Quantum Supremacy, Random Circuit Sampling, and Their Critiques

Quantum Supremacy / Advantage

Quantum supremacy (or advantage):

A quantum device performs a well-defined computational task that is infeasible for any classical computer. Experimental violation of the extended Church-Turing theses.

Typically:

$$T_Q(n) \ll T_C(n)$$

for the best known algorithms.

Important features of current demonstrations:

- Task need not be practically useful
- Must be precisely specified
- Classical hardness justified by complexity evidence
- Current devices are noisy (NISQ)

Random Circuit Sampling (RCS)

Given a random quantum circuit U on n qubits:

$$p_U(x) = |\langle x|U|0^n\rangle|^2$$

Task: sample $x \in \{0,1\}^n$ according to p_U.

Why this is attractive:

- Requires no structure in input
- Natural output of quantum evolution
- Believed classically hard to simulate
- Feasible on near-term devices
- Google: 52 *qubit circuits* of depth ~ 20; gate fidelity ~ 0.99. Number of qubits large enough for 2^n to be impressive, yet manageable by a classical computer (Goldilock's principle).

Verification Problem

If the distribution is classically intractable:

How can we verify the device is sampling from it?

Cannot compute all probabilities $p_U(x)$.
Instead:

- Compute $p_U(x_i)$ for sampled outputs only. Exponential computation
- Use statistical correlation tests
- Validate on smaller circuits first

Verification is therefore indirect and assumption-based.

Cross-Entropy Benchmarking (XEB)

Given samples $x_1, \ldots, x_m$ estimate $E[P_U(x)]$.
Interpretation:

- $E[P_U(x)] \approx 2/2^n$: expected probability of a heavy outcome ($>$ median) for an ideal (chaotic) device
- $E[P_U(x)] = 1/2^n$ uniform random output
- Intermediate: noisy quantum device. Google's experiment gave estimates of $1.002/2^n$. But the measured departure from uniform was definite.

Relies on Porter–Thomas distribution of probabilities for a random (chaotic)) quantum circuit. $\boxed{P(x) = Ne^{-Nx}, \qquad N = 2^n}$

"Teacup Supremacy" Criticism

Main objection:

The task is artificial and has no practical value.

Analogy:

A teacup "outperforms" a supercomputer at shattering into pieces.

Concerns:

- Problem engineered for quantum hardware
- No useful output
- *Classical algorithms may catch up.* [Not for this problem though]
- Verification is indirect

Kalai's Noise-Based Critique

Claim: Noise may destroy computational hardness.

Ideal state:

$$|\psi\rangle = U|0^n\rangle$$

System plus environment picture:

$$|\psi_{\mathrm{SE}}\rangle = V\big(U|0^n\rangle \otimes |e_0\rangle\big)$$

With sufficient noise, tracing out the environment gives:

$$\text{Output distribution} \approx \text{Uniform}$$

which is classically trivial to sample.

Further Noise Concerns

Kalai and others emphasize:

- Errors accumulate with circuit depth
- Correlated noise may scale with entanglement
- High-order interference terms are suppressed
- Resulting distributions may admit efficient classical descriptions

Supremacy claims therefore depend critically on **how close the device is to the ideal distribution**.

BFNV: Complexity of Random Circuit Sampling

Bouland, Fefferman, Nirkhe, Vazirani (2018):

Show that computing output probabilities of *typical* random circuits is as hard as worst case.

Key ingredients:

- Average-case $\#P$-hardness of amplitudes
- Anti-concentration of output distribution
- Polynomial structure of amplitudes

Provides strong evidence that ideal RCS is classically hard.

From Probability Computation to Sampling Hardness

To conclude classical sampling is hard, additional assumptions are needed:

- Average-case relative-error hardness
- No collapse of the Polynomial Hierarchy (PH)
- Ability to approximate probabilities implies solving $\#P$ problems

Thus supremacy claims are conditional, not absolute.

Effect of Noise on RCS Hardness

BFNV results apply to *ideal* or near-ideal distributions.

In realistic devices:

- Noise may move distribution toward uniform
- Hardness reductions may no longer apply
- Classical simulation may become feasible

Recent work shows polynomial-time classical algorithms for sufficiently noisy circuits.

Verification vs Complexity Evidence

Key distinction:

Complexity evidence:
Ideal distribution is hard to sample.

Experimental verification:
Device produces outputs statistically consistent with it.

There is no proof that the experimental distribution remains hard.

Why Cryptography Gives a Cleaner Advantage

Breaking RSA/ECC using Shor's algorithm would yield:

- Immediate real-world impact
- Unambiguous success criterion
- Compact inputs and outputs
- Easy verification

Either the key is recovered or it is not.

No statistical testing required.

Post-Quantum Cryptography (PQC)

PQC is defensive:

Design classical schemes secure against quantum attacks.

Not a use of quantum power, but a response to it.

However, successful quantum cryptanalysis would be a clear demonstration of quantum advantage.

Overall Picture

Random Circuit Sampling:

- Strong theoretical evidence of hardness (BFNV)
- Feasible on near-term devices
- Hard to verify rigorously
- Sensitive to noise

Cryptographic breaking:

- Requires fault-tolerant quantum computers
- Clean, decisive notion of advantage
- Immediate practical consequences

Conclusion

Quantum supremacy experiments demonstrate:

- Control of large quantum systems
- Evidence of computational regimes beyond classical reach
- But rely on assumptions about noise and complexity

Future large-scale quantum computers may establish advantage more decisively on practical problems.