# Block Multilinear Degree

Paper Review

Snehal Raj

IIT Kanpur

## Table of contents

# Introduction

## Quantum Mechanics

One of the most basic quantum mechanical systems is a simple 2-state system called the qubit. The qubit is a linear superposition of two states, $|0\rangle$ and $|1\rangle$, which form an orthonormal basis of the qubit space.

We thus write the state of the qubit as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $\alpha$ and $\beta$ are called the amplitudes and can be complex numbers in general.

Measuring this qubit must result in one of the basis states, with probability equal to the square of the corresponding amplitude. Thus, we have

$$\alpha^2 + \beta^2 = 1.$$

## Quantum Query Model

Given a boolean function $x$, we are required to calculate a property $f(x)$ by querying $x$.

For our convenience, we assume $x$ is a function from $\{-1, 1\}^n$ to $\{-1, 1\}$. Let us represent it in truth table form as $x = (x_1, \ldots, x_N)$, where $N = 2^n$ and each $x_i \in \{-1, 1\}$ corresponds to the $i$th output. We assume that we only want to answer a yes/no question about $x$. Thus, we wish to calculate

$$f \colon \{-1, 1\}^N \longrightarrow \{0, 1\}.$$

**Definition**
A block multilinear polynomial on $\{-1,1\}^n$ is a polynomial of the form

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

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

## Forrelation

Intuitively, 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 $f, g \colon \{0,1\}^n \to \{-1,1\}$, 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 $\left|\Phi_{f,g}\right| \leq 0.01$, and we are promised that one of these is the case.

# Block-multilinear degree vs degree

## Approximate bmdeg

If we are given a polynomial approximation of $f$, we can construct a block-multilinear approximation as follows [?].

**Theorem**
*Let $p(x)$ be a polynomial of degree $d$ such that $|p(x)| \leq 1$ for all*
*$x \in \{-1, 1\}^n$. Then there is a block-multilinear polynomial*
*$\tilde{p} \colon R^{(n+1)d} \to R$ such that*

1. *$\tilde{p}(x, \ldots, x) = p(x)$ for any $x \in \{-1, 1\}^n$.*
2. *$|\tilde{p}(\bar{x})| \leq C_d$ for any $\bar{x} \in \{-1, 1\}^{(n+1)d}$ where $C_d$ is a constant that depends only on $d$.*

## Exact bmdeg

This is a construction we tried from the exact polynomial of $f \colon \{-1, 1\}^n \to \{0, 1\}$, of degree $d$. In the fourier basis representation,
Our construction is

$$f_{sym}(\bar{x}) := \sum_{S \subseteq [n]} \sum_{m \in I_S} \frac{\hat{f}(S)}{|I_S|} \chi_m(\bar{x}) \tag{2}$$

where $\bar{x} \in \{-1, 1\}^{(n+1)d}$. This construction, unfortunately, is not bounded in $[-1, 1]$.

# Classical-Quantum Gap

$k$-fold Forrelation can be solved using a total of only $\lceil k/2 \rceil$ queries to the $k$ corresponding oracles.

The following circuit solves the problem in $k$ queries.

## Randomized Lower Bound

Forrelation can be solved using $O(1)$ queries.

Classical randomized algorithm must make $\Omega(\frac{\sqrt{N}}{\log N})$ queries, therefore implying a separation of order $\Omega(\frac{\sqrt{N}}{\log N})$ between quantum and classical methods.

This separation is also optimal, as we show in our report that Forrelation can be solved classically using $\sqrt{N}$ queries.

## 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 approximating the block-multilinear polynomial corresponding to the quantum algorithm and get the following result.

Let $Q$ be any quantum algorithm that makes $t = O(1)$ queries to an oracle $O_x$ where $x \in \{0,1\}^N$. 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 $x$.

# Experiments

# References