we can experimentally test imminently

Example: Random Circuit Sampling [BIS+16]

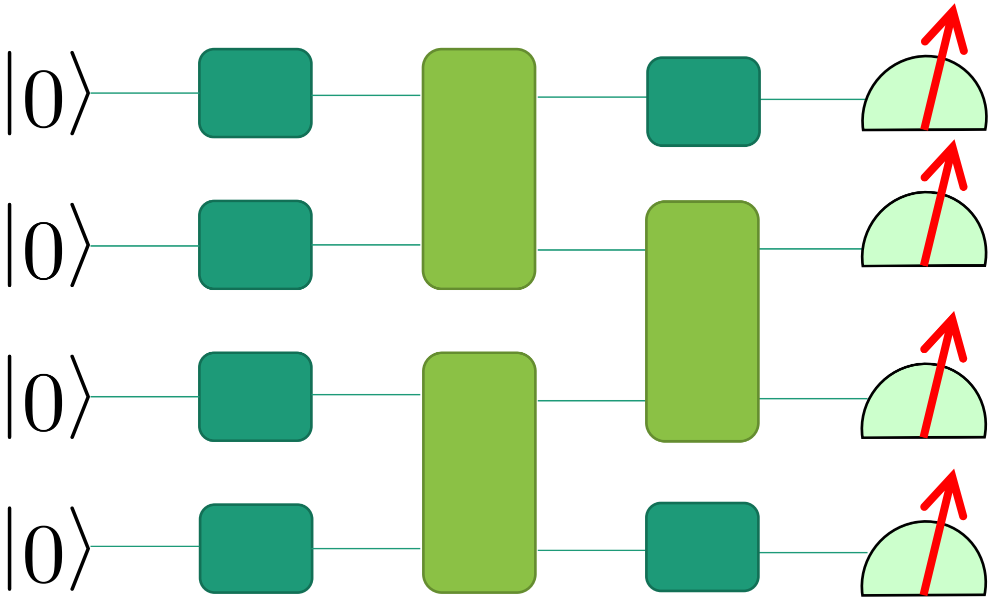
Near-term experimentally feasible due to high-quality superconducting qubits

A Quantum Supremacy Proposal

Random Circuit Sampling

Given the description of a quantum circuit C, sample from the output distribution of the quantum circuit.

Fix an architecture over quantum circuits

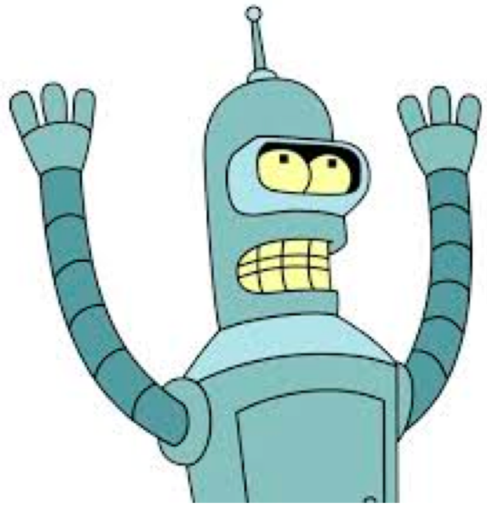


Given a circuit from the architecture, sample from its output probability distribution

Sampling Proposal

Choose a random instance of your sampling problem on ~50 qubits

Candidate Quantum Computer



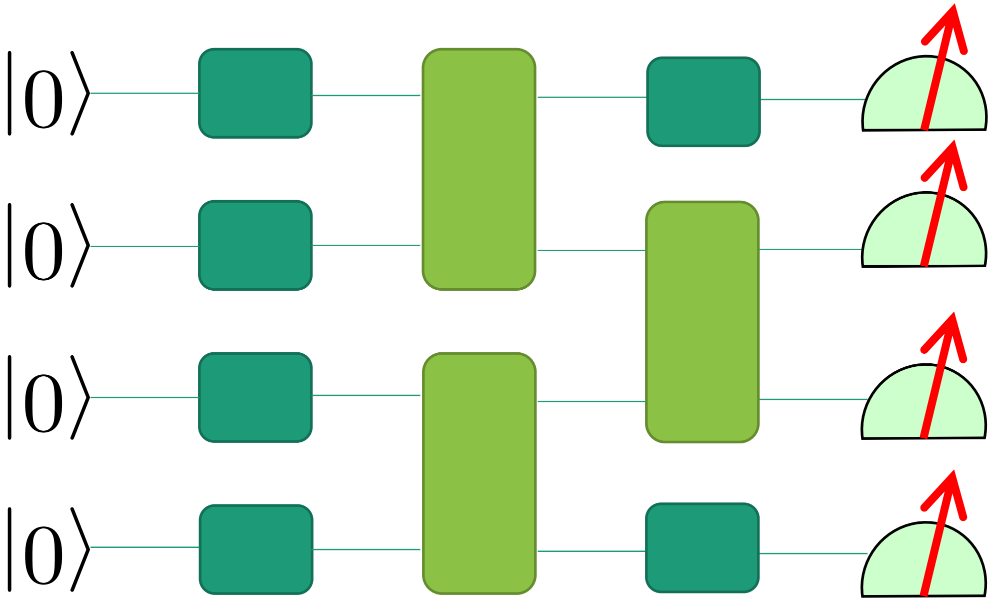
Classical Supercomputer

Outputs samples

Compare and accept if close

Calculates ideal output distribution exactly

Sampling from the exact output distribution of a quantum circuit is #P-hard



Trick: Since proving #P-hardness, by Toda's Theorem can use PH reductions instead of just P reductions

Exact classical sampling from quantum circuits would give us:

$$\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{BPP}^{\mathrm{NP}}$$

Contradicts the non-collapse of the PH:

$$\mathrm{BPP}^{\mathrm{NP}} \subseteq \Sigma_3 \subsetneq \mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$$

Toda's Theorem

Proof: Estimating output probabilities is #P-hard. Apply $\mathrm{BPP}^{\mathrm{NP}}$ reduction due to Stockmeyer's Thm '85 to get sampling is #P-hard as well.

Therefore, *exact* quantum sampling is #P-hard under BPP^{NP}-reductions

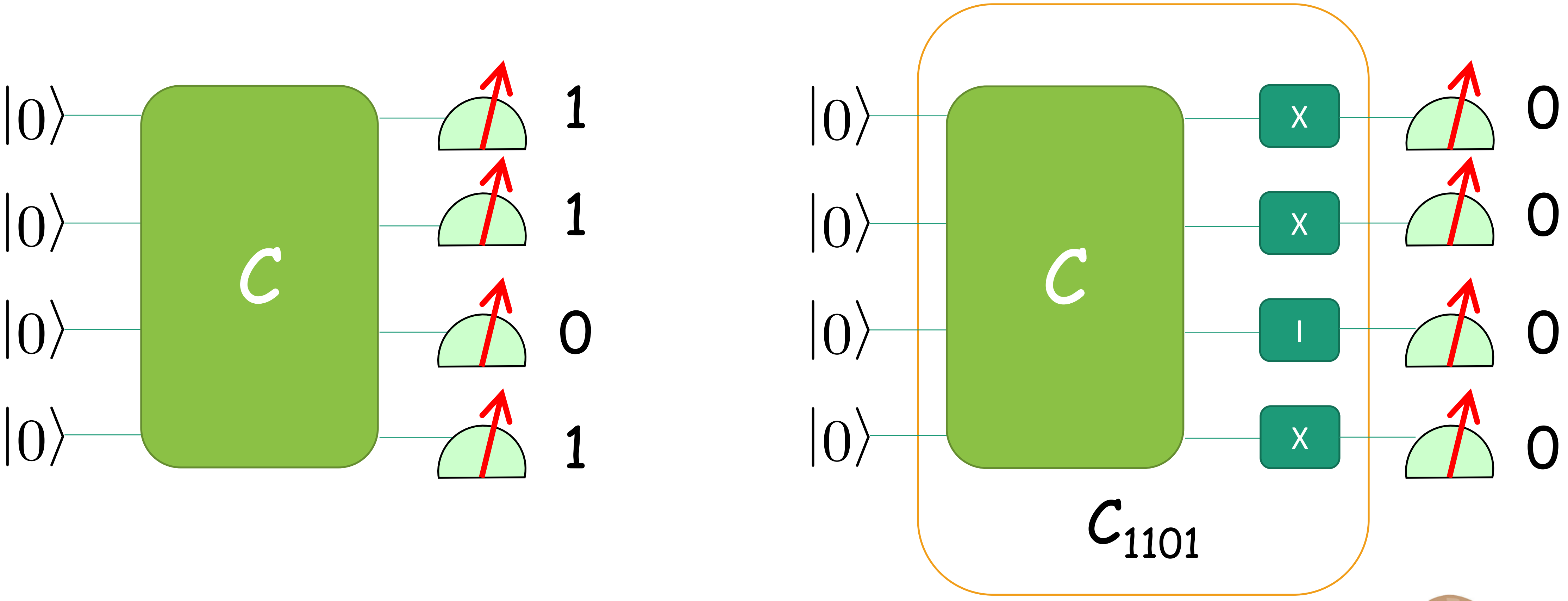
But you aren't done yet! No quantum device would *exactly* sample from the output distribution due to noise!

So in order to make this argument, you have to show that no classical sampler can even *approximately* sample from the same distribution!

We want to embed the hardness across all the outputs of the probability distribution.

We want a robustness condition: Being able to compute most probabilities should be #P-hard.

Hiding



$$\Pr[C \text{ outputs } 1101] = \Pr[C_{1101} \text{ outputs } 0000]$$

~~We want a robustness condition: Being able to compute most probabilities should be #P hard.~~

We want a robustness condition: Being able to compute $Pr_0(C)$ for most circuits C should be #P-hard.

$Pr_0(C)$ = prob. C outputs 0

Which known problem has such a property?

$$\mathrm{perm}(M) = \sum_{\sigma \in S_n} \prod_{j=1}^{n} M_{j,\sigma(j)}$$

Theorem [Lip91,GLR+91]: The following is #P-hard: For sufficiently large q, given uniformly random n x n matrix M over F_q, output perm(M) with probability > $\frac{3}{4}$ + 1/poly(n)

Basis for Boson Sampling

Permanent is avg-case hard

$$\text{perm}(A) = \sum_{\sigma \in S_n} \prod_{j=1}^{n} A_{j,\sigma(j)}$$

perm(A) is a degree n polynomial in the matrix entries

Choose R a random matrix. Let $M(t) = A + Rt$.
$M(0) = A$ and $M(t)$ for $t \neq 0$ is uniformly random.
perm(M(t)) is a degree n polynomial in t

Choose random $t_1, \ldots, t_{n+1}$, calculate perm($M(t_i)$)
Interpolate the polynomial perm(M(t)). Output perm(M(0))

Proof Permanent is avg-case hard

Assume we can calculate perm(R) for random R with probability > 1 - 1 /(3n + 3).

By union bound, we calculate perm(A) with probability 2/3. Since permanent is worst-case #P-hard [Val79], This proves statement for probability 1 – 1/(3n + 3).

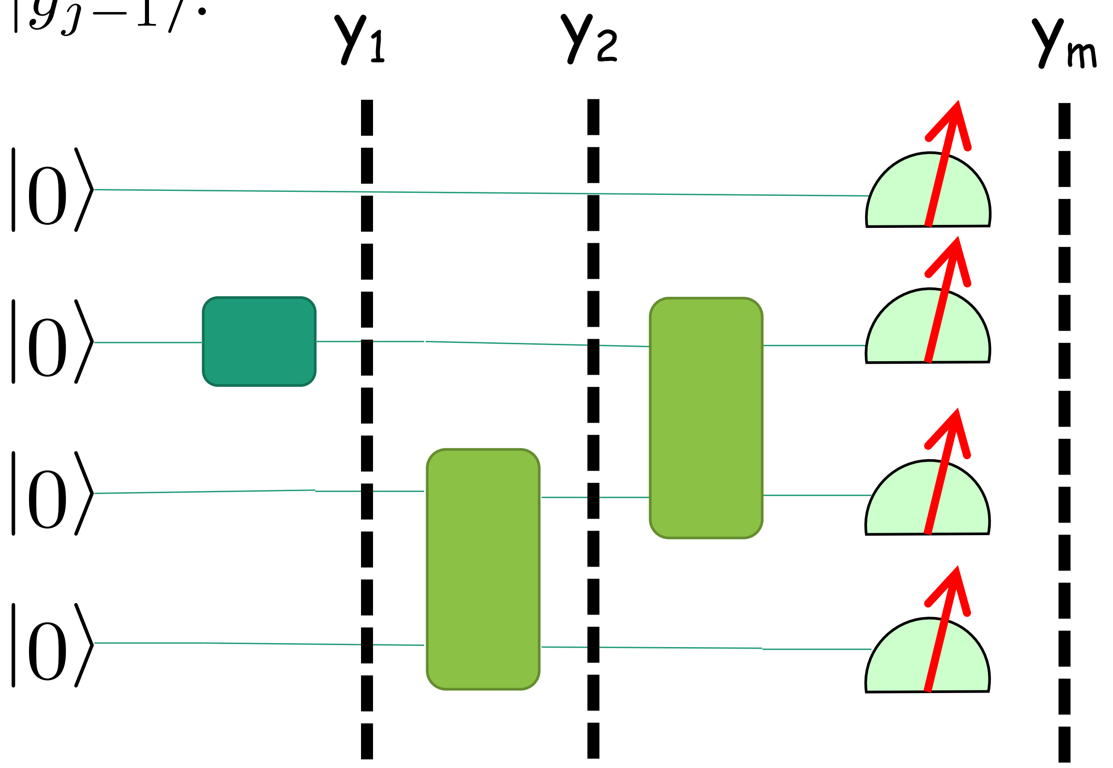
Better interpolation techniques bring the probability down to $\frac{3}{4}$ + 1/poly(n).

Goal: find a similar polynomial structure in the problem of Random Circuit Sampling

High-level idea

Feynman Path Integral:

$$\langle y_m|C|y_0\rangle = \sum_{y_1,y_2,\ldots,y_{m-1}\in\{0,1\}^n} \prod_{j=1}^{m} \langle y_j|C_j|y_{j-1}\rangle.$$



Quantum analog of space-efficient brute-force evaluation of a circuit

Feynman Path Integral

$$\langle 0|C|0\rangle = \sum_{y_1,y_2,\ldots,y_{m-1}\in\{0,1\}^n} \prod_{j=1}^{m} \langle y_j|C_j|y_{j-1}\rangle.$$

Then $\Pr_0(C)$ is a low-degree polynomial in the gate entries. We want to apply a similar interpolation technique as permanents.

Idea 1:

$$\langle 0|C|0\rangle = \sum_{y_1,y_2,\ldots,y_{m-1}\in\{0,1\}^n} \prod_{j=1}^{m} \langle y_j|C_j|y_{j-1}\rangle.$$

Consider the circuit $C(t)$ formed by changing each gate C_i to $C_i + tH_i$ for random gate H_i.

Just like permanent!

But, $C_i + tH_i$ isn't a quantum gate!

Idea 2:

$$\langle 0|C|0\rangle = \sum_{y_1,y_2,\ldots,y_{m-1}\in\{0,1\}^n} \prod_{j=1}^{m} \langle y_j|C_j|y_{j-1}\rangle.$$

Consider the circuit C(θ) formed by changing each gate

$$C_i \mapsto C_i H_i e^{-i\theta h_i} \text{ where } h_i = -i \log H_i$$

1. C(1) = C
2. For small θ, circuit looks θ-close to random!
3. Not a low-degree polynomial in θ

Applying fraction of a gate is inherently quantum! No classical analog!

Idea 3:

$$\langle 0|C|0\rangle = \sum_{y_1,y_2,\ldots,y_{m-1}\in\{0,1\}^n} \prod_{j=1}^{m} \langle y_j|C_j|y_{j-1}\rangle.$$

Taylor Series!

$$\text{Replace } e^{-i\theta h_i} \text{ with } \sum_{k=0}^{\mathrm{poly}(n)} \frac{(-i\theta h_i)^k}{k!}$$

1. $C(1) \approx C$
2. For small θ, circuit looks θ-close to random!
3. A low-degree polynomial in θ
4. For more complicated technical reasons, this is a necessary, but not sufficient, proof of average-case hardness.

Current state of Quantum Supremacy Proposals

Proposal	Worst-case hardness	Average-case hardness	Imminent experiment
BosonSampling			
FourierSampling			
IQP			
Random Circuit Sampling			