Forrelation and block-multilinear polynomials

Snehal Raj

February 6, 2020

1 Introduction

The paper centers around the question "`What is the biggest advantage that QC can give for any problem?`". The authors mention that problems like factoring and discrete logarithms have separations like $\widetilde{O}\left(n^2\right)$ steps quantumly and $2^{\widetilde{O}\left(n^{1/3}\right)}$ steps classically. However, these separations are only conjectural as the lowerbound on the classical case is still not known.

To prove lower bounds, the authors introduce the quantum query model where the time complexity of the algorithm is related to the number of queries made to the oracle. In the model, the authors define

$$Q(P) = Bounded-error\ quantum\ query\ complexity\ of\ P$$

$$R(P) = Bounded-error\ randomized\ query\ complexity\ of\ P$$

They then mention one of the core motivations of the paper is to answer "`The Speedup Question`" raised by Buhrman et. al in 2002. which asks "*Within the black-box model, just how large of a quantum speedup is possible? For example, could there be a function of N bits with a quantum query complexity of 1, but a classical randomized query complexity of* $\Omega(N)$*?*"

The authors then proceed to list out some of the known separations of quantum/classical query complexities

- Period Finding : $Q(P) = O(1)$ and $R(P) = \widetilde{\Omega}\left(N^{1/4}\right)$
- Simon's Probelm : $Q(P) = O(log\ N)$ and $R(P) = \Omega(\sqrt{N})$
- Glued Trees Problem (Childs et. al.) $Q(P) = O(polylog\ N)$ and $R(P) = \Omega(\sqrt{N})$

They also mention the results by [BBCMW'98] which state the for total boolean functions, $Q(P) = T$ and $R(P) = O(T^6)$ and the results by [A.-Ambainis'13] which state that for permutation symmetric functions, $Q(P) = T$ and $R(P) = O(T^7)$

Now, the main contributions laid out in the paper are as follows:

1. **Largest Known Quantum Speedup**

   They introduce a problem named "*Forrelation*" and show that this problem has the largest known separation in quantum query model. The problem is shown to have separation of the form,

   $$Q(P) = O(1), \quad R(p) = \Omega\left(\frac{\sqrt{N}}{\log N}\right)$$

   They do this by showing a lower bound on number of randomized queries needed to detect small pairwise covariance in real gaussian variables $x_1, x_2, ..., x_n$

2. **Optimality of speedup**

   They also show the optimality of speedup by proving that for every partial boolean function, $if\ Q(P) \leq T\ then\ R(P) = O(N^{1-\frac{1}{2T}})$
   They prove the above theorem by analysing randomized algorithms to approximate bounded, low-degree "block-multilinear" polynomials with a sublinear number of queries.

2 Theory

2.1 The Forrelation Problem

Given black-box access to two Boolean function f,g: $\{0,1\}^n \to \{-1,1\}$, let

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

The problem is to decide whether $\Phi_{f,g} \geq 0.6$ or $|\Phi_{\mathrm{f,g}}| \leq 0.01$, promised that one of these is the case.

2.2 Randomized Lower Bound

One of the first steps that the authors take to prove the randomized lower bound is to convert the "Forrelation" problem into a "Real Forrelation"

2.2.1 Real Forrelation

In Real Forrelation, we are given oracle access to two real functions f,g : $\{0,1\}^n \to \mathbb{R}$ and are promised that either

1. every f(x) and g(y) value is an independent $\mathcal{N}(0,1)$ Gaussian, or else

2. every f(x) value is an independent $\mathcal{N}(0,1)$ Gaussian and every g(y) value equals $\hat{f}(y)$ (i.e. the Fourier transform of f evaluated at y). The problem is to decide which holds.

Theorem 1. *Suppose $\langle f, g\rangle$ are drawn from the forrelated measure $\mathcal{F}$. Define boolean functions F,G : $\{0,1\}^n \to \{-1,1\}$ by F(x) = sgn(f(x)) and G(x) = sgn(g(x)). Then,*

$$\mathrm{E}_{f,g\sim\mathcal{F}}\left[\Phi_{F,G}\right] = \frac{2}{\pi} \pm O\left(\frac{\log N}{N}\right) \tag{2}$$

Corollary 1.1. *Suppose there exists a T-query algorithm that solves "Forrelation" with bounded error. Then there also exists and O(T)-query algorithm that solves "real forrelation" with bounded error.*

2.2.2 Gaussian Distinguishing

Given Oracle access to a collection of $\mathcal{N}(0,1)$ real gaussian variables $x_1, x_2..., x_m$, we are asked to decide whether

- *variables are all independent, or*
- *variables lie in a known low dimensional subspace $S \leq R^m$ such that there is a covariance of at most ϵ between each pair of variables i.e. $\mid Cov(x_i, x_j) \mid \leq \epsilon \ \ \forall \ \ i, j$*

Theorem 2. *Gaussian Distinguishing requires $\Omega\left(\frac{1/\varepsilon}{\log(M/\varepsilon)}\right)$ classical randomized queries.*

Theorem 3. *Any classical randomized algorithm for forrelation must make $\Omega\left(\frac{\sqrt{N}}{\log N}\right)$ queries.*

Theorem 3 is deduced as a more general result on *Gaussian Distinguishing* stated in Theorem 2 such that according to the given case M = 2N , $\epsilon = \frac{1}{\sqrt{N}}$

2.3 Proof of Optimality

Theorem 4. *Let A be a quantum algorithm that makes t-queries to a Boolean input* $x \in \{-1,1\}^N$. *Then there exists a degree-2t block-multilinear polynomial p:* $\mathbb{R}^{2tN} \to \mathbb{R}$, *with 2t-blocks of N variables each such that*

1. *the probability that A accepts x equals p(x,x,...,x) (with x repeated 2t times)*
2. $p(z) \in [-1,1]$ *for all* $z \in \{-1,1\}^{2tN}$

Theorem 5. *Every degree-k real polynomial p:* $\{-1,1\}^N \to \mathbb{R}$ *that is*

1. *bounded in [-1,1] at every boolean point*
2. ***block multilinear*** *i.e. is a polynomial whose variables can be partitioned into k-blocks such that every monomial is the product of one variable from each block.*

can be approximated to within $\pm\epsilon$ *with high probability by querying the oracle* $O\left(N^{1-1/2t}\right)$ *times.*

Using the above stated theorems on classical sublinear algorithms, we deduce theorem 6

Theorem 6. *Let Q be any quantum algorithm that makes t=O(1) queries to an N-bit string* $X \in \{0,1\}^N$. *Then we can estimate Pr[Q accepts X], to constant additive error with high probability, by making only* $O\left(N^{1-1/2t}\right)$ *classical randomized queries to X (non-adaptive)*

This theorem answers Buhrman et al.'s question in the negative by proving that there is no problem with constant vs linear classical/quantum gap. Note that this however, doesn't rule out a possibility of log N vs N quantum/classical separation.