On the power of random quantum circuits

Bill Fefferman

(University of Chicago)

Based on "**On the complexity and verification of quantum random circuit sampling**" with A. Bouland, B. Fefferman, C. Nirkhe, U. Vazirani (Nature Physics, arXiv: 1803.04402)

And "**Noise and the frontier of quantum supremacy**" with A. Bouland, B. Fefferman, Z. Landau, Y. Liu (FOCS 2021, arXiv: 2102.01738)

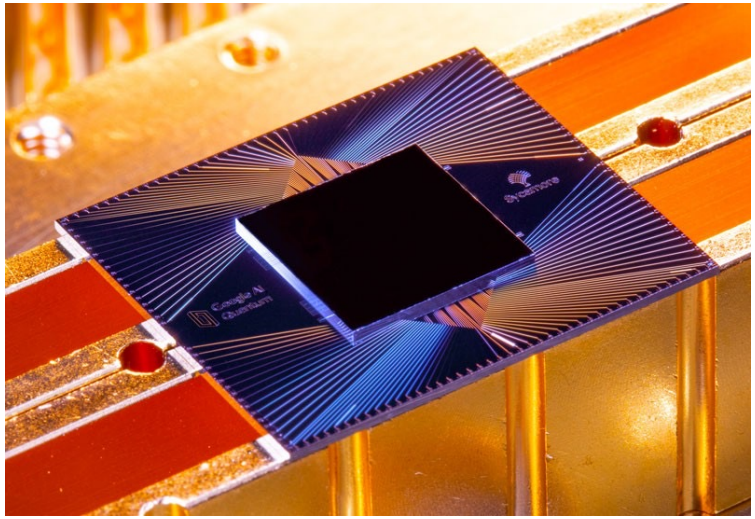
Stanford University

THE UNIVERSITY OF CHICAGO

Berkeley UNIVERSITY OF CALIFORNIA

Noisy Intermediate-Scale Quantum Systems: Advances and Applications workshop*, KITP UCSB*

The first “Quantum advantage” claims have now been made…



Random Circuit Sampling (Google “Sycamore”) in late 2019

Gaussian BosonSampling – USTC “Jiuzhang” in late 2020, Xanadu’s “Borealis” in 2022

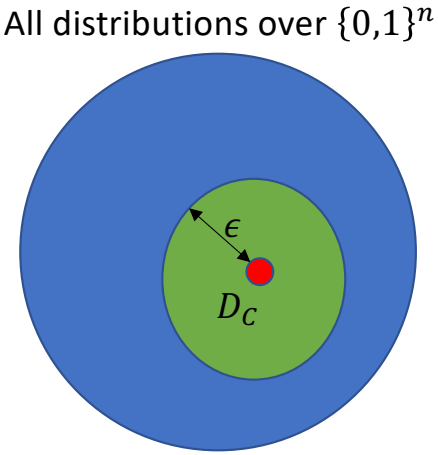
This talk: the latest complexity theoretic evidence to believe these “random quantum circuit” experiments might be solving classically intractable problems

What do we mean by “classically intractable”?

- **Our setting: asymptotic hardness** – prove there’s no classical simulation algorithm with running time that is polynomial in the system size
  - In my view this is necessary, but *not sufficient* to conclude “quantum advantage”
- Also important to consider non-asymptotic issues (i.e., the best supercomputer takes “a long amount of time” to solve the problem at the same system size as the experiment)

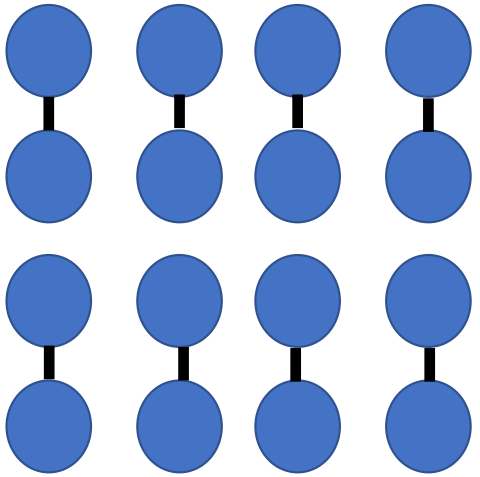
What do we mean by "classical simulation" algorithm?

- **Goal:** prove impossibility of an efficient *"classical Sampler"* that:
  - takes as input a random circuit C which specifies distribution D_C over $\{0,1\}^n$
  - outputs a sample from *any* distribution $X \sim_{TV} D_C$
    - Total variation distance models *imprecision of the classical algorithm*, not physical noise (but we'll talk about physical noise later!)



Google's RCS proposal [Boixo et. al. 2017]

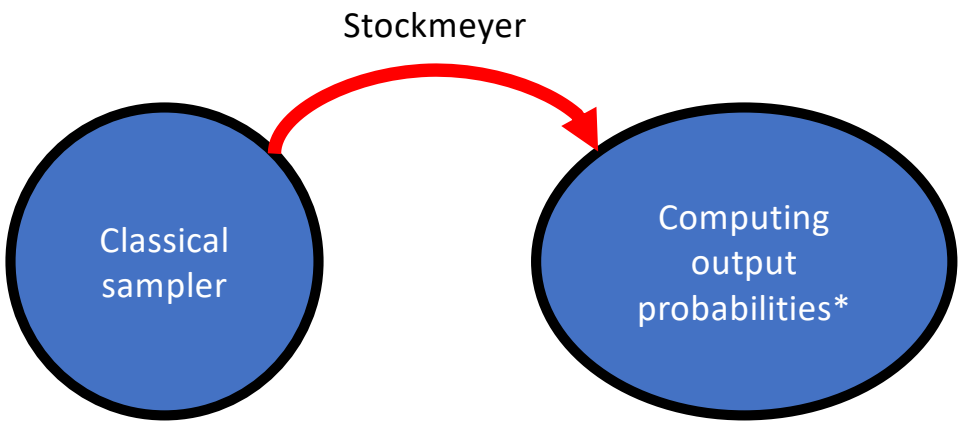
- Generate a quantum circuit C on n qubits on a 2D lattice, with $d \sim \sqrt{n}$ layers of (Haar) random nearest-neighbor gates
  - In practice use a discrete approximation to the Haar random distribution
- Start with $|0^n\rangle$ input state, apply random quantum circuit and measure in computational basis



(single layer of Haar random two qubit gates applied on 2D grid of qubits)

Proof first step: from sampling to computing

- By well-known reductions [Stockmeyer ’85], [Aaronson & Arkhipov ’11] it suffices to prove that ***estimating*** the output probability of a ***random*** quantum circuit is **#P**-hard

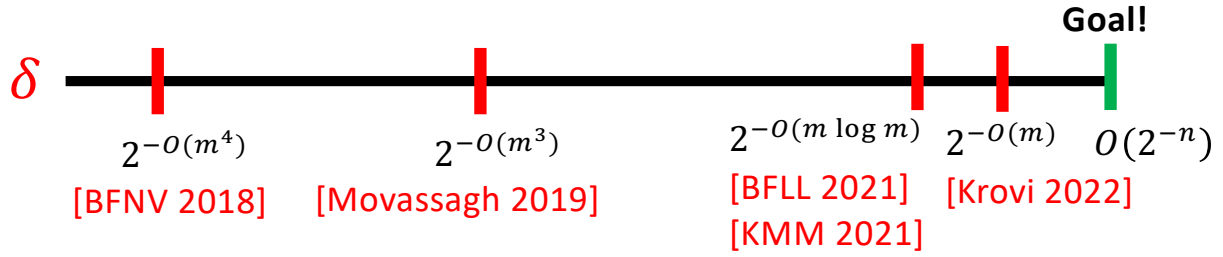


Formal statement of q. supremacy conjecture

- **Definition:** Let the "output probability", $p_0(C) = |\langle 0^n|C|0^n\rangle|^2$
- Then consider the $\delta -$ ***Random Circuit Estimation*** problem:

> Given as input circuit C, output q so that $|q - p_0(C)| \leq \boldsymbol{\delta}$ with probability 2/3 over C

- To prove goal, it suffices to show that the $\delta = O\left(\frac{1}{2^n}\right)$ problem is **#P**-hard
- **Known hardness results** with respect to C on n qubits, size $m = O(n \cdot d)$



- BosonSampling: goal is $\frac{1}{e^{n \log n}}$, whereas we have hardness at $\frac{1}{e^{6n \log n}}$ [BFLL'21]

Roadmap for the rest of talk

1. Proof of hardness result from [F., with Bouland, Nirkhe & Vazirani '19]
   - To do this, will first discuss Lipton's average-case hardness result for computing the Permanent of a random matrix
   - Then we'll adapt Lipton's result from Permanent to output probability of random quantum circuit
2. We'll prove that these results are "robust to uncorrected depolarizing noise" [F., with Bouland, Landau & Liu'21]

Average case hardness for **Permanent** [Lipton '91]

- **Permanent** of $n \times n$ matrix is **#P**-hard in the worst-case [Valiant '79]
  - $Per[X] = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i,\sigma(i)}$
- *Algebraic property*: $Per[X]$ is a degree n polynomial with n^2 variables
- Need compute $Per[X]$ of worst-case matrix X
  - But we only have access to algorithm O that correctly computes *most* permanents over $\mathbb{F}_p$
  - i.e., $\Pr_{Y \in_R \mathbb{F}_p^{n \times n}}[O(Y) = Per[Y]] \geq 1 - \frac{1}{poly(n)}$
- Choose $n+1$ fixed non-zero points $t_1, t_2 \ldots, t_{n+1} \in \mathbb{F}_p$ and uniformly random matrix R
- Consider line $A(t) = X + tR$
  - *Observation 1 "scrambling property"*: for each i, $A(t_i)$ is a random matrix over $\mathbb{F}_p^{n \times n}$
  - *Observation 2*: "univariate polynomial": $Per[A(t)]$ is a degree n polynomial in t
- But now these $n+1$ points uniquely define the polynomial, so use polynomial extrapolation to evaluate $Per[A(0)] = Per[X]$

[BFNV'18]: Hardness for Random Quantum Circuits

- *Algebraic property*: much like $Per[X]$, output probability of random quantum circuits has polynomial structure
  - Consider circuit $C = C_m C_{m-1} \dots C_1$
  - Polynomial structure comes from path integral:
    - $\langle 0^n|C|0^n\rangle = \sum_{y_2,y_3,\dots,y_m \in \{0,1\}^n} \langle 0^n|C_m|y_m\rangle\langle y_m|C_{m-1}|y_{m-1}\rangle \dots \langle y_2|C_1|0^n\rangle$
- This is a polynomial of degree m in the gate entries of the circuit
- So the output probability $p_0(C)$ is a polynomial of degree $2m$

First attempt at adapting Lipton's proof

- Fix m Haar random two qubit gates $\{H_i\}_{i\in[m]}$
- ***Main idea*:** Implement tiny fraction of H_i^{-1}
  - i.e., $C_i' = C_i H_i e^{-ih_i\theta}$
  - This scrambles C if $\theta \approx small$, since each gate is close to Haar random
  - However, if $\theta = 1$ the corresponding circuit $C' = C$
- ***Strategy (in style of Lipton):*** take several non-zero but small θ, compute output probabilities of "random but correlated" circuits ${C'}_{\theta_1}, {C'}_{\theta_2}$ … and apply polynomial extrapolation to compute $p_0(C)$

This is not quite the "right way" to scramble!

- ***Problem*:** $e^{-ih_i\theta}$ is not polynomial in θ
- ***Solution:*** take fixed truncation of Taylor series for $e^{-ih_i\theta}$
  - i.e., each gate of C' is $C_i H_i \sum_{k=0}^{K} \frac{(-ih_i\theta)^k}{k!}$
  - So each gate entry is a polynomial in θ and so is $p_0(C')$
  - Now extrapolate and compute $q(1) = p_0(C)$

Extensions to [BFNV'19]

- How do we motivate the Taylor series truncations?
  - Main technical result [BFNV'19]: ***estimation*** of $p_0(C')$ is hard **iff *estimating*** $p_0(C)$ is hard
    - **Intuitively, because the "truncation error" is so much smaller than the desired precision, $\mathbf{o}\left(\frac{1}{2^n}\right)$.**
- More recently, [Movassagh'20] has given related arguments that eliminates the need for these truncations
- Most recently, we've been able to extend this result to larger additive imprecision i.e., computing $p_0(C)$ within additive error $\mathbf{2^{-O(m)}}$ is **#P**-hard [BFLL'21] [KMM'21] [Krovi'22]
  - Moreover, there's reason to think this imprecision will be difficult to improve…

Understanding hardness of *noisy* random quantum circuits [BFLL'21]

- Without error-correction noise eventually overwhelms
  - e.g., Google's RCS experiment ~0.2% fidelity and 99.8% noise
- Fix noise model: e.g., Each gate C_i is followed by two qubit depolarizing noise channel:
  - $\mathcal{E}_i = (1-\gamma)\rho + \frac{\gamma}{15}\sum_{\alpha,\beta\in\mathcal{P}\times\mathcal{P}-(I,I)}(\sigma_\alpha \otimes \sigma_\beta)\rho(\sigma_\alpha \otimes \sigma_\beta)$
- That is, we can think about choosing a noisy random circuit by:
  - First pick ideal circuit $C = C_m C_{m-1} \dots C_1$ from the random circuit distribution
  - Then environment chooses operators N, from a distribution $\mathcal{N}$ (i.e., via $\mathcal{E}_i$)
  - We get a sample from output distribution of $N \cdot C$ without learning the noise operators

Similar hardness arguments work with noise!

- The output probability of noisy circuit can still be written as a weighted sum of path integrals:
  - $E_{N\sim\mathcal{N}}[|\langle 0^n|N\cdot C|0^n\rangle|^2] =$
    $\sum_N \Pr_{\mathcal{N}}[N]\cdot\left|\sum_{y_1,y_2,\ldots,y_m\in\{0,1\}^n}\langle 0^n|N_m C_m|y_m\rangle\ldots\langle y_2|N_1 C_1|0^n\rangle\right|^2$
  - **Key point:** this is still a polynomial of degree $2m$ in the ideal gate entries
- So using essentially the same arguments as before, providing that the noise rate γ, is a sufficiently small constant, we can prove it's hard to compute this noisy output probability, $E_{N\sim\mathcal{N}}[p_{0^n}(N\cdot C)]$, to within $\pm 2^{-O(m)}$ [BFLL'21] [Fujii '16]

But there's also a (trivial) classical algorithm!

- **Issue:** uncorrected depolarization noise causes output distribution to rapidly converge to uniform as system size grows
  - And it's clearly not hard to output a probability from the uniform distribution!
- **Key question:** How accurate is this trivial algorithm (i.e., what is the imprecision?)
- **Conjecture**: for "deep" random circuits, $\mathbf{2}^{-\boldsymbol{O}(\boldsymbol{\gamma}\cdot\boldsymbol{d}\cdot\boldsymbol{n})} = \mathbf{2}^{-\boldsymbol{O}(\boldsymbol{m})}$ [e.g., Boixo, Smelyanskiy, Neven '17]!
  - We can prove this in certain simplified toy models of random circuits [BFLL'21]
  - Recent work [**arXiv: 2112.00716** – in QIP 2022]: this isn't true for shallow circuits!

The “noise barrier” to improving robustness

- On the one hand we’ve established that computing output probabilities of ***noisy*** random circuits of size m is **hard** to within imprecision $\mathbf{2^{-O(m)}}$
- On the other hand, there might be reason to think it’s classically **easy** to solve this problem to within slightly larger imprecision (i.e., still $\mathbf{2^{-O(m)}}$)
- **Upshot:** So if we want to dramatically improve this robustness in the ***noiseless*** case we need to invent new proof techniques that are ***not*** robust to noise.

Future directions regarding RCS

- Are there useful applications for random quantum circuits? One direction: certified randomness (our work on this: **arXiv: 2111.14846** based on a proposal by Aaronson)
- Benchmarking/verification: how can we verify classically intractable quantum experiments without too much trust in the experiment? (our work on this: **arXiv: 2105.05232**)
- How close are the output distributions of noisy random quantum circuits to the uniform distribution? (our work on this: **arXiv: 2112.00716**)

Thanks!