“Quantum Supremacy” and the Complexity of Random Circuit Sampling

Adam Bouland*, Bill Fefferman†, Chinmay Nirkhe* and Umesh Vazirani*

*Electrical Engineering and Computer Sciences, University of California, Berkeley
†Joint Center for Quantum Information and Computer Science (QuICS), University of Maryland/NIST

Quantum supremacy

- Quantum supremacy is a demonstration of any quantum computation that is prohibitively hard for classical computers.
- It is both a necessary milestone on the path to useful quantum computers as well as a test of quantum theory in the realm of high complexity.
- A physical refutation of the extended Church-Turing thesis.

How did we get here?

- Complexity theoretic results of the 90’s (e.g. Bernstein-Vazirani, Simon, and Shor) give evidence (oracle separation) of the power of quantum computers over classical.
- Sampling-problems are proposed as tasks for quantum supremacy such as BosonSampling [1] and IQP [3].
- It is designed so that it can be estimated with a few samples from an output distribution close to $D$, and
- Experimentally difficult to verify.
- Vast improvements are made in “noisy intermediate-scale quantum” (NISQ) devices [5] especially in the realm of superconducting qubits [2].
- Google/UCSB proposes the ‘Random Circuit Sampling’ problem as the task with which they will demonstrate supremacy [4].

This leads to a need for complexity-theoretic evidence for the Random Circuit Sampling tasks.

Random Circuit Sampling

$|0\rangle$ $\rightarrow$ $|0\rangle$ $\rightarrow$ $|0\rangle$ $\rightarrow$ $|0\rangle$

Random Circuit Sampling task: Given a circuit $C$ from the architecture, sample from a distribution close to the distribution induced by $C$:
$$\Pr(y) = \langle |y| C|0\rangle^2; \text{ for } y \in \{0,1\}^n.$$

Requirements for a proposal

The computational task is to sample from the output distribution $D$ of some experimentally feasible quantum process or algorithm. To establish quantum supremacy, we must show

- **Hardness**: No efficient classical algorithm can sample from any distribution close to $D$, and
- **Verification**: an algorithm can check that the experimental device sampled from a distribution close to $D$.

Average-case hardness

Verification imposes a robustness condition of the difficulty of sampling. In any reasonable noise model, a single outcome $x$ has exponentially small occurrence probability $D(x)$ (a #P-hard quantity) — therefore, is extremely difficult to verify. Any convincing proof of supremacy must establish that $D$ is actually uniformly difficult to sample from. This is a worst-to-average-case reduction.

Theorem 1 (Simplified)

It is #P-hard to compute $\|\{0\}|C|0\rangle^2$ with probability $> 0.76$ over the choice of $C$, where $C'$ is drawn from any one of a family of discretizations of the Haar measure.

Establishing Verification

- The leading statistical measure proposed for verification is the “cross-entropy” [2]
  $$\sum p_{D|x}(x) \log \frac{1}{p_D(x)}.$$
- It is designed so that it can be estimated with a few samples $x_1, \ldots, x_k$ and computing the average value $\mathbb{E}_x \log (1/p_D(x))$ using a classical supercomputer.
- Without assumptions as to how the quantum device operates, cross-entropy does not certify closeness in total variation distance.
- However, there is a natural assumption under which cross-entropy measure certifies closeness in total variation distance.

Theorem 2. If $H(p_{D|x}) > H(p_C)$, then achieving a cross-entropy score $\epsilon$-close to ideal implies that $||p_{D|x} - p_C|| \leq \epsilon/2$.

Proof. Pinsker’s inequality.

The leading proposals

<table>
<thead>
<tr>
<th>Proposal</th>
<th>Worst-case hardness</th>
<th>Exact average-case hardness</th>
<th>Approximate average-case hardness</th>
<th>Anti-concentration</th>
<th>Frame experiment?</th>
</tr>
</thead>
<tbody>
<tr>
<td>BosonSampling</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FourierSampling</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IQP</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Random Circuit Sampling</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

References