Towards Putting Quantum Supremacy on a Rigorous Footing

Umesh V. Vazirani

U. C. Berkeley

Google Nov 2019: Announcement of ”Quantum supremacy” based on 52 qubits circuit of depth ~20, with gate fidelity ~ .99

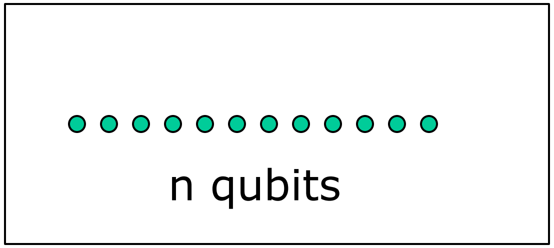
USTC Dec 2020: Boson sampling experiment led by Jian-Wei Pan and Chao-Yang Lu -- ~ 76 qubits

Theoretical Roots and Justification

- BV'93 Quantum computers violate the Extended Church-Turing Thesis

The Quantum Veil

The classical description of the state of n qubits requires 2^n complex numbers.



$$\text{State} = \sum_x \alpha_x |x\rangle$$

The Quantum Veil

Even though the classical description of the state of n qubits requires 2^n complex numbers, can get at most n classical bits of information about the state through a measurement – Holevo's theorem.

State $= \sum_x \alpha_x |x\rangle$

Computational probes: peering behind the Quantum Veil

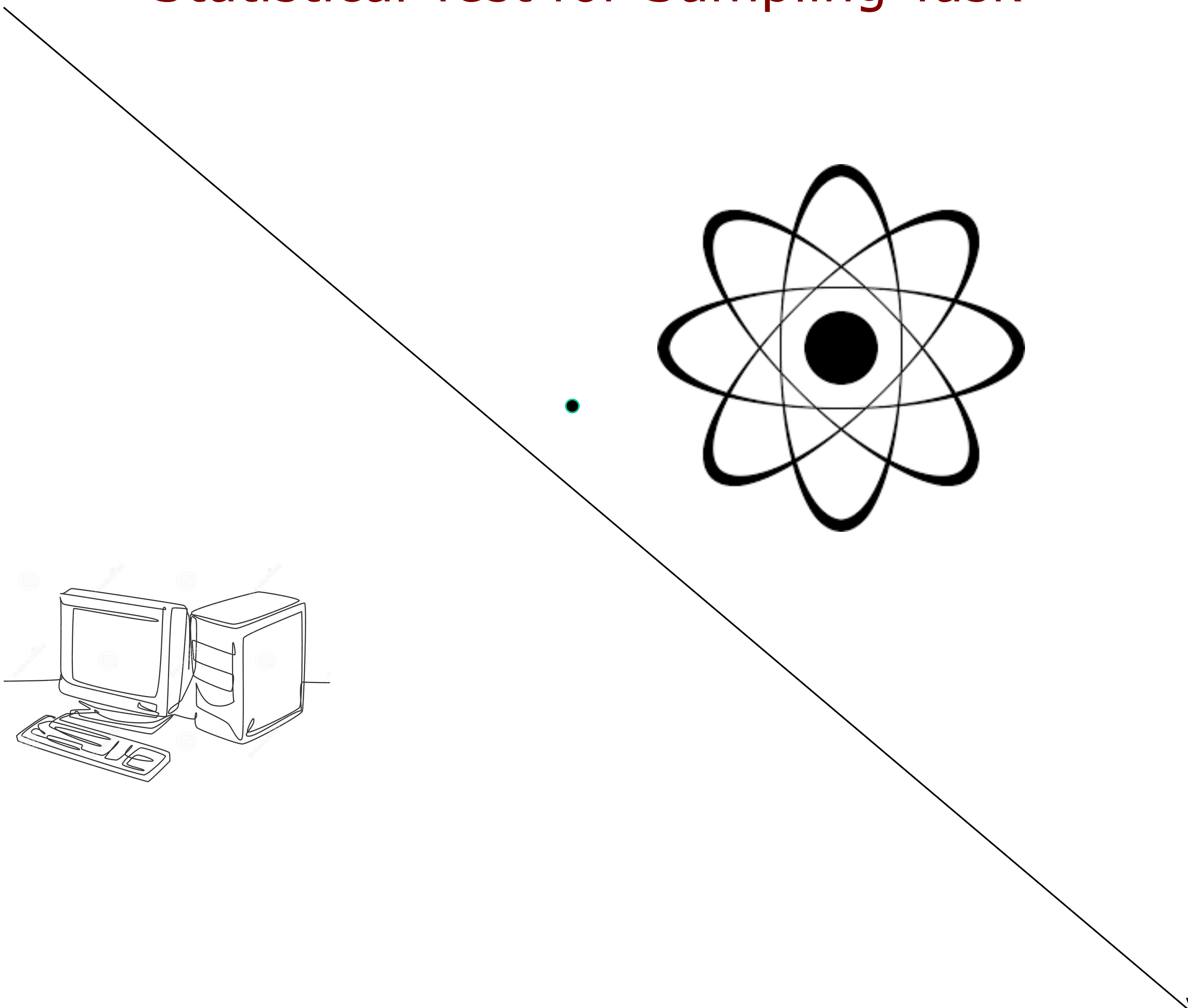
For example, one might naively argue that it is impossible to experimentally verify the exponentially large size of the Hilbert space associated with a discrete quantum system, since any observation leads to a collapse of its superposition. However, an experiment demonstrating the exponential speedup offered by quantum computation over classical computation would establish that something like the exponentially large Hilbert space must exist.

-BV 97

Theoretical Roots and Justification

- BV'93 Quantum computers violate the Extended Church-Turing Thesis
- Quantum supremacy = experimental violation of ECT
- Shor'94 Factoring algorithm – easy to check
- Sampling tasks as basis for quantum supremacy:
  Boson Sampling [Aaronson, Arkhipov '11] and
  IQP [Brebner, Jozsa, Shepherd '11]

Statistical Test for Sampling Task



Sampling Tasks

Probability distributions generated by quantum circuits look very different from those generated by classical circuits

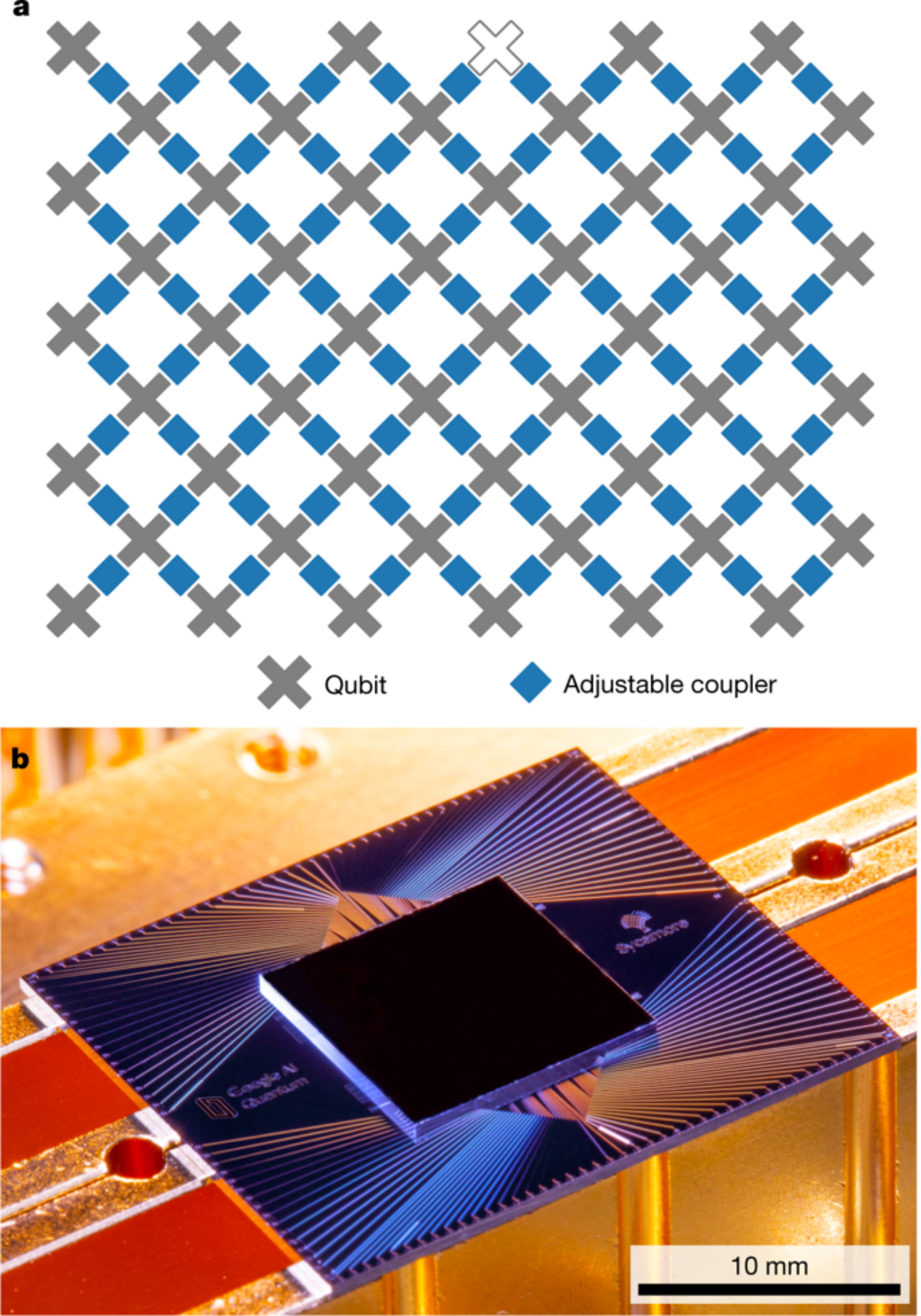
[BV'93] BQP $\subseteq$ GapP

Quantum circuit C on input 0^n Output = sample from distribution

Feynman path integral: constructive and destructive interference across exponentially many paths:
$P[x] = (a_+ - a_-)^2$ where a_+ and a_- can each be very large

Probabilistic circuit: computing $P_C[x]$ in #P
Quantum circuit: computing $P_C[x]$ Gap-P hard for worst case C

[AA'11, BJS'11] Suppose classical computer can sample from output distribution. Then Stockmeyer implies can approximate $P_C[x]$ in Polynomial Hierarchy (PH).



Fix a random circuit C --- i.e. a random sequence of gates of depth ~ 20

Initialize each qubit to 0

Measure the qubits to get a random 52 bit string x sampled according to some distribution.

Use supercomputer to compute
$P_C(x)$ = P[C outputs x on input 0^n]

Check whether sampled x's are consistent with $P_C(x)$

Two Challenges:

- Statistical test to check whether sampled x's consistent with $P_C(x)$
- How do we know that approximating $P_C(x)$ for a **random** quantum circuit C is hard?

And therefore by Stockmeyer sampling from any distribution with constant TVD from P_C is hard

How do we know that approximating $P_C(x)$ for a **random** quantum circuit C is hard?

- Worst-case to average case reduction.

- Model random quantum circuit as a Haar random unitary on n qubits.

- Model reduction after Lipton’s permanent reduction
  $A(t) = X + tR$
  Perm(A(t)) is a degree n polynomial in t.
  Perm(A(0)) = Perm(X)

  [Bouland, Fefferman, Nirkhe, V Nature Physics 2019]

Worst case to Average case ingredients

- Output probability $P_C(x)$ of a quantum circuit with m gates is a polynomial of degree 2m:

$$\langle 0^n|C|0^n\rangle = \sum_{y_2,y_3,\ldots,y_m\in\{0,1\}^n} \langle 0^n|C_m|y_m\rangle\langle y_m|C_{m-1}|y_{m-1}\rangle \ldots \langle y_2|C_1|0^n\rangle$$

- Cannot just take C + tR for random quantum circuit R because C+tR is not unitary

- Attempt 1:
  Choose and fix $\{H_i\}_{i\in[m]}$ Haar random gates

Consider $C' = C'_m C'_{m-1} \ldots C'_1$ so that for each gate $C'_i = C_i H_i$

C' random quantum circuit: each gate in C' is completely random

Problem: no univariate polynomial structure connects worst-case circuit C with the new circuit C' !

Worst case to Average case ingredients

- Output probability $P_C(x)$ of a quantum circuit with m gates is a polynomial of degree 2m:

$$\langle 0^n|C|0^n\rangle = \sum_{y_2,y_3,\dots,y_m\in\{0,1\}^n} \langle 0^n|C_m|y_m\rangle\langle y_m|C_{m-1}|y_{m-1}\rangle \dots \langle y_2|C_1|0^n\rangle$$

- Cannot just take C + tR for random quantum circuit R because C+tR is not unitary

- Attempt 2:

Main idea: "Implement tiny fraction of H_i^{-1}"

i.e., $C_i' = C_i H_i e^{-ih_i\theta}$

If $\theta = 1$ the corresponding circuit $C' = C$, and if $\theta \approx small$, each gate is close to Haar random

Now take several non-zero but small θ and apply polynomial extrapolation (as per Lipton's proof)

Worst case to Average case ingredients

- Attempt 2:

Main idea: "Implement tiny fraction of H_i^{-1}"

i.e., $C_i' = C_i H_i e^{-ih_i\theta}$

If $\theta = 1$ the corresponding circuit $C' = C$, and if $\theta \approx\ small$, each gate is close to Haar random

Now take several non-zero but small θ and apply polynomial extrapolation (as per Lipton's proof)

- *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 $q(1) = p_0(C)$

- [Movassagh '19,'20] gives a "Cayley path" interpolation between the worst-case and random quantum circuit, which stays unitary throughout

[Bouland, Fefferman, Landau, Liu & Kondo, Mori, Movassagh FOCS21]

m = #gates in quantum circuit

Given $O(m^2)$ noisy evaluation points $\{(\theta_i, y_i)\}$ to a polynomial q(θ) of degree m where:

1. θ_i are equally spaced in the interval $[0, \beta = 1/\text{m}]$
2. ***at least*** *2/3* of y_i are ***δ-close*** to $q(\theta_i)$

can use **NP** oracle to output z:

$|z - q(1)| \leq \delta 2^{O(m \log \beta^{-1})} = \delta 2^{O(m \log m)}$ whp

Improved from $\delta 2^{O(m\beta^{-1})}$

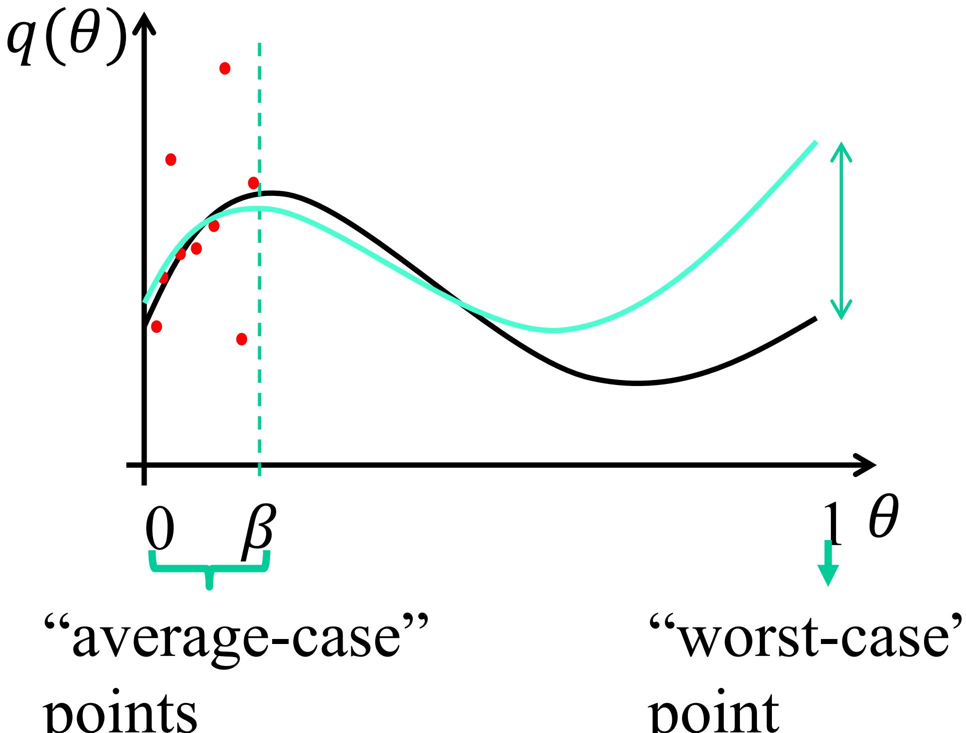
Want $\delta 2^{O(n)}$ so $\delta \sim 2^{-n}$

Idea: substitute $\theta = x^k$.

Endpoints 0,1 unchanged

$\beta \rightarrow \beta^{1/k}$ and m → mk

Choose k = log m



[Bouland, Fefferman, Landau, Liu & Kondo, Mori, Movassagh FOCS21]

m = #gates in quantum circuit

Given $O(m^2)$ noisy evaluation points $\{(\theta_i, y_i)\}$ to a polynomial q(θ) of degree m where:

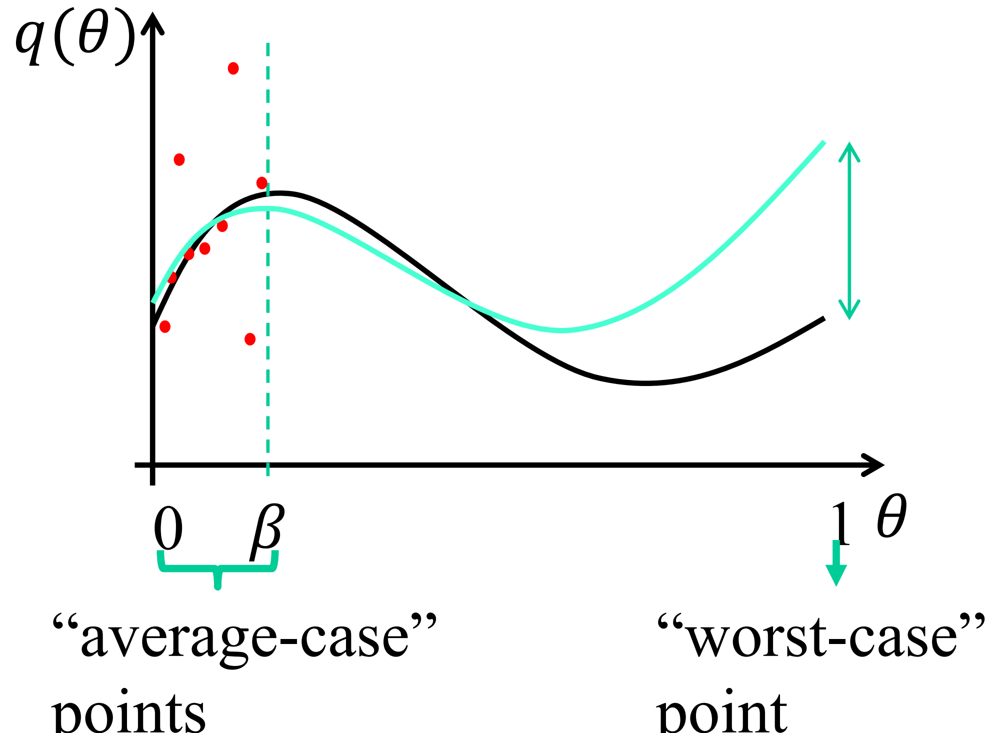
1. θ_i are equally spaced in the interval $[0, \beta = 1/\mathrm{m}]$
2. ***at least*** *2/3* of y_i are ***δ-close*** to $q(\theta_i)$

can use **NP** oracle to output z:

$|z - q(1)| \leq \delta 2^{O(m \log \beta^{-1})} = \delta 2^{O(m \log m)}$ whp

For Boson Sampling,
n Bosons, n^2 modes
Degree of polynomial = n
Dimension of Hilbert space = n^2+n-1 choose n ~ $2^{n\log n}$

So want $\delta \sim 2^{-n\log n}$



Statistical test to check whether sampled x's consistent with $P_C(x)$

Linear cross entropy $E[P_C(x)]$

Intuition: Higher probability x's ($P_C(x)$ large) should show up more often.

Exponential distribution $P(x) = a/2^n \sim \exp(-a)$

For a random quantum circuit C, $E[P_C(x)] = 2/2^n$

For reference, if C outputs uniformly random string

$$E[P_C(x)] = 1/2^n$$

Estimate $E[P_C(x)]$ from samples x_1, x_2, … output by circuit

Google's experiment gave estimates of $1.002/2^n$

Heavy Output Generation

[Aaronson, Chen '17]
HOG: Given random quantum circuit C, generate $x_1, \ldots x_k$ such that at least 2/3 fraction have $P_C(x_i)$ larger than the median probability.

[Aaronson, Gunn '19]
XHOG: Given random quantum circuit C, generate $x_1, \ldots x_k$ such that the average of $P_C(x_i)$ is at least $(1+b)2^{-n}$, where b is 1/poly(n)

Xquath: There is no polynomial time algorithm that on input a random quantum circuit C produces an estimate for $p_0 = P_C(0^n)$ such that
$E_C[(p-p_0)^2] < E[(2^{-n} - p_0)^2] - 3^{-n}$

Xquath implies XHOG. Use hiding to switch 0^n to r, then appeal to Markov.

Discussion

- n = # qubits versus m = # gates for random circuit sampling.
  Robustness of worst case to average case reduction: $\delta 2^{O(m \log m)}$
  Estimate for linear cross entropy for Xquath

- Cryptographic schemes for proofs of quantumness