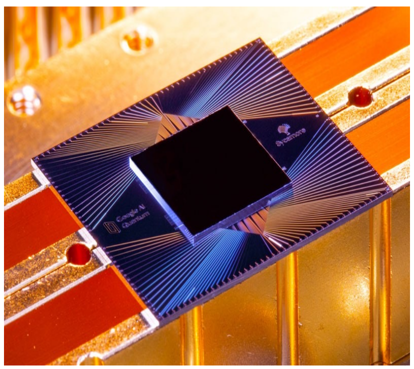
Have we seen a demonstration of experimental quantum advantage?

Bill Fefferman

THE UNIVERSITY OF CHICAGO

ASPIRE Quantum Kick-off Workshop, U. of Tokyo, July 26, 2024

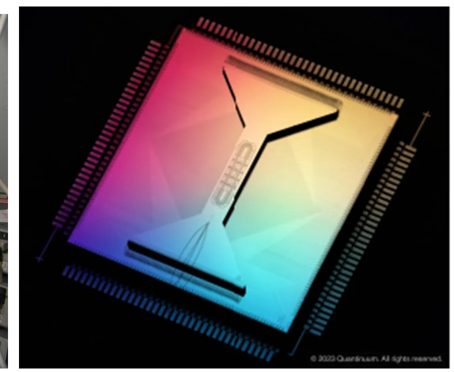
The first "Quantum advantage" claims have now been made…



Random Circuit Sampling (Google "Sycamore" in 2019, 2023)

Gaussian BosonSampling (USTC, Xanadu in 2021,2022,2023)

IQP sampling with logical qubits made from Rydberg atoms (Harvard/QuEra 2023)

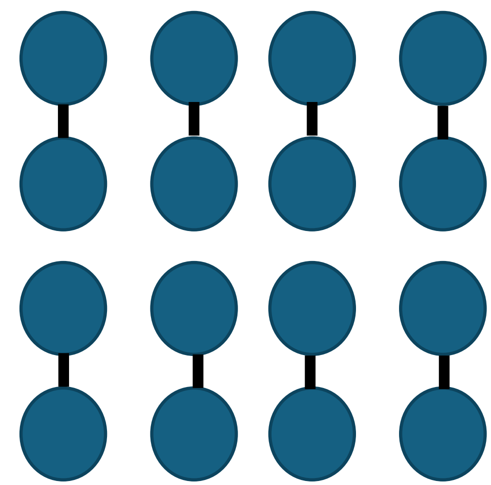


Random Circuit Sampling with trapped ions (Quantinuum "H2-1" in 2024)

This talk: these are all "random quantum circuit" experiments.
Why should any of these be hard to simulate classically?

What is Random Circuit Sampling? [Boixo et. al. 2017]

- Generate a quantum circuit C on n qubits on a 2D lattice, with d 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 all qubits in computational basis
  - i.e., Sample from a distribution D_C over $\{0,1\}^n$
- Has now been implemented e.g.,:
  - n = 53 qubits, d = 20 [Google, 2019]
  - n = 60 qubits, d = 24 [USTC, 2021]
  - n = 70 qubits, d = 24 [Google, 2023]



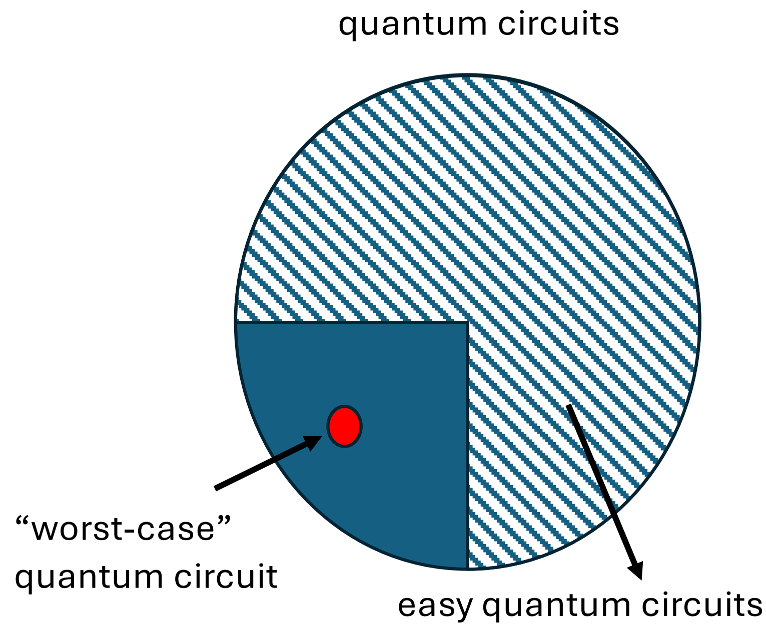
(single layer of Haar random two qubit gates applied on 2D grid of qubits)

Question 1: *Why should this sampling problem be so hard for classical computers?*

- Not at all obvious! Previous quantum algorithms (e.g., Shor, Grover) use very structured quantum circuits to achieve speedup
- **Formally:** goal is to prove impossibility of an efficient *"classical sampler"* algorithm that solves the same problem as quantum experiment:
  - takes as input a quantum circuit C
  - outputs a sample from D_C with high probability over C

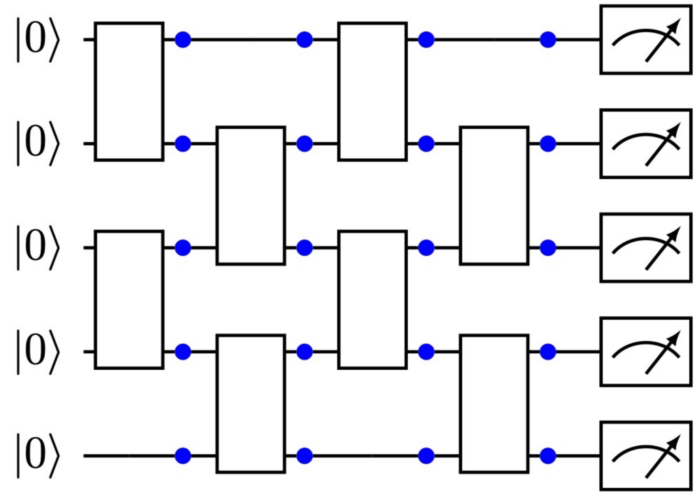
Our work gives evidence for classical hardness of random quantum circuits

- There are a few very special "worst-case" quantum circuits that are known to be hard to simulate classically
  - e.g., think of Shor's quantum circuit for factoring
  - But these circuits are very unlikely to be chosen at random!
- Our results [BFNV'19][BFLL'21] establish a "worst-to-average-case" reduction!
  - i.e., suppose it's easy to classically simulate (compute output probability) of *most* quantum circuits, then we can use this ability to simulate the worst-case circuit classically too
  - This is a contradiction, since the worst-case circuit is hard!
  - So there can't exist a classical algorithm that simulates random quantum circuits (with high probability)!



Question 2: How hard are *noisy* random circuits?

- Noise is overwhelming in near-term experiments
  - e.g., Google's 2019 experiment: ~0.2% signal, 99.8% noise!
- How to theoretically model this? First, consider just single qubit depolarizing – i.e., each layer random gates followed by:
  - $\mathcal{E}(\rho) = (1-\gamma)\rho + \frac{\gamma I}{2} Tr[\rho]$
  - Where the noise strength, γ is positive constant
  - This is a popular model, but oversimplified!



Depolarizing noise and complexity

- Intuitively, uncorrected depolarizing noise increases entropy. As the circuit gets deeper the output distribution converges to uniform
- **First question:** how close are the output distribution of noisy (i.e., depolarizing) random circuit and uniform distribution?
  - $2^{-\Theta(d)}$ close in TVD [Aharonov et. al. '96][Deshpande et. al.'22]
- This rules out *scalable noisy* quantum advantage at *super-logarithmic depth*
- [Aharonov et. al. '22] give a classical algorithm for sampling from the output distribution of noisy, $\log(n)$ depth random quantum circuits

Can we extend the [Aharonov et. al. ’22] algorithm to other noise models?

- Analysis of [Aharonov et. al. ’22] relies on “anti-concentration” property
  - i.e., Output distribution of random circuit is “*uniform-ish*” or well-spread over outcomes
  - Anti-concentration is a property of sufficiently deep noisy random quantum circuits as long as the noise channel is *unital* or entropy increasing
- What if the noise doesn’t always increase entropy?
  - e.g., amplitude damping channel: $K_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, K_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$
  - This noise can decrease entropy!
  - In recent work [Ghosh et. al.’24] we show that such circuit distributions *never anti-concentrate*!
  - *So in such cases we know neither hardness, nor easiness!*

Future directions for random quantum circuits

- **Is near-term quantum advantage possible with realistic uncorrected noise?**
- Useful applications of random quantum circuit experiments?
  - We are currently working on using these experiments to *certifiably produce random numbers*, with cryptographic applications (see e.g., Aaronson & Hung'23)
- To make these applications work we'll need far better ways to classically verify any of these sampling tasks…
- For much more complete discussion please see my Institute for Advanced Study/Park City lectures (on youtube, lecture notes coming soon…)