Quantum Computational ~~Supremacy~~ advantage? superiority? inimitability?

Scott Aaronson, UT Austin

ACM TechTalk, Sep. 9, 2021

Quantum Mechanics

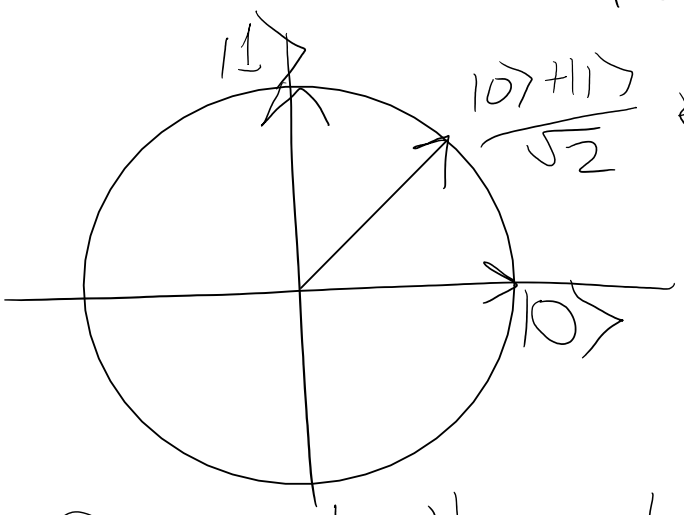
- Strange set of rules, discovered in 1920s, for calculating the probability something happens
- OS that (AFAWK) everything else in Nature runs on as application software
- Much simpler once you take the physics out!

The state of any isolated physical system is a unit vector of complex numbers, called "amplitudes"

E.g., a qubit (quantum bit) has an

E.g., a qubit (quantum bit) has an amplitude to be 0 & an amplitude to be 1:

$$a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2 \qquad |a|^2 + |b|^2 = 1$$



← superposition of |0⟩ state & |1⟩ state

If you ask the qubit whether it's |0⟩ or |1⟩ ("measure"), it says |0⟩ with $|a|^2$ probability & |1⟩ with $|b|^2$ probability

But besides measuring, we can also apply norm-preserving linear transformations ("unitaries") to the vector of amplitudes

$$\text{E.g., } R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$ (45° counterclockwise rotation)

And these can create interference, the central signature of quantum...

central signature of quantumness!

E.g., $R^2|0\rangle = R\,\frac{|0\rangle+|1\rangle}{\sqrt{2}}$

$$= \frac{R|0\rangle + R|1\rangle}{\sqrt{2}}$$

$$= \frac{\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \frac{-|0\rangle+|1\rangle}{\sqrt{2}}}{\sqrt{2}}$$

$$= \boxed{|1\rangle}$$

An n-qubit state has the form

$$\sum_{x\in\{0,1\}^n} a_x|x\rangle \in \mathbb{C}^{2^n}$$

Generally entangled (not factorizable into state of qubit 1, qubit 2, etc. separately)

$n = 1000 \Rightarrow 2^{1000}$ amplitudes

This is why QM seems exponentially hard to simulate on classical computers, & why a

quantum computer might do better!

BUT BEWARE: QC is not just free exponential parallelism! (much as "pointy-haired bosses" want it to be)

When you observe, you see just a single n-bit string x, with probability $|a_x|^2$.

Only hope of a quantum advantage:

Exploit interference to boost the amplitudes of the outputs x you want

RIGHT ANSWER WRONG ANSWER

We should only expect this to work for some special tasks!

QUANTUM SUPREMADVANTAGE

Refers to the first use of a QC to do some welldefined mathematical task, faster than we know how with any classical computer on earth.

NOTE: I didn't say a useful task! ☺

But we do want to do better than some molecule that "achieves supremacy at simulating itself"

Ideally: A programmable device that gets exactly the same input as a competing classical computer & has to perform exactly the same task.

V.S.

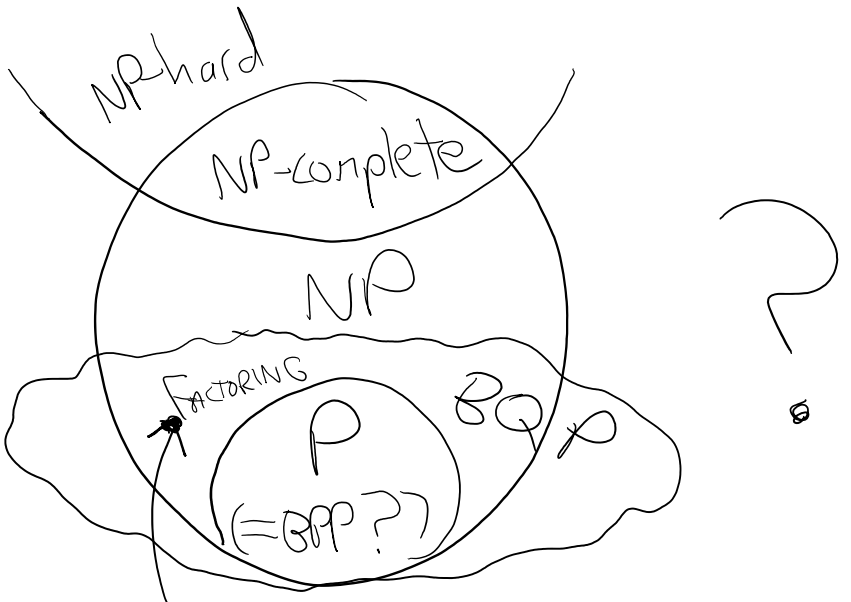
We not only want the QC to win, we want to rule out any explanation for how it won other than "by exploiting 2^n amplitudes!"

What's the point? Cf. Wright Flyer.

BRIEF HISTORY OF QUANTUM SUPREMADVANTAGE

1982 Feynman suggests QCs would be exponentially faster at simulating QM itself

1993 Bernstein & Vazirani define BQP:
Bounded-Error Quantum Polynomial-Time



1994 Shor's fast quantum factoring algorithm!

1996 Theory of quantum fault-tolerance suggests building a QC able to run Shor's algorithm should be possible, but staggeringly hard!

2011 Alex Arkhipov & I propose BOSON SAMPLING as a quicker route to a clear quantum speedup, using optical devices.

Idea: Have the QC sample a distribution D over n-bit strings, such that if a classical computer could sample the same distribution in poly(n) time, the polynomial

hierarchy would collapse.

Bremner, Jozsa & Shepherd independently propose a similar scheme ("IQP")

2012 John Preskill coins "quantum supremacy" for things like BosonSampling & IQP

2014 Google hires John Martinis, forms lab in Santa Barbara that aims to do the first-ever demonstration of quantum supremacy

2017 Lijie Chen & I adapt the theory of BosonSampling to superconducting circuits like Google's

2019 Google publishes a supremacy claim in Nature!
53 qubits, $2^{53} \approx 9$ quadrillion amplitudes,
~3 minutes to collect enough samples from D,
>10,000 yrs to generate similar samples classically?
IBM hits back that they could classically spoof Google's results in only 2.5 days—albeit, using Summit, the largest supercomputer on earth (+they didn't actually do it)
Debate about classical spoofing rages on

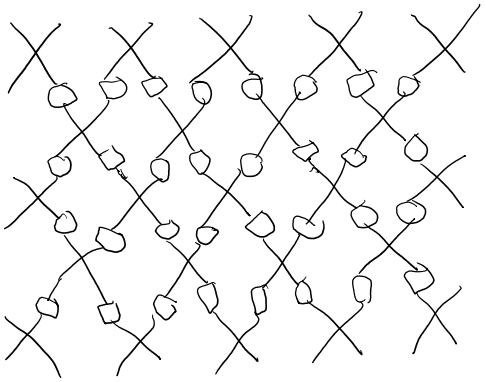
2020 USTC, in China, reports a demonstration of BOSON SAMPLING with 50-70 photons

2021 USTC reports improved BOSON SAMPLING demo with ~110 photons, + sampling-based quantum supremacy using superconducting circuits (like Google's) with 56 qubits, & just last night 60 qubits

Skeptics continue trying to poke holes.

arXiv:2109.03494

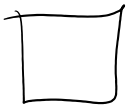
WHAT EXACTLY DID GOOGLE & USTC DO?



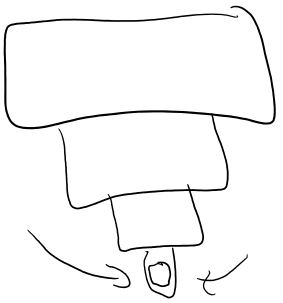
X - superconducting qubits

O - controllable 2-qubit couplings

On a normal-looking computer chip:



But placed in a dilution refrigerator:



& cooled to ~0.01 K, which lets the qubits behave as qubits for a few 10s of microseconds.

A quantum circuit C (i.e. sequence of couplings) is chosen randomly (with depth = 20-24)

is chosen <u>randomly</u> (with depth = $20 \cdot 2^n$)

Over and over, we:

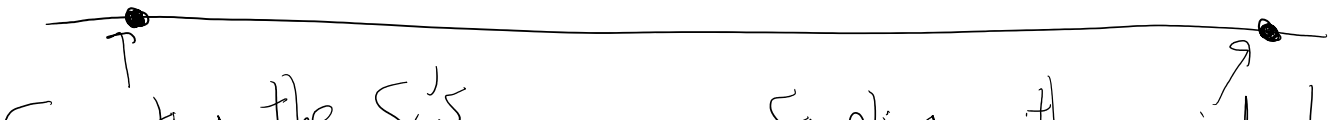
- Initialize all n qubits to the state $|0\rangle$
- Apply C to them
- Measure all qubits in the $\{|0\rangle, |1\rangle\}$ basis to get a <u>sample</u>, $s_i \in \{0,1\}^n$.

After a few minutes we have $s_1, \ldots, s_k$ for $k =$ a few million!

But how do we check whether $s_1, \ldots, s_k$ were actually sampled from $\mathcal{D}$ — whether a QC was even used at all?

Using many classical computers + knowledge of C + as much time as needed, we calculate the Linear Cross-Entropy Benchmark:

$$\text{LXEB} = \frac{2^n}{k} \sum_{i=1}^{k} |\langle 0^n | C | s_i \rangle|^2$$



Generating the S_i's uniformly at random would yield LXEB ≈ 1

Sampling with an ideal QC would yield LXEB ≈ 2, due to quantum interference boosting the probabilities of some S_i's over others

$\frac{0.5}{2^n}$ $\frac{1.6}{2^n}$ $\frac{3}{2^n}$

Google's Result: LXEB ≈ 1.002

USTC's: LXEB ≈ 1.0005

Would achieving similar LXEB scores via a classical algorithm require exp(n) time?

We're not sure (we're not even sure that P≠PSPACE...), but plausibly!

Hardness Reduction (A.-Gunn 2019): Any better-than-brute-force classical algorithm to spoof samples $S_1, \ldots, S_K$ with LXEB $= 1+\eta$, $\eta > 0$, could be turned into such an algorithm

to estimate $|\langle 0^n|C|0^n\rangle|^2$ for a random quantum circuit C with nontrivial variance.

FAQ

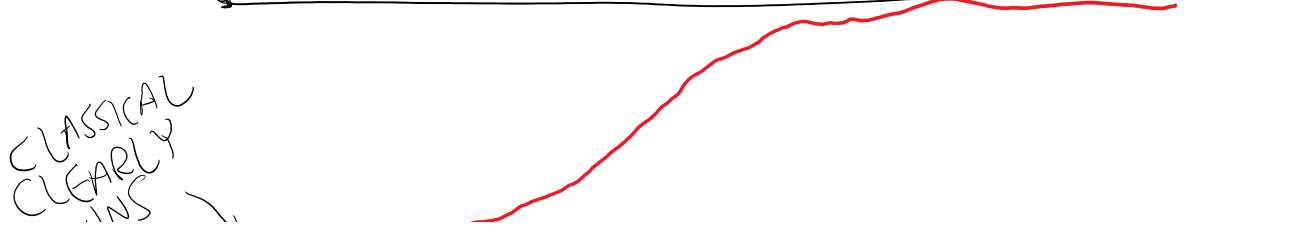
So is this quantum supremadvantage?

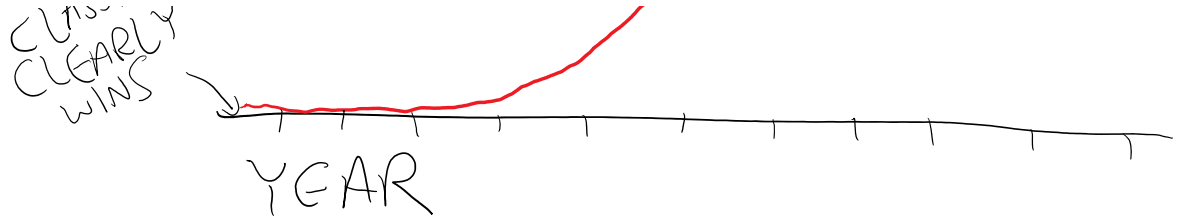
Not yet clear! People continue to design better classical spoofing algorithms. So far, though, they take days on a supercomputer, or produce too-low LXEB scores, or can be defeated by checking that the s_i's are not too similar.

At the same time, the experiments are rapidly improving!

Don't think of quantum supremacy as a single event, like landing on the moon. Think of it as:

QUANTUM CLEARLY WINS ON THESE SAMPLING TASKS





Is the quantum speedup scalable?

No, not yet! Without error-correction & fault-tolerance, the LXEB score will fall like $1 + \frac{1}{\exp(n)}$, which classical algs. can ultimately spoof in poly(n) time. What's been demonstrated is that interference among 2^{50}-2^{60} amplitudes can be harnessed for fast computation!

Are quantum speedups USEFUL yet?

Probably not! Most applications (code-breaking, Grover search...) REQUIRE error-correction & fault-tolerance. Some hope to eke out a near-term advantage for e.g. quantum simulation with little or

no error-correction. But claims that we know how to get near-term speedups for optimization, machine learning, etc. are ~95% BS!

A 2018: Could we repurpose the current sampling-based quantum supremacy experiments as sources of cryptographically certified random bits — e.g., for proof of stake cryptocurrencies?

Where to go next?

- Higher fidelity / LXEB!
- Near-term quantum supremacy experiments whose results are easy to check classically
- Better complexity-theoretic evidence for classical hardness
- Applications, e.g. to simulation, cryptocurrencies?
- Of course, error-correction to enable truly scalable quantum speedups!

THANK YOU