Mathematical aspects of Google's quantum supremacy experiment

Ion Nechita (CNRS, LPT Toulouse)

GT Info Quantique, January 26th, 2021

Talk outline

Quantum supremacy

Google's experiment

Random quantum circuits

Random circuit sampling

Verifying the output

Classical hardness

Quantum supremacy

The quest for quantum supremacy

- Simulating classically physics (and chemistry) is hard due to the exponential complexity of quantum phenomena $\dim(\mathbb{C}^2)^{\otimes n} = 2^n$
- Feynman suggested that a quantum computer would be an effective tool for such problems [Fey82]
- Quantum supremacy, introduced by Preskill [Pre12]:

  "The day when well controlled quantum systems can perform tasks surpassing what can be done in the classical world"

- What is needed to achieve it:
  1. A mathematical specification of a computational problem with a well defined solution
  2. A high-fidelity programmable computational device able to perform the task
  3. A scaling runtime difference between the quantum and classical computational processes that can be made large enough as a function of problem size so that it becomes impractical for a supercomputer to solve the task using any known classical algorithm

Quantum supremacy — so what???

1. Experimental evidence against the Extended Church-Turing thesis
   - The Church-Turing thesis: any behavior of a real-world physical system can be simulated on a probabilistic Turing machine
   - The Extended Church-Turing thesis [BV97]: any behavior of a real-world physical system can be simulated on a probabilistic Turing machine using computational resources polynomial in the size of the system
   - Theoretical evidence against the Extended Church-Turing thesis: Shor's algorithm:

$$(\textsc{Factoring} \notin \mathrm{P} \implies) \qquad \mathrm{BQP} \neq \mathrm{P}$$

2. Certified randomness
3. Silence quantum computing skeptics 😂

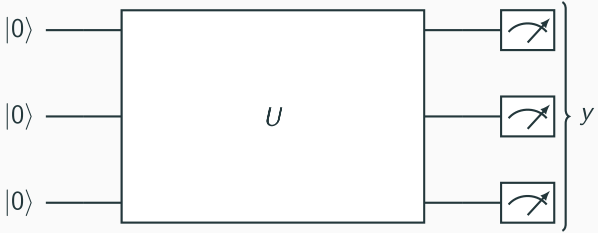
Google's experiment

The computational task

RCS : Sampling from a random quantum circuit

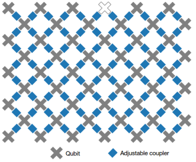
1. Let n be a given number of qubits
2. Choose a random quantum circuit C on n qubits, corresponding to a Haar-distributed random unitary matrix $U \in \mathcal{U}(2^n)$
3. Sample from the output distribution P_U:

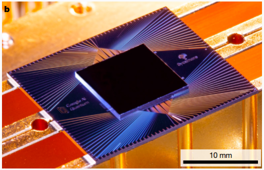
$$P_U(y) = |\langle y|U|0\rangle|^2 \qquad \forall y \in \{0,1\}^n$$



The experiment [A+19]

- "We designed a quantum processor named 'Sycamore' which consists of a two-dimensional array of 54 transmon qubits, where each qubit is tunably coupled to four nearest neighbors, in a rectangular lattice. [...] One qubit did not function properly, so the device uses 53 qubits and 86 couplers"



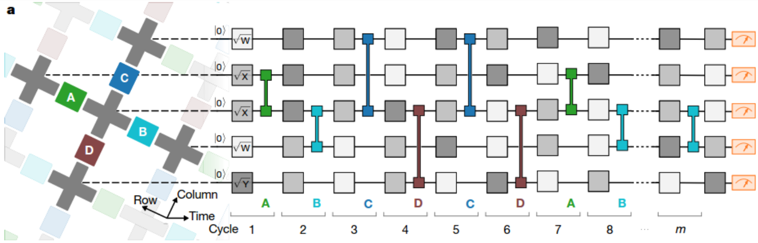


- "Our largest random quantum circuits have 53 qubits, 1,113 single-qubit gates, 430 two-qubit gates, and a measurement on each qubit, for which we predict a total fidelity of 0.2%"
- "For the largest circuit with 53 qubits and 20 cycles, we collected $N_s = 30 \cdot 10^6$ samples over ten circuit instances. [...] We have archived the data"
- "The data is thus in the quantum supremacy regime"

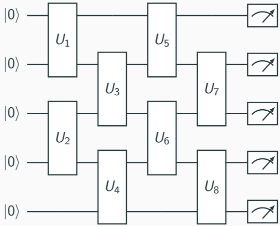
Random quantum circuits

Pseudo-random unitary circuits

- We want: Haar-distributed $U \in \mathcal{U}(2^n)$
- What Google has:



- Random unitary circuit model: 2D version of



, where $U_i \in \mathcal{U}(4)$ are i.i.d. Haar

Approximating the Haar measure

Definition

A probability measure μ on $\mathcal{U}(N)$ is called a k-design [DCEL09] if it agrees with the Haar measure for moments up to k:

$$\forall a, b, c, d \in [N]^k, \qquad \mathbb{E}_\mu[U_{a_1 b_1} \cdots U_{a_k b_k} \bar{U}_{c_1 d_1} \cdots \bar{U}_{c_k d_k}] = \mathbb{E}_{\mathrm{Haar}}[\cdots]$$

Equivalently [CŚ06]

$$\mathbb{E}_\mu[U^{\otimes k} \otimes (U^*)^{\otimes k}] = \mathbb{E}_{\mathrm{Haar}}[U^{\otimes k} \otimes (U^*)^{\otimes k}] = \sum_{\alpha,\beta \in \mathcal{S}_k} P_{\alpha,\beta} \mathrm{Wg}_N(\alpha, \beta)$$

Example

The Weyl unitaries $W_{xy} = U^x V^y$, with $U|k\rangle = |k+1\rangle$ and $V|k\rangle = \omega^k |k\rangle$, $\omega = \exp(2\pi \mathrm{i}/N)$ form a 1-design

Theorem ([BHH16, HM18])

Random circuits on n qubits in D dimension of depth T become approximate k-designs when

$$T \gtrsim n^{1/D} k^{O(1)}$$

Random circuit sampling

Porter-Thomas distribution

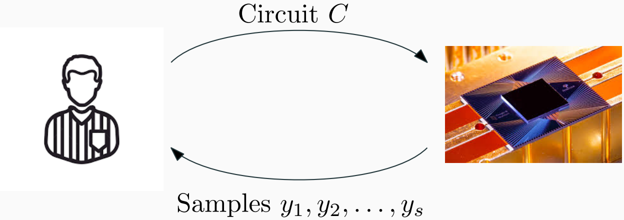
- RCS: given a description of a random circuit C, sample output bit-strings $y \in \{0,1\}^n$, with probabilities $P_C(y) = |\langle y|U_C|0\rangle|^2$
- U is (approx.) Haar distributed, so $z = U|0\rangle$ is distributed uniformly on the unit sphere of $\mathbb{C}^N$
- What is the distribution of the squared amplitudes $|z_i|^2$?
- If g is a standard complex Gaussian vector, $z \overset{\text{law}}{=} g/\|g\|$
- Fact: $(|z_i|^2)_{i\in[N]}$ and $\|g\|^2$ are independent random variables
- $\|g\|^2$ is χ^2 distributed as a sum of squared Gaussians
- We have

$$\mathbb{E}_U|z_i|^{2k} = \frac{k!}{N(N+1)\cdots(N+k-1)} \sim \frac{k!}{N^k}$$

- As $N \to \infty$, for all i, $|z_i|^2$ is close the distribution with density $N\exp(-Nx)$, the Porter-Thomas distribution
- Note that the probabilities fluctuate exponentially on the scale $1/N$, so the distribution is far from "flat" [RSK20]

Verifying the output

How it's done



- The verifier (i.e. Google!) uses the linear cross entropy benchmark (LXEB):

$$\text{Is } \sum_{i=1}^{s} P_C(y_i) = \sum_{i=1}^{s} |\langle y_i|C|0\rangle|^2 \geq \frac{bs}{2^n} \text{ for some } b > 1 + \varepsilon \,?$$

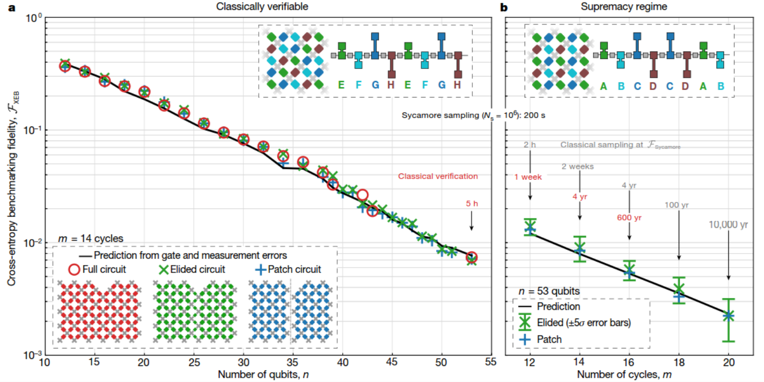
- Uniform guessing: $b = 1$
- Perfect quantum computer:

$$b = \int_0^\infty x \cdot xe^{-x}\,\mathrm{d}x = 2$$

- Google reports $b = 1.002 \rightsquigarrow$ quantum supremacy

Verifier's job

- The (classical) verifier needs to compute $P_C(y_i) = \sum_{i=1}^{s} |\langle y_i|C|0\rangle|^2$



- The best classical algorithms for computing output probabilities are a mixture of the Schrödinger method (evolving the full state vector, fast, but exp. memory use ⇝ IBM's speedup claim) and the Feynman method (contracting the tensor network in an efficient way; finding optimal contraction is hard)

Classical hardness

"Evidence" for classical hardness

- Let $\textsc{ExactSampBPP}$ be the class of sampling problems: given a family of prob. distributions $\{D_x\}_{x\in\{0,1\}^n}$, produce a sample in poly time using a randomized classical alg.; same for $\textsc{ExactSampBQP}$

Theorem

If $\textsc{ExactSampBPP} = \textsc{ExactSampBQP}$, *then* PH *collapses*

- Idea: equality would imply $\mathrm{BPP}^{\mathrm{NP}} = \mathrm{P}^{\#\mathrm{P}}$ [AA11, BFNV18, BIS+18, Mov19]
- Same definition for $\textsc{ApproxSampBPP}$ but allowing for an error ε in total variation and requiring poly-time in n and $1/\varepsilon$

Conjecture

If $\textsc{ApproxSampBPP} = \textsc{ApproxSampBQP}$, *then* PH *collapses*

Conjecture

There is no poly-time classical algorithm which can pass the LXEB $\sum_{i=1}^{s} |\langle y_i|C|0\rangle|^2 \geq \frac{bs}{2^n}$ *for* $b \geq 1+\varepsilon$

Take-home slide: Google's supremacy computational task

A suitable computational task

To demonstrate quantum supremacy, we compare our quantum processor against state-of-the-art classical computers in the task of sampling the output of a pseudo-random quantum circuit[11,13,14]. Random circuits are a suitable choice for benchmarking because they do not possess structure and therefore allow for limited guarantees of computational hardness[10–12]. We design the circuits to entangle a set of quantum bits (qubits) by repeated application of single-qubit and two-qubit logical operations. Sampling the quantum circuit's output produces a set of bitstrings, for example {0000101, 1011100, …}. Owing to quantum interference, the probability distribution of the bitstrings resembles a speckled intensity pattern produced by light interference in laser scatter, such that some bitstrings are much more likely to occur than others. Classically computing this probability distribution becomes exponentially more difficult as the number of qubits (width) and number of gate cycles (depth) grow.

References

[A+19] Frank Arute et al.
Quantum supremacy using a programmable superconducting processor.
Nature, 574:505–510, 2019.

[AA11] Scott Aaronson and Alex Arkhipov.
The computational complexity of linear optics.
In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[BFNV18] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani.
Quantum supremacy and the complexity of random circuit sampling.
arXiv preprint arXiv:1803.04402, 2018.

[BHH16] Fernando GSL Brandão, Aram W Harrow, and Michał Horodecki.
Local random quantum circuits are approximate polynomial-designs.
Communications in Mathematical Physics, 346(2):397–434, 2016.

[BIS+18] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J Bremner, John M Martinis, and Hartmut Neven.
Characterizing quantum supremacy in near-term devices.
Nature Physics, 14(6):595, 2018.

[BV97] Ethan Bernstein and Umesh Vazirani.
Quantum complexity theory.
SIAM Journal on computing, 26(5):1411–1473, 1997.

[CŚ06] Benoît Collins and Piotr Śniady.
Integration with respect to the haar measure on unitary, orthogonal and symplectic group.
Communications in Mathematical Physics, 264(3):773–795, 2006.

[DCEL09] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine.
Exact and approximate unitary 2-designs and their application to fidelity estimation.
Physical Review A, 80(1):012304, 2009.

[Fey82] Richard P Feynman.
Simulating physics with computers.
Int. J. Theor. Phys, 21(6/7), 1982.

[HM18] Aram Harrow and Saeed Mehraban.
Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates.
arXiv preprint arXiv:1809.06957, 2018.

[Mov19] Ramis Movassagh.
Quantum supremacy and random circuits.
arXiv preprint arXiv:1909.06210, 2019.

[Pre12] John Preskill.
Quantum computing and the entanglement frontier.
Rapporteur talk at the 25th Solvay Conference on Physics, Brussels, 2012.

[RSK20] Yosef Rinott, Tomer Shoham, and Gil Kalai.
Statistical aspects of the quantum supremacy demonstration.
arXiv preprint arXiv:2008.05177, 2020.