What is the biggest possible gap between quantum and classical computing?

Scott Aaronson (MIT)
Andris Ambainis (U. of Latvia)
Query model

- Function $f(x_1, ..., x_N)$, $x_i \in \{0,1\}$.
- $x_i$ given by a black box:

Complexity = number of queries
Quantum query model

\[ |\psi_{\text{start}}\rangle \rightarrow U_0 \rightarrow Q \rightarrow U_1 \rightarrow \ldots \rightarrow Q \rightarrow U_T \]

- Q – queries:
  \[ \sum_i a_i|i\rangle \rightarrow \sum_i a_i (-1)^{x_i} |i\rangle \]

- \(U_0, U_1, \ldots, U_T\) – independent of \(x_1, \ldots, x_N\).
Reasons to study query model

- Encompasses many quantum algorithms (Grover’s search, quantum part of factoring, etc.).
- Provable quantum-vs-classical gaps.
1 query quantumly

How many queries classically?
Period finding

$x_1, x_2, \ldots, x_N$ - periodic

Find period $r$

1 query quantumly

Quantum part of Shor’s factoring algorithm
How many queries classically?

- Quantum algorithm works if $N \geq r^2$.
- $T$ classical queries – can test $T^2$ possible periods.

$\frac{4}{\sqrt[4]{N}}$ queries classically
Our result [Aaronson, A]

- Task that requires 1 query quantumly, $\Theta(\sqrt{N})$ classically.
- Method for simulating any 1 query quantum algorithm by $O(\sqrt{N})$ query probabilistic algorithm.
Fourier checking/Forrelation
Forrelation

- Input: \((x_1, \ldots, x_N, y_1, \ldots, y_N) \in \{-1, 1\}^{2N}\).
- Are vectors well correlated one with another?

\[
\begin{pmatrix}
    x_1 \\
    x_2 \\
    \vdots \\
    x_N
\end{pmatrix}
\quad F_N
\quad \begin{pmatrix}
    y_1 \\
    y_2 \\
    \vdots \\
    y_N
\end{pmatrix}
\]

- \(F_N\) – Fourier transform over \(Z_N\).
More precisely...

Is the inner product

\[(\tilde{x}, \ F \tilde{y}) = \frac{1}{N} \sum_{i,j} F_{i,j} x_i y_j\]

at least $3/5$ or at most $1/100$?
Quantum algorithm

1. Generate states

\[ |\Psi_x\rangle = \sum_{i=1}^{N} x_i |i\rangle, \quad |\Psi_y\rangle = \sum_{i=1}^{N} y_i |i\rangle \]

in parallel (1 query).

2. Apply \( F_N \) to 2\(^{nd} \) state.

3. Test if states equal (SWAP test).
Classical lower bound

- **Theorem** Any classical algorithm for FORRELATION uses
  \[ \Omega \left( \frac{\sqrt{N}}{\log N} \right) \] queries.
REAL FORRELATION

- Real-valued vectors

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix} \quad \vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{pmatrix}$$

- Distinguish between
  - $\vec{x}, \vec{y}$ random ($x_i$'s - Gaussian);
  - $\vec{\chi}$ random, $\vec{y} = F_N \vec{\chi}$. 
Proof idea: achieve $x_i \in \{-1, 1\}$ by replacing $x_i \rightarrow \text{sgn}(x_i)$. 
Lower bound

- **Claim**: Solving REAL FORRELATION on most instances requires \( \Omega\left(\frac{\sqrt{N}}{\log N}\right) \) queries.

- **Intuition**: if \( \vec{y} = F_N \vec{x} \), correlations between \( x_i \)'s and \( y_j \)'s - weak.

- \( o(\sqrt{N}) \) values \( x_i \) and \( y_j \) look like uncorrelated random variables.
Simulating 1 query quantum algorithms
Simulation

- **Theorem** Any 1 query quantum algorithm computing $f(x_1, ..., x_N)$ can be simulated probabilistically using $O(\sqrt{N})$ queries.
Analyzing query algorithms

\[ \psi_{\text{start}} \]

\[ \alpha_{1,1}|1,1\rangle + \alpha_{1,2}|1,2\rangle + \ldots + \alpha_{N,M}|N,M\rangle \]

\( \alpha_{1,1} \) is actually \( \alpha_{1,1}(x_1, \ldots, x_N) \)
Lemma [Beals et al., 1998] If is a state after k queries, then $\alpha_{i,j}(x_1, \ldots, x_N)$ are polynomials in $x_1, \ldots, x_N$ of degree $\leq k$.

Measurement:
(i, j) w. probability $|\alpha_{i,j}(x_1, \ldots, x_N)|^2$

Polynomial of degree $\leq 2k$
Our task

- $\Pr[A \text{ outputs 1}] = p(x_1, \ldots, x_N)$, $\deg p = 2$.
- $0 \leq p(x_1, \ldots, x_N) \leq 1$.
- Task: estimate $p(x_1, \ldots, x_N)$ within precision $\varepsilon$.

Solution: random sampling
Pre-processing

- **Problem**: some $x_i$’s in $p(x_1, ..., x_N)$ may be more influential than others.

variable-splitting
Claim: If we sample N out of $N^2$ terms $Y_{i,j} = a_{i,j}x_i x_j$, then

$$\sum_{i,j} Y_{i,j} \quad - \text{good estimate}$$

Problem: requires sampling N variables $x_i$. 

$$p(x_1, x_2, \ldots, x_N) = \sum_{i,j} a_{i,j} x_i x_j$$
Sampling 2

\[ p(x_1, x_2, \ldots, x_N) = \sum_{i,j} a_{i,j} x_i x_j \]

Sampling \( \sqrt{N} \) variables \( x_i \)

\[ \sqrt{N} \cdot \sqrt{N} = N \]
Extension to k queries

- **Theorem** Any k query quantum algorithm can be simulated probabilistically with $O(N^{1-1/2k})$ queries.

- **Proof** Describe algorithm by polynomial of degree $2k$, use random sampling.

- **Question**: Is this optimal?
K-fold forrelation
Forrelation: given black box functions $f(x)$ and $g(y)$, estimate

$$\sum_{x, y} F_{x, y} f(x) g(y)$$

K-fold forrelation: given $f_1(x)$, ..., $f_k(x)$, estimate

$$\sum_{x_1, x_2, \ldots, x_k} f_1(x_1) F_{x_1, x_2} f_2(x_2) F_{x_2, x_3} \ldots f_k(x_k)$$
k-query quantum algorithm

1. Generate $\sum_{x} \frac{1}{\sqrt{N}} |x\rangle$
2. Apply black box for $f_1(x)$;
3. Apply QFT;
4. Apply black box for $f_2(x)$;
5. ....

Creates amplitude equal to

$$\sum_{x_1, \ldots, x_k} f_1(x_1) F_{x_1, x_2} f_2(x_2) F_{x_2, x_3} \cdots f_k(x_k)$$
More results

- **Theorem** k-fold forrelation can be solved with $\lceil k/2 \rceil$ quantum queries.

- **Conjecture** k-fold forrelation requires $\Omega(N^{1-1/k})$ queries classically.

- $\Omega(N^{1-1/k})$ queries = estimating the sum by classical sampling.
Let $k = \text{poly}(n)$ and $f_1(x), \ldots, f_k(x)$ - poly-size quantum circuits.

**Theorem** $k$-fold forrelation is BQP-complete.

Captures the power of BQP!

No Jones polynomial or other advanced notions!
BQP-completeness proof

- Need to show:
  poly-size quantum circuits $\Rightarrow$ k-fold forrelation.

- Hadamard + sign (cc-Z) – universal.

- Transformation:
  - Sign gates $\Rightarrow f_1(x), f_2(x), ..., f_k(x)$;
  - Hadamard $\Rightarrow$ Fourier transform;
1 quantum query algorithms for sampling problems
Fourier sampling

- Black box for $f(x)$, $x \in \{0,1\}^N$.
- Probability distribution: $P[y] = \left(\hat{f}(y)\right)^2$,

$$\hat{f}(y) = \frac{1}{\sqrt{2^N}} \sum_x F_{x,y} f(x).$$

- Task: sample from this distribution.
Quantum algorithm

1. Use 1 query to generate

\[ |\Psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x} f(x) |x\rangle, \]

2. Apply QFT to obtain

\[ |\Psi'\rangle = \sum_{y} \hat{f}(y) |y\rangle, \]

\[ \hat{f}(y) = \frac{1}{\sqrt{2^N}} \sum_{x} F_{x,y} f(x). \]
Classical lower bound

- Theorem Fourier sampling requires $\Omega(N/\log N)$ queries, even for approximate sampling
Summary

- 1 quantum query = $\Theta(\sqrt{N})$ classical queries.
- $k$ quantum queries can be simulated with $O(N^{1-1/2k})$ classical queries.
- Sampling: at least $\Omega(N/\log N)$ classical queries to simulate 1 quantum query.
Open problem 1

- Does $k$-fold FORRELATION require $\Omega(N^{1-1/2k})$ queries classically?
- Plausible but looks quite difficult mathematically.
Open problem 2

- Best quantum-classical gaps:
  - 1 quantum query - $\Omega(\sqrt{N})$ classical queries;
  - 2 quantum queries - $\Omega(\sqrt{N})$ classical queries;
  - ...
  - log $N$ quantum queries - $\Omega\left(\sqrt{N \log N}\right)$ classical queries.

Any problem that requires $O(\log N)$ queries quantumly, $\Omega(N^c)$, $c>1/2$ classically?
Open problem 3

- What else is FORRELATION/k-fold FORRELATION useful for?