

# Block Multilinear Degree

## Paper Review

---

Akash Kumar Singh, Siddhant Kar, Snehal Raj

IIT Kanpur

# Table of contents

1. Introduction
2. Block-multilinear Degree vs Degree
3. Classical-Quantum Gap
4. References

# Introduction

---

# Quantum Query Model

- The quantum query model is the most widely used model to study quantum algorithms.
- Given a boolean function  $x: \{-1, 1\}^n \rightarrow \{-1, 1\}$ , we are required to calculate a property  $f(x)$ , where  $f: \{-1, 1\}^N \rightarrow \{0, 1\}$  and  $N = 2^n$ .
- An algorithm based on this model is allowed to make several queries to  $x$  in order to calculate  $f(x)$ .
- The minimum number of queries that any such algorithm must make in order to determine  $f$  is called the quantum query complexity  $Q_f$  of  $f$ .

- The polynomial method puts a lower bound on  $Q_f$ .
- Using the method, we can construct a degree  $2Q_f$  polynomial that approximates  $f$  up to some  $\epsilon$ .
- The minimum degree that any such polynomial can attain is called the  $\epsilon$ -approximate degree of  $f$ , denoted  $\widetilde{\deg}_\epsilon(f)$ .
- Thus,  $2Q_f \geq \widetilde{\deg}_\epsilon(f)$ .

# Block-multilinear polynomials

- Aaronson et al. [1] introduced a new notion and approximated  $f$  up to  $\pm\epsilon$  using a "block-multilinear" polynomial of degree  $2Q_f$ .
- A block multilinear polynomial on  $\{-1, 1\}^n$  is of the form

$$p(x) = p(x_{1,1}, x_{1,2}, \dots) = \sum_{(i_1, \dots, i_k)} a_{i_1 \dots i_k} x_{1,i_1} \dots x_{k,i_k}$$

where its  $n$  variables can be partitioned into  $k$  disjoint blocks  $B_i, i \in [k]$ , such that  $x_{i,j} \in B_i \forall j$ .

- The minimum degree attainable by a block-multilinear polynomial that approximates  $f$  up to  $\pm\epsilon$  is called the  $\epsilon$ -approximate block-multilinear degree, denoted  $\widetilde{\text{bmdeg}}_\epsilon(f)$ .
- We thus have  $2Q_f \geq \widetilde{\text{bmdeg}}_\epsilon(f)$ .

# Forrelation

- This notion of block-multilinear polynomials was used in [1] to solve a problem called Forrelation.
- It is a measure of the correlation between a function  $f$  and the fourier transform of a second function  $g$ .
- Given oracle access to two boolean functions  $f, g: \{0, 1\}^n \rightarrow \{-1, 1\}$ , let

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

- We have to decide whether  $\Phi_{f,g} \geq 0.6$  or  $|\Phi_{f,g}| \leq 0.01$ , promised that one of them is the case.

## Block-multilinear Degree vs Degree

---



# Bmdeg vs Deg

- We compare the exact block-multilinear degree of a boolean function to its degree.
- $\text{bmdeg}$  is at least equal to the degree.
- Interested in the gap between the two and want to find a function  $f$  for which the inequality is strict, or that  $\text{bmdeg}_\epsilon(f) > \deg_\epsilon(f)$ .
- Construction a block-multilinear polynomial by symmetrically splitting the coefficients of a given polynomial.
- Second approach which involves finding a dual witness for a suitable linear program.

- From an exact polynomial representation of a polynomial in fourier basis, that is,

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \chi_S(x) \quad (2)$$

where  $\chi_S(x) = \prod_{i \in S} x_i$  is the  $S$ th Fourier function. we devise two different symmetrization construction (the details of which are given in the report).

- Checked whether each polynomial constructed is bounded in  $[-1, 1]$  on all possible inputs using a Integer Linear Program.
- Found a counter example where the polynomials weren't bounded.

- Dual Witness based approach considering the linear program to find the best possible approximation of a function  $f: \{-1, 1\}^N \rightarrow \{0, 1\}$  using a block-multilinear polynomial  $g$  of degree  $d = \deg(f)$ .
- The value of its dual being strictly greater than  $\epsilon_0$ , implies, by weak duality, that the value of the primal is greater than  $\epsilon_0$  as well, and thus  $\text{bmdeg}_{\epsilon_0}(f) > d$ .

## Theorem

Let  $f: \{-1, 1\}^N \rightarrow \{0, 1\}$  have degree  $d$ . Then  $\text{bmdeg}_0(f) > d$  if and only if there exist  $\phi: \{-1, 1\}^N \rightarrow \mathbb{R}$  and  $\psi_1, \psi_2: \{-1, 1\}^{(N+1)^d} \rightarrow \mathbb{R}^+$  such that

1.  $\sum_x \phi(x)f(x) \geq \sum_{\bar{x}} (\psi_1(\bar{x}) + \psi_2(\bar{x}))$ .
2.  $\hat{\psi}_1(m) - \hat{\psi}_2(m) = \frac{N}{2^{(N+1)^d}} \hat{\phi}(S_m) \quad \forall m \in \{0, \dots, N\}^d$ .

# Classical-Quantum Gap

---

- Aaronson et al. [1] introduced a new notion, where they approximated  $f$  up to  $\epsilon$  using a block-multilinear polynomial.
- This notion of block-multilinear polynomials was used in [1] to solve Forrelation.
- Forrelation has achieved the largest gap between quantum and classical query complexities known yet among promise problems.
- In our report we give an overview of the results mentioned in [1] which show this gap.

We first convert the Forrelation problem into a Real Forrelation problem. In Real Forrelation, we are given oracle access to two real functions  $f, g: \{0, 1\}^n \rightarrow \mathbb{R}$  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  $y$ ).

In the Gaussian Distinguishing problem, we are given oracle access to a collection of  $\mathcal{N}(0, 1)$  real Gaussian variables  $x_1, x_2, \dots, x_m$  and are asked to decide whether

1. the variables are all independent, or
2. the variables lie in a known low dimensional subspace  $S \leq R^m$  such that there is a covariance of at most  $\epsilon$  between each pair of variables, i.e.,  $| \text{Cov}(x_i, x_j) | \leq \epsilon \forall i, j$ .

# Randomized Lower bound

- If there exists a  $T$ -query algorithm that solves Forrelation with bounded error, then there also exists an  $O(T)$ -query algorithm that solves Real Forrelation with bounded error. The details of this reduction can be found in [1].
- Gaussian distinguishing requires  $\Omega\left(\frac{1/\varepsilon}{\log(M/\varepsilon)}\right)$  classical randomized queries.
- Using the above stated results, we show in the report that that any classical randomized algorithm for must make  $\Omega\left(\frac{\sqrt{N}}{\log N}\right)$  queries, therefore implying a separation of order  $\Omega\left(\frac{\sqrt{N}}{\log N}\right)$  between quantum and classical complexities.



# Optimized Randomized Algorithm

- Forrelation requires at least  $\Omega(\sqrt{N}/\log n)$  queries classically but just one quantum query.
- We then show in our report that this 1-query quantum algorithm can be converted to a  $\sqrt{N}$ -query randomized algorithm.
- We do this by using an estimator on estimate the block-multilinear polynomial.

## References

---

## References

---

- [1] Scott Aaronson and Andris Ambainis. Forrelation: A problem that optimally separates quantum from classical computing, 2014.