Forrelation: A Problem that Optimally Separates Quantum from Classical Computing

Authors: Scott Aaronson & Andris Ambianis (2015)

Manish Kumar

Quantum Tech. (M. Tech) IISc Bengaluru

October 14, 2023

Table of Contents

Table of Contents

Let two Boolean functions $f,\ g : \{0,\ 1\}^n \to \{-1,\ 1\}$. An estimation of the correlation between f and the Fourier transform of g be defined as:

$$\Phi_{f,g} := \frac{1}{2^{3n/2}} \sum_{x,y \in \{0,\ 1\}^n} f(x)(-1)^{x \cdot y} g(y)$$

Promise Problem:

Given Oracle access to Boolean functions f and g, determine if $\Phi_{f,g} \leq t_1$ or $\Phi_{f,g} \geq t_2$, where $t_1, t_2 \in (0, 1)$ is specified before hand.

Quantum and Classical Query Complexity

The (strict) lower bound on Quantum and Classical query complexities are as follows:

Quantum:

One query is sufficient.
Reason: An explicit algorithm exists.

Classical

$\Omega(\frac{\sqrt{N}}{log\ N})$ query required.
Reason: Due to Theorem 1 from the paper.

Theorem 1: Any classical randomised algorithm for FORRELATION must make $\Omega(\frac{\sqrt{N}}{log\ N})$.

BQP completeness of k-fold FORRELATION

Guiding Question

- Classical random sampling could be said to capture the advantage of randomized over deterministic query complexity
- Is there a single problem or technique that captures the advantage of quantum over classical query complexity?

k-fold FORRELATION

It is a generalization of the FORRELATION problem to k different Boolean functions. It is among the hardest problems in (promise)BQP.
Reason: Due to Theorem 5 from the paper

Theorem 5: If $f_1, ..., f_k$ are described explicitly (say, by circuits to compute them), and $k = poly(n)$, then k-fold FORRELATION is a BQP-complete promise problem.

Table of Contents

Key Observation

$\Phi_{f,g} = \langle 0^n|(H^{\otimes n})(U_f)(H^{\otimes n})(U_g)(H^{\otimes n})|0^n\rangle$

Quantum Algorithm:

- **Step I:** Use the oracle to generate the below quantum states as:

$$|\psi_x\rangle = \sum_{n=1}^{N} x_i |i\rangle \ \ and \ \ |\psi_y\rangle = \sum_{n=1}^{N} y_i |i\rangle$$

- **Step II:** Apply QFT to $|\psi_y\rangle$, i.e, $QFT|\psi_y\rangle$
- **Step III:** Use the SWAP test between $|\psi_x\rangle$ and $QFT|\psi_y\rangle$.
- **Step IV:** Match the output of Step III with the condition given in the FORRELATION promise problem

Techniques to prove classical lower bound on FORRELATION

Proof Strategy for Theorem 1

- Reduction: REAL FOORELATION (RF) $\rightarrow$ FORRELATION (F)
- Any query complexity lower bound on RF $\implies$ same lower bound for F

Techniques:

- Benefit of analysis on RF: It is a (real-valued) continuous version of F. Hence, the probabilistic analysis becomes (relatively) easier.
- It allows a geometric interpretation of the problem: to distinguish if there is a confined subspace ($\mathbb{R}^N$) in the given space ($\mathbb{R}^{2N}$).
- Analysing lower bound on RF is equivalent to a lower bound on a known problem in statistics named GAUSSIAN DISTINGUISHING

Remark: This is my partial understanding of the proof.

Table of Contents

Conclusions

Main points

- In the oracle model, FORRELATION offers optimal separation between Quantum and Classical computation
- Generalization of FORRELATION is shown to be among the hardest problems in BQP. [BQP-completness of k-FORRELATION]
- An independent research of Raz-Tal(2018) used a modified version of FORRELATION to shown an oracle separation of BQP with Polynomial Hierarchy(PH)
- It is still unknown if this oracle separation can be used to produce a real-world separation. [Does FORRELATION solve a real-world problem of 'interest'?]

Thank You for Your Attention!