CHICAGO JOURNAL OF THEORETICAL COMPUTER SCIENCE 2024, Article 2, pages 1–20
http://cjtcs.cs.uchicago.edu/

Influences of Fourier Completely Bounded Polynomials and Classical Simulation of Quantum Algorithms

Francisco Escudero Gutiérrez

Received June 29, 2023; Revised August 23, 2024; Published August 28, 2024

Abstract: We give a new presentation of the main result of Arunachalam, Briët and Palazuelos (SICOMP'19) and show that quantum query algorithms are characterized by a new class of polynomials which we call Fourier completely bounded polynomials. We conjecture that all such polynomials have an influential variable. This conjecture is weaker than the famous Aaronson–Ambainis (AA) conjecture (Theory of Computing'14), but has the same implications for classical simulation of quantum query algorithms.

We prove a new case of the AA conjecture by showing that it holds for homogeneous Fourier completely bounded polynomials. This implies that if the output of d-query quantum algorithm is a homogeneous polynomial p of degree $2d$, then it has a variable with influence at least $\mathrm{Var}[p]^2$.

In addition, we give an alternative proof of the results of Bansal, Sinha and de Wolf (CCC'22 and QIP'23) showing that block-multilinear completely bounded polynomials have influential variables. Our proof is simpler, obtains better constants and does not use randomness.

1 Introduction

Understanding the quantum query complexity of Boolean functions $f : D \to \{-1,1\}$, where D is a subset of $\{-1,1\}^n$, has been a crucial task in quantum information science [5]. Query complexity is a model of

Key words and phrases: Quantum query complexity, polynomials, completely bounded norm, influence of Boolean functions, functional analysis.

DOI: 10.4086/cjtcs.2024.02

computing where rigorous upper and lower bounds can be proven, which allows one to compare the power of quantum computers with classical ones. Many celebrated quantum algorithms show an advantage in terms of query complexity, for example in unstructured search [18], period finding [30], Simon's problem [31], NAND-tree evaluation [16] and element distinctness [4]. However, these query complexity advantages are limited to being polynomial in the case of total functions (for functions $D = \{-1,1\}^n$ quantum and classical query complexity are polynomially related), while it can be exponential for highly structured problems (for functions with $|D| = o(2^n)$ classical query complexity can be exponentially larger than quantum query complexity), such as for Simon's problem [31], period finding [30] or k-fold forrelation [2, 32, 8, 29]. It is widely believed that a lot of structure is necessary for superpolynomial speedups.[1] The following folklore conjecture, which has circulated since the late 90s, but was first formally posed by Aaronson and Ambainis [1], formalizes this idea.

Conjecture 1.1 (Folklore)**.** *The output of d-query quantum algorithms can be simulated with error at most ε on at least a $(1-\delta)$-fraction of the inputs using* $\mathrm{poly}(d, 1/\varepsilon, 1/\delta)$ *classical queries.*

In other words, it is believed that quantum query algorithms can be approximated almost everywhere by classical query algorithms with only a polynomial overhead.

In this work we will interpret quantum query algorithms as polynomials, which can be done thanks to a result by Beals et al. [10]. They proved that the output of a d-query quantum algorithm is a bounded polynomial $p : \{-1,1\}^n \to \mathbb{R}$ of degree at most $2d$.[2] Here, *bounded* means that its infinity norm

$$\|p\|_\infty = \sup_{x \in \{-1,1\}^n} |p(x)| \tag{1.1}$$

is at most 1. Based on this observation, Aaronson and Ambainis conjectured that every bounded polynomial of bounded degree has an influential variable, which would imply Theorem 1.1 [1].

Conjecture 1.2 (Aaronson-Ambainis (AA))**.** *Let $p : \{-1,1\}^n \to \mathbb{R}$ be a polynomial of degree at most d with $\|p\|_\infty \leq 1$. Then, p has a variable with influence at least* $\mathrm{poly}(\mathrm{Var}[p], 1/d)$*.*

The argument to show that Theorem 1.2 would imply Theorem 1.1 works as follows [1, Theorem 7]. Let p be the bounded polynomial of degree at most $2d$ that represents the output of d-query quantum algorithm. Say that we want to approximate $p(y)$ for some $y \in \{-1,1\}^n$. First, we query the most influential variable i of y. Then, the restricted polynomial $p|_{x(i)=y(i)}$ would also be a bounded polynomial of degree at most $2d$. We query again the most influential variable and repeat the process a polynomial (in d) number of times. Given that the influences of these variables are inverse polynomially big (in d), after a polynomially small (in d) number of queries, the remaining restriction of p would have a low variance, so if we output its expectation it would be close to $p(y)$ with high probability.

Despite capturing the attention of a wide range of areas, little is known about Conjecture 1.2. In fact, it was motivated by a similar result from analysis of Boolean functions, which proves a weaker version of

[1] Recently, Yamakawa and Zhandry showed that superpolynomial speedups can be attained in unstructured search problems. However, that does not contradict the believe that structure is needed to achieve superpolynomial speedups for decision problems, which are those modeled by Boolean functions [34].

[2] In this work we identify the output of quantum query algorithms on an input $x \in \{-1,1\}^n$ with the expectation of the quantum query algorithm on x, namely the difference of probability of accepting and the probability of rejecting.

the conjecture with inverse exponential dependence on the degree [15]. This weaker version was also reproved from a functional analytic perspective, and in the same work the authors highlighted the relation of AA conjecture with the Bohnenblust-Hille inequality [14]. A few reductions to other conjectures have been made. The first one is that is sufficient to prove the conjecture for one-block decoupled polynomials [27]. Very recently, Lovett and Zhang stated two conjectures related to fractional certificate complexity that, if true, would imply the AA conjecture [22]. Also recently, Austrin et al. showed a connection of the AA conjecture with cryptography: they proved that if the AA conjecture is false, then there is a secure key agreement in the quantum random oracle model that cannot be broken classically [7]. The most recent work in this line of research is the one by Bhattacharya, who showed that the conjecture is true for random restrictions of the polynomial [11]. Regarding particular cases, it is only known to be true in a few scenarios: Boolean functions $f:\{-1,1\}^n\to\{-1,1\}$ [23, 26, 20], symmetric polynomials [19], multilinear forms whose Fourier coefficients are all equal in absolute value [24] and block-multilinear completely bounded polynomials [9].

The last result is relevant in this context because Arunachalam, Briët and Palazuelos showed that quantum query algorithms output polynomials that are not only bounded, but also completely bounded [6]. This is a more restricted normalization condition, which can be informally understood as the polynomial taking bounded values when evaluated not only on bounded scalars, but also on bounded matrix inputs. This way, one could try to use this extra condition to prove results about quantum query algorithms.

This idea was first put in practice by Bansal, Sinha and de Wolf [9]. They showed that the AA conjecture holds for completely bounded block-multilinear forms, which implies an almost everywhere classical simulation result, similar to Theorem 1.1, for the amplitudes of certain quantum query algorithms. These algorithms query different bit strings on every query, while Conjecture 1.1 concerns algorithms that query the same controlled bit string on every query.

1.1 Our results

We follow that line of work and use the characterization of Arunachalam et al. to design a route towards Theorem 1.1. Our first result is a new characterization of quantum query algorithms, that is similar to the one Arunachalam et al., but more convenient for our purposes. To do this we introduce the *Fourier completely bounded d-norms* ($\|\cdot\|_{\mathrm{fcb},d}$). These norms are defined in a similar way to the infinity norm, by taking the supremum of the polynomial over some set. In the case of the infinity norm this set consists of the Boolean strings. By contrast, in the Fourier completely bounded norms the set also includes matrix inputs that *behave like Boolean strings*. We will not include formal definitions in the introduction, but we illustrate the concept of having *Boolean behavior of degree d* with an example. Consider $d=4$ and $n=6$, and let m be a natural number. If a given pair of vectors $u,v\in\mathbb{R}^m$ and a given string of matrices $A\in(M_m)^6$ (where M_m is the space of $m\times m$ real matrices) have Boolean behavior of degree 4, then they will satisfy the same relations as the products of 4 entries of a Boolean string. For instance, it will hold that

$$\langle u,A(1)A(1)A(2)A(3)v\rangle=\langle u,A(5)A(2)A(3)A(5)v\rangle,$$

because they should simulate the relation $x(1)x(1)x(2)x(3)=x(5)x(2)x(3)x(5)$, satisfied by any $x\in\{-1,1\}^6$.

Using the Fourier expansion of polynomials defined on the Boolean hypercube we will introduce a natural way of evaluating polynomial on matrix inputs that have Boolean behavior, which allows us to introduce the Fourier completely bounded d-norm.

Definition 1.3. (Informal version of Theorem 2.2) Let $p : \{-1,1\}^n \to \mathbb{R}$ be a polynomial of degree at most d. Its *Fourier completely bounded d-norm* is given by

$$\|p\|_{\mathrm{fcb},d} := \sup |p(u,v,A)| \tag{1.2}$$

where the supremum is taken over all (u,v,A) that have Boolean behavior of degree d.

Motivated by the characterization by Aruchalam et al., Gribling and Laurent proposed a semidefinite program to compute the completely bounded norm of a tensor, and thus gave a characterization of quantum query algorithms in terms of semidefinite programs [6, 17]. We reinterpret these programs to show that the Fourier completely bounded d-norms characterize quantum query algorithms.

Theorem 1.4. *Let $p : \{-1,1\}^n \to \mathbb{R}$. Then, p is the output of a d-query quantum algorithm if and only if its degree is at most $2d$ and $\|p\|_{\mathrm{fcb},2d} \leq 1$.*

Theorem 1.4 is a new presentation of the main result of Arunachalam et al. that is more compact than the original one [6]. It is presented directly in terms of polynomials of the Boolean hypercube, does not involve a minimization over possible completely bounded extensions of p, and eludes the use of tensors.

It is (implicitly) known the Fourier completely bounded norm can be much bigger than the infinity norm,[3] so Theorem 1.4 suggests that Conjecture 1.2 may be more general than necessary for the application to quantum computing. Hence, we propose the following weaker conjecture, that would also imply Conjecture 1.1.

Conjecture 1.5. *Let $p : \{-1,1\}^n \to \mathbb{R}$ be a polynomial of degree at most d with $\|p\|_{\mathrm{fcb},d} \leq 1$. Then, p has a variable with influence at least $\mathrm{poly}(\mathrm{Var}[p], 1/d)$.*

We can prove a particular case of Theorem 1.2.

Theorem 1.6. *Let $d \in \mathbb{N}$. Let $p : \{-1,1\}^n \to \mathbb{R}$ be a homogeneous polynomial of degree d and with $\|p\|_{\mathrm{fcb},d} \leq 1$. Then, the maximum influence of p is at least $\mathrm{Var}[p]^2$.*

The proof of Theorem 1.6 is based on a generalization of the construction used by Varopoulos to rule out a von Neumann's inequality for degree-3 polynomials [33]. Sadly, the proof of the homogeneous case does not generalize in a straightforward manner (see Theorem 4.3), but it suggests a way to solve the general case (see Theorem 4.4). In particular, we propose Question 4.5 (with some flavour of tensor networks and almost-quantum correlations, as explained in Theorem 4.4), which if answered affirmatively would imply Theorem 1.5.

Theorem 1.6 is the first known particular case of the AA conjecture were the lower bound for the maximum influence is independent of the degree (to prove Theorem 1.1 we could afford a polynomial dependence on the degree). Also, it requires considerably fewer algebraic constraints than the other particular cases for which we know that AA conjecture holds. In addition, thanks to Theorem 1.4, it can be interpreted directly in terms of quantum query algorithms.

[3] From the results of Briët and Palazuelos it can be inferred that there is a sequence of polynomials p_n of degree-3 such that $\|p_n\|_{\mathrm{fcb},3}/\|p_n\|_\infty \to_n \infty$ [12].

Corollary 1.7. *Let $d \in \mathbb{N}$. Let $\mathcal{A}$ be a d-query quantum algorithm whose output is a homogeneous polynomial $p : \{-1,1\}^n \to \mathbb{R}$ of degree $2d$. Then, the maximum influence of p is at least* $\mathrm{Var}[p]^2$.

With a similar construction as the one we used for Theorem 1.6, we can reprove the results of Bansal et al. regarding the influence of block-multilinear completely bounded polynomials [9]. These polynomials have a particular algebraic structure and also a normalization condition when evaluated on matrix inputs (see Section 4.1 below).

Theorem 1.8. *Let $d \in \mathbb{N}$. Let $p : \{-1,1\}^{n\times d} \to \mathbb{R}$ be a block-multilinear degree d polynomial with $\|p\|_{\mathrm{cb}} \leq 1$. Then, p has a variable of influence at least* $(\mathrm{Var}[p]/d)^2$. *In addition, if p is homogeneous of degree d, then it has a variable of influence at least* $\mathrm{Var}[p]^2$.

Theorem 1.8 corresponds to [9, Theorem 1.4], where Bansal et al. proved the same result but with influences at least $\mathrm{Var}[p]^2/[e(d+1)^4]$ in the general case and with $\mathrm{Var}[p]^2/(d+1)^2$ in the homogeneous degree d case. Their proofs involve evaluating p in *random infinite dimensional matrix inputs*, which they can control using ideas of free probability. However, our proof evaluates p in explicit finite dimensional matrix inputs, is shorter and obtains better constants. In particular, our constant for the homogeneous case is optimal.

1.2 Some notation

Given $n \in \mathbb{N}$, $[n]$ denotes the set $\{1,\dots,n\}$, $[n]_0$ the set $\{0,1,\dots,n\}$, M_n the space of $n\times n$ real matrices, $B_n \subseteq M_n$ the space of $n\times n$ real matrices with operator norm (largest singular value) at most 1, and $S^{n-1} \subseteq \mathbb{R}^n$ the set of vectors with euclidean norm 1. Given, $d,n \in \mathbb{N}$, we use $\mathbf{i}$ to denote a multi-index in $[n]^d$.

2 The Fourier completely bounded d-norms

There is a vast theory concerning the properties of multilinear maps $T : \mathbb{R}^n \times \cdots \times \mathbb{R}^n \to \mathbb{R}$ that are completely bounded, i.e., bounded when they are extended to matrix domains [28]. Here, we propose a notion of completely bounded norm for polynomials $p : \{-1,1\}^n \to \mathbb{R}$. First, we introduce a matrix notion of *behaving like a Boolean string*. Then, using the Fourier expansion of these polynomials we define the evaluation of the polynomials on these matrix inputs that*behave like Boolean strings*. Finally, we define the Fourier completely bounded d-norms and prove a few of their properties.

Every $p : \{-1,1\}^n \to \mathbb{R}$ can be written as

$$p(x) = \sum_{S\subseteq[n]} \widehat{p}(S) \prod_{i\in S} x(i), \tag{2.1}$$

where $\widehat{p}(S)$ are the Fourier coefficients of p. We say that p has degree at most d if $\widehat{p}(S) = 0$ for every $|S| > d$, where $|S|$ denotes the cardinality of S.

We will be interested on simulating the behavior of bit strings $x \in \{-1,1\}^n \times \{1\}$ with one extra frozen variable.[4] Given $d \in \mathbb{N}$ and $\mathbf{i},\mathbf{j} \in [n+1]^d$ we say that $\mathbf{i} \sim \mathbf{j}$, if

$$x(i_1)\dots x(i_d) = x(j_1)\dots x(j_d) \text{ for every } x \in \{-1,1\}^n \times \{1\}. \tag{2.2}$$

In other words, if we define

$$S_{\mathbf{i}} := \{k \in [n] : \ k \text{ occurs an odd number of times in } \mathbf{i}\},$$

then $\mathbf{i} \sim \mathbf{j}$ if and only if $S_{\mathbf{i}} = S_{\mathbf{j}}$. Note that $n+1$ does not belong to these sets $S_{\mathbf{i}}$. Given $S \subseteq [n]$ with $|S| \leq d$, we write $[\mathbf{i}^S]$ to denote the equivalence class of indices $\mathbf{i}$ such that $S_{\mathbf{i}} = S$.

Definition 2.1. Let $n,d,m \in \mathbb{N}$. Let $u,v \in S^{m-1}$ and let $A \in (B_m)^{n+1}$. We say that (u,v,A) has *Boolean behavior of degree d* if

$$\langle u, A(i_1)\dots A(i_d)v\rangle = \langle u, A(j_1)\dots A(j_d)v\rangle$$

for all $\mathbf{i},\mathbf{j} \in [n+1]^d$ such that $\mathbf{i} \sim \mathbf{j}$. We call $\mathscr{BB}^d$ to the set of (u,v,A) with Boolean behavior of degree d.

Informally, having Boolean behavior of degree d means that the relations of Eq. (2.2) and some normalization conditions are satisfied. In particular, for any bit string $x \in \{-1,1\}^n \times \{1\}$ and any $d \in \mathbb{N}$, we have that $(1,1,x)$ has Boolean behavior of degree d. Also note that the $(n+1)$-th matrix in Theorem 2.1 *behaves as an identity*, but the rest resemble to *matrices that square to identity*.

Also note that given $d \in \mathbb{N}$, for every $S \in [n]$ with $|S| \leq d$ there is at least one $\mathbf{i} \in [n+1]^d$ such that $S_{\mathbf{i}} = S$. Thus, given (u,v,A) with Boolean behavior of degree d, for every $|S| \leq d$ the product $\prod_{i \in S} x(i)$ can be simulated (in a unique manner) by $\langle u, A(i_1^S)\dots A(i_d^S)v\rangle$. In particular, this means that for a polynomial p of degree at most d, we can define through Eq. (2.1) an evaluation of p on every (u,v,A) that has Boolean behavior of degree d, which leads to the definition of Fourier completely bouded d-norm.

Definition 2.2. Let $p : \{-1,1\}^n \to \mathbb{R}$ be a polynomial of degree at most d. Then, its *Fourier completely bounded d-norm* is defined by

$$\|p\|_{\mathrm{fcb},d} = \sup_{(u,v,A) \in \mathscr{BB}^d} \sum_{S \subseteq [n], |S| \leq d} \widehat{p}(S) \langle u, A(i_1^S)\dots A(i_d^S)v\rangle.$$

The rest of the section is devoted to prove a few results concerning the Fourier completely bounded d-norms. First of all we show that, indeed, they are norms.

Proposition 2.3. *Let $d \in \mathbb{N}$. Then, $\|\cdot\|_{\mathrm{fcb},d}$ is a norm in the space of polynomials $p : \{-1,1\}^n \to \mathbb{R}$ of degree at most d.*

Proof: It clearly satisfies the triangle inequality and is homogeneous. Also, if $p = 0$ then $\|p\|_{\mathrm{fcb},d} = 0$, and vice versa, because $\|p\|_\infty \leq \|p\|_{\mathrm{fcb},d}$. □

[4] The extra variable set to 1 is there because quantum query algorithms query a controlled bit string, and not a non-controlled version, which would not require that extra variable.

One nice property of these norms is that they can be computed as semidefinite programs (SDPs), which are optimization problems involving linear positive semidefinite constraints whose value can be efficiently approximated (see [21] for an introduction to SDPs and [17] for similar semidefinite programs for computing the completely bounded norm of a tensor).

Proposition 2.4. *Let $p : \{-1,1\}^n \to \mathbb{R}$ be a polynomial of degree at most d. Then, its Fourier completely bounded d-norm can be written as the following SDP*

$$\|p\|_{\mathrm{fcb},d} = \sup \sum_{S\in[n],|S|\leq d} \widehat{p}(S)\langle u, v_{\mathbf{i}^S}\rangle, \tag{2.3}$$

$$u, v, v_{\mathbf{i}} \in \mathbb{R}^m,\ m\in\mathbb{N},\ \mathbf{i}\in[n+1]^s,\ s\in[d],$$

$$\langle u, v_{\mathbf{i}}\rangle = \langle u, v_{\mathbf{j}}\rangle,\ \text{if } \mathbf{i}\sim\mathbf{j},\ \mathbf{i},\mathbf{j}\in[n+1]^d, \tag{2.4}$$

$$\langle u,u\rangle = \langle v,v\rangle = 1, \tag{2.5}$$

$$\mathrm{Gram}_{\substack{\mathbf{j}\in[n+1]^s,\\ s\in[d-1]_0}}\{v_{i\mathbf{j}}\} \preccurlyeq \mathrm{Gram}_{\substack{\mathbf{j}\in[n+1]^s,\\ s\in[d-1]_0}}\{v_{\mathbf{j}}\},\ \text{for } i\in[n+1], \tag{2.6}$$

where by $v_{\mathbf{j}}$ with $\mathbf{j}\in[n+1]^0$ we mean v, Gram *denotes the gram matrix and the symbol '$\preccurlyeq$' the usual matrix inequality, and $i\mathbf{j}$ is the concatenation of i and $\mathbf{j}$.*

To gain some intuition about Theorem 2.4, one should think of $v_{\mathbf{i}}$ as $A(i_1)\dots A(i_d)v$, of Eq. (2.4) as the conditions that encode the Boolean Behaviour, while Eq. (2.6) encodes that $A(i)$ are contractions.

Proof: Let $|||p|||$ be the expression on the right-hand side of Eq. (2.3). Note that Eq. (2.4) represents the relations of bit strings of Eq. (2.2), while Eqs. (2.5) and (2.6) encode normalization conditions.

On the one hand, every $(u,v,A)\in\mathscr{B}\mathscr{B}^d$ defines a feasible instance for $|||p|||$ through

$$v_{\mathbf{i}} := A(i_1)\dots A(i_s)v$$

for every $\mathbf{i}\in[n+1]^s$ and every $s\in[d]$. Given that the value of this instance is

$$\sum_{S\subseteq[n],|S|\leq d}\widehat{p}(S)\langle u, A(i_1^S)\dots A(i_d^S)v\rangle$$

we have that $|||p|||\geq\|p\|_{\mathrm{fcb},d}$.

On the other hand, let $u,v,v_{\mathbf{i}}\in\mathbb{R}^m$ be a feasible instance of $|||p|||$. For $i\in[n+1]$ define $A(i)\in M_m$ as the linear map from $\mathbb{R}^m$ to $\mathbb{R}^m$ that takes $v_{\mathbf{j}}$ to $v_{i\mathbf{j}}$ for every $\mathbf{j}\in[n+1]^s$ and every $s\in[d-1]_0$, and it is extended to the orthogonal complement as 0. First of all, we should check that this is a correct definition, meaning that for every $\lambda\in\mathbb{R}^m$, with $m=(n+1)^{d-1}+\dots+(n+1)^0$, we have that

$$\sum_{\mathbf{j}}\lambda_{\mathbf{j}}v_{\mathbf{j}} = 0 \implies \sum_{\mathbf{j}}\lambda_{\mathbf{j}}v_{i\mathbf{j}} = 0.$$

Indeed, we can prove something stronger:

$$\begin{aligned}(\sum_{\mathbf{j}}\lambda_{\mathbf{j}}v_{i\mathbf{j}})^T\sum_{\mathbf{j}'}\lambda_{\mathbf{j}'}v_{i\mathbf{j}'} &= \lambda^T\mathrm{Gram}_{\substack{\mathbf{j}\in[n+1]^s,\\ s\in[d-1]_0}}\{v_{i\mathbf{j}}\}\lambda \leq \lambda^T\mathrm{Gram}_{\substack{\mathbf{j}\in[n+1]^s,\\ s\in[d-1]_0}}\{v_{\mathbf{j}}\}\lambda\\ &= (\sum_{\mathbf{j}}\lambda_{\mathbf{j}}v_{\mathbf{j}})^T\sum_{\mathbf{j}'}\lambda_{\mathbf{j}'}v_{\mathbf{j}'}.\end{aligned}$$

The above calculation also proves that the $A(i)$'s are contractions, and thanks to Eq. (2.4) it follows that (u,v,A) has Boolean behavior of degree d. Finally, note that the value of this (u,v,A) for $\|p\|_{\text{fcb},d}$ is the same as the value of $(u,v,v_{\mathbf{j}})$ for $|||p|||$, so $\|p\|_{\text{fcb},d} \geq |||p|||$. □

Given $d,d' \in \mathbb{N}$ with $d' > d$ and a polynomial $p : \{-1,1\}^n \to \mathbb{R}$ of degree at most d, $\|p\|_{\text{fcb},d}$ and $\|p\|_{\text{fcb},d'}$ have different definitions, but they are comparable. In particular, we prove that the Fourier completely bounded d-norms are not increasing.

Proposition 2.5. *Let $p : \{-1,1\}^n \to \mathbb{R}$ be a polynomial of degree at most d. Then,*

$$\|p\|_{\text{fcb},d+1} \leq \|p\|_{\text{fcb},d}.$$

Remark 2.6. Theorem 2.5 is coherent with Theorem 1.4 (proved below), because allowing more queries to quantum algorithms only increases their power. Theorem 1.4 also suggests that $\|p\|_{\text{fcb},n} = \|p\|_\infty$ should hold, because n quantum queries should be enough to evaluate any bounded polynomial. If true, alongside Theorems 2.4 and 2.5, it would mean that $(\|p\|_{\text{fcb},d})_{d\in[n]}$ is a decreasing hierarchy of SDPs that tend to $\|p\|_\infty$.

Proof of Theorem 2.5: Let (u,v,A) have Boolean behavior of degree $d+1$. Then,

$$(\widetilde{u},\widetilde{v},\widetilde{A}) = \Big(u, \frac{A(n+1)v}{\|A(n+1)v\|}, A\Big) \tag{2.7}$$

has Boolean behavior of degree d. Also, given that $d+1 > d$, we have that for every $S \subseteq [n]$ with $|S| \leq d$, there exists $\mathbf{i} \in [n+1]^{d+1}$ such that $S_{\mathbf{i}} = S$, $i_{d+1} = n+1$, and

$$\langle u, A(i_1)\dots A(i_{d+1})v\rangle = \|A(n+1)v\|\langle \widetilde{u}, \widetilde{A}(i_1)\dots\widetilde{A}(i_d)\widetilde{v}\rangle. \tag{2.8}$$

This way,

$$\begin{aligned}
\|p\|_{\text{fcb},d+1} &= \sup_{(u,v,A)\in\mathscr{B}\mathscr{B}^{d+1}} \sum_{S\subseteq[n],|S|\leq d} \widehat{p}(S)\langle u, A(i_1^S)\dots A(i_{d+1}^S)v\rangle \\
&= \sup_{(u,v,A)\in\mathscr{B}\mathscr{B}^{d+1}} \|A(n+1)v\| \sum_{S\subseteq[n],|S|\leq d} \widehat{p}(S)\langle \widetilde{u}, \widetilde{A}(i_1^S)\dots \widetilde{A}(i_d^S)\widetilde{v}\rangle \\
&\leq \sup_{(u,v,A)\in\mathscr{B}\mathscr{B}^{d+1}} \sum_{S\subseteq[n],|S|\leq d} \widehat{p}(S)\langle \widetilde{u}, \widetilde{A}(i_1^S)\dots \widetilde{A}(i_d^S)\widetilde{v}\rangle \\
&\leq \sup_{(u',v',A')\in\mathscr{B}\mathscr{B}^{d}} \sum_{S\subseteq[n],|S|\leq d} \widehat{p}(S)\langle u', A'(i_1^S)\dots A'(i_d^S)v'\rangle \\
&= \|p\|_{\text{fcb},d},
\end{aligned}$$

where in the second line we have used Eq. (2.8), and in the third line that $\|A(n+1)v\| \leq 1$, and in the fourth that $(\widetilde{u},\widetilde{v},\widetilde{A})$ has Boolean behavior of degree d. □

The next proposition states that $\|\cdot\|_{\text{fcb},d}$ does not increase after restrictions, which is a relevant feature to ensure that Conjecture 1.5 implies Conjecture 1.1. Given a polynomial $p : \{-1,1\}^n \to \mathbb{R}$ and $i \in [n]$, the *restriction of p to the i-th variable being set to $y \in \{-1,1\}$* is the polynomial $q : \{-1,1\}^{n-1} \to \mathbb{R}$ (whose variables we index with $x(1),\dots,x(i-1),x(i+1),\dots,x(n)$ for convenience) defined by $q(x) := p(x(1),\dots,x(i-1),y,x(i+1),\dots,x(n))$.

Proposition 2.7. *Let $p:\{-1,1\}^n\to\mathbb{R}$ be a polynomial of degree at most d and let $i\in[n]$. Let $q:\{-1,1\}^{n-1}\to\mathbb{R}$ be the restriction of p to the i-th variable being set to $y\in\{-1,1\}$. Then,*

$$\|q\|_{\mathrm{fcb},d}\leq\|p\|_{\mathrm{fcb},d}.$$

Proof: Consider a pair of vectors and a string of matrices $(u,v,A(1),\dots,A(i-1),A(i+1),\dots,A(n+1))$ with Boolean behavior of degree d. Define $\widetilde{u}:=u$, $\widetilde{v}:=v$ and $\widetilde{A}(j)$ for $j\in[n+1]$ as

$$\widetilde{A}(j)=\begin{cases}A(j) & \text{if } j\neq i,\\ yA(n+1) & \text{if } j=i.\end{cases}$$

It can be verified that $(\widetilde{u},\widetilde{v},\widetilde{A}(1),\dots,\widetilde{A}(n+1))$ has Boolean behavior of degree d. Now note that for every $S\subseteq[n]-\{i\}$, it is satisfied that

$$\widehat{q}(S)=\widehat{p}(S)+y\widehat{p}(S\cup\{i\}). \tag{2.9}$$

Also, for every $S\subseteq[n]-\{i\}$ with $|S|\leq d-1$, it is satisfied that

$$\langle\widetilde{u},\widetilde{A}(j_1^S)\dots\widetilde{A}(j_d^S)\widetilde{v}\rangle=y\langle\widetilde{u},\widetilde{A}(j_1^{S\cup\{i\}})\dots\widetilde{A}(j_d^{S\cup\{i\}})\widetilde{v}\rangle. \tag{2.10}$$

Thus,

$$\begin{aligned}\|q\|_{\mathrm{fcb},d} &= \sup_{\substack{(u,v,A(j))\in\mathscr{B}\mathscr{B}^d\\ j\in[n+1]-\{i\}}} \sum_{S\subseteq[n]-\{i\},|S|\leq d}\widehat{q}(S)\langle u,A(j_1^S)\dots A(j_d^S)v\rangle\\
&= \sup_{\substack{(u,v,A(j))\in\mathscr{B}\mathscr{B}^d\\ j\in[n+1]-\{i\}}} \sum_{S\subseteq[n]-\{i\},|S|\leq d}\widehat{p}(S)\langle u,A(j_1^S)\dots A(j_d^S)v\rangle\\
&+ \sum_{S\subseteq[n]-\{i\},|S|\leq d-1} y\widehat{p}(S\cup\{i\})\langle u,A(j_1^S)\dots A(j_d^S)v\rangle\\
&= \sup_{\substack{(u,v,A(j))\in\mathscr{B}\mathscr{B}^d\\ j\in[n+1]-\{i\}}} \sum_{S\subseteq[n]-\{i\},|S|\leq d}\widehat{p}(S)\langle\widetilde{u},\widetilde{A}(j_1^S)\dots\widetilde{A}(j_d^S)\widetilde{v}\rangle\\
&+ \sum_{S\subseteq[n]-\{i\},|S|\leq d-1}\widehat{p}(S\cup\{i\})\langle\widetilde{u},\widetilde{A}(j_1^{S\cup\{i\}})\dots\widetilde{A}(j_d^{S\cup\{i\}})\widetilde{v}\rangle\\
&\leq \sup_{\substack{(u',v',A'(j))\in\mathscr{B}\mathscr{B}^d\\ j\in[n+1]}} \sum_{S\subseteq[n],|S|\leq d}\widehat{p}(S)\langle u',A'(j_1^S)\dots A'(j_d^S)v'\rangle\\
&= \|p\|_{\mathrm{fcb},d},\end{aligned}$$

where in the second line we have used Eq. (2.9), in the fourth line Eq. (2.10), and in the sixth line that $(\tilde{u},\tilde{v},\tilde{A})$ has Boolean behavior. □

3 Quantum query algorithms are Fourier completely bounded polynomials

Now we are ready to prove Theorem 1.4, that fully characterizes quantum query algorithms in terms of the Fourier completely bounded d-norms.

Theorem 1.4. *Let $p : \{-1,1\}^n \to \mathbb{R}$. Then, p is the output of a d-query quantum algorithm if and only if its degree is at most $2d$ and $\|p\|_{\mathrm{fcb},2d} \leq 1$.*

To prove Theorem 1.4 we just have to reinterpret the semidefinite programs by Gribling and Laurent, based on the work of Arunachalam et al. [17, 6].

Theorem 3.1 (Gribling-Laurent)**.** *Let $p : \{-1,1\}^n \to \mathbb{R}$. Then, p is the output of d-query quantum algorithm if and only if its degree is at most $2d$ and the value of the following semidefinite program is at most 0,*

$$\begin{aligned} &\max \ -w + \sum_{x\in\{-1,1\}^n} \frac{p(x)\phi(x)}{2^n} \qquad (3.1)\\ &\text{s.t. } w \geq 0,\ m \in \mathbb{N},\ A_s \in (B_m)^{n+1},\ u,v \in \mathbb{R}^m,\ s \in [2d],\\ &\quad \|\phi\|_1 = 1,\ \|u\|^2 = \|v\|^2 = w,\\ &\quad \widehat{\phi}(S_{\mathbf{i}}) = \langle u, A_1(i_1)\dots A_{2d}(i_{2d})v\rangle,\ \mathbf{i} \in [n+1]^{2d}, \end{aligned}$$

where $\|\phi\|_1 = \sum_{x\in\{-1,1\}^n} \frac{|\phi(x)|}{2^n}$.

Remark 3.2. Theorem 3.1 corresponds to [17, Equation (24)]. There, the authors not only ask for the $A_s(i)$ to be contractions, but also unitaries. However, that extra restriction does not change the value of the semidefinite program because we can always block-encode a contraction in the top left corner of an unitary (see for instance [3, Lemma 7]). We also want to remark that $A_s(i)$ can be taken to be equal to $A_{s'}(i)$ for every $s,s' \in [2d]$ and every $i \in [n+1]$, as this extra restriction does not change value of the semidefinite program. Indeed, let (u,v,A_s,w,ϕ) be part of feasible instance of Eq. (3.1). Define now

$$\begin{aligned} \widetilde{u} &:= u \otimes e_1,\\ \widetilde{v} &:= v \otimes e_{2d+1},\\ A(i) &:= \sum_{s\in[2d]} A_s(i) \otimes e_s e_s^T, \end{aligned}$$

where $\{e_s\}_{s\in[2d+1]}$ is an orthonormal basis of $\mathbb{R}^{2d+1}$. Then,

$$\langle u, A_1(i_1)\dots A_d(i_{2d})v\rangle = \langle \widetilde{u}, \widetilde{A}(i_1)\dots \widetilde{A}(i_{2d})\widetilde{v}\rangle,$$

for every $\mathbf{i} \in [n+1]^{2d}$. Hence, $(\widetilde{u},\widetilde{v},\widetilde{A},w,\phi)$ is a feasible instance for Eq. (3.1) that attains the same value as (u,v,A_s,w,ϕ).

Proof of 1.4: Thanks to Theorem 3.1 and Theorem 3.2, we know that p is the output of d-query quantum algorithm if and only if its degree is at most $2d$ and the following constraint is satisfied

$$\sum_{x\in\{-1,1\}^n} \frac{p(x)\phi(x)}{2^n} \leq w \qquad (3.2)$$

$$\begin{aligned} &\text{s.t. } w \geq 0,\ m \in \mathbb{N},\ A \in (B_m)^{n+1},\ u,v \in \mathbb{R}^m,\\ &\quad \|\phi\|_1 = 1, \qquad (3.3)\\ &\quad \|u\|^2 = \|v\|^2 = w,\\ &\quad \widehat{\phi}(S_{\mathbf{i}}) = \langle u, A(i_1)\dots A(i_{2d})v\rangle,\ \mathbf{i} \in [n+1]^{2d}. \end{aligned}$$

Now, note that if (u,v,A,ϕ,w) satisfies all conditions of Eq. (3.2) except for Eq. (3.3), then $(u/\sqrt{\|\phi\|_1}, v/\sqrt{\|\phi\|_1}, A, \phi/\|\phi\|_1, w/\|\phi\|_1)$ would be a feasible instance. Furthermore, given that

$$\sum_{x\in\{-1,1\}^n} \frac{p(x)\phi(x)}{2^n} \le w \iff \frac{1}{\|\phi\|_1} \sum_{x\in\{-1,1\}^n} \frac{p(x)\phi(x)}{2^n} \le \frac{w}{\|\phi\|_1},$$

we can write Eq. (3.2) forgetting about the normalization condition of Eq. (3.3). In other words, Eq. (3.2) is equivalent to

$$\sum_{x\in\{-1,1\}^n} \frac{p(x)\phi(x)}{2^n} \le w \tag{3.4}$$

$$\begin{aligned} \text{s.t. } & w \ge 0,\ m\in\mathbb{N},\ A\in(B_m)^{n+1},\ u,v\in\mathbb{R}^m, \\ & \|u\|^2 = \|v\|^2 = w, \\ & \widehat{\phi}(S_{\mathbf{i}}) = \langle u, A(i_1)\dots A(i_{2d})v\rangle,\ \mathbf{i}\in[n+1]^{2d}. \end{aligned} \tag{3.5}$$

In addition, by homogeneity we can assume $w = 1$, as if (u,v,A,ϕ,w) is a feasible instance, then $(u/\sqrt{w}, v/\sqrt{w}, A, \phi/w, 1)$ also is, and Eq. (3.4) is satisfied for the first instance if and only if is satisfied for the second instance. Also note, that if (u,v,A) are part of a feasible instance of Eq. (3.4), then it automatically has Boolean behavior of degree $2d$, and any (u,v,A) defines a feasible instance for Eq. (3.4). Finally, by Parseval's identity we can rewrite $\sum_{x\in\{-1,1\}^n} \frac{p(x)\phi(x)}{2^n}$ as $\sum_{S\subseteq[n]} \widehat{p}(S)\widehat{\phi}(S)$. Putting altogether we get that p is the output of d-query quantum algorithm if and only if its degree is at most $2d$ and

$$\begin{aligned} &\sum_{S\subseteq[n],|S|\le 2d} \widehat{p}(S)\langle u, A(i_1^S)\dots A(i_{2d}^S)v\rangle \le 1 \\ &\text{s.t. } (u,v,A) \text{ has Boolean behavior of degree } 2d, \end{aligned}$$

which is the same as saying that $\|p\|_{\mathrm{fcb},2d} \le 1$. □

4 Aaronson and Ambainis conjecture for (Fourier) completely bounded polynomials

In this section we prove Theorem 1.6 and Theorem 1.8. Both are based on the construction used by Varopoulos to disprove a degree-3 von Neumann's inequality [33]. First of all, we recall the expressions of variance and influences of a polynomial $p:\{-1,1\}^n\to\mathbb{R}$. The variance is given by

$$\mathrm{Var}[p] = \sum_{|S|\ge 1} \widehat{p}(S)^2,$$

and the influence of the i-th variable by

$$\mathrm{Inf}_i[p] = \sum_{S\ni i} \widehat{p}(S)^2.$$

The maximum influence of p is $\mathrm{MaxInf}[p] := \max_{i\in[n]} \mathrm{Inf}_i[p]$. $\mathrm{Var}[p]$ measures how much p deviates from its expectation, because $\mathrm{Var}[p] = \mathbb{E}_x[(f(x)-\mathbb{E}_y f(y))^2]$. By contrast, $\mathrm{Inf}_i[p]$ amounts for how much p changes the i-th variable variable is flipped, because $\mathrm{Inf}_i[p] = \mathbb{E}_x[(p(x)-p(x^{\oplus i})^2/2]$, where $x^{\oplus i}$ is obtained by flipping the i-th entry of x.

4.1 AA conjecture for block-multilinear completely bounded polynomials

Before proving Theorem 1.8, we shall specify what is a block-multilinear completely bounded polynomial. A *block-multilinear polynomial* of degree d is a polynomial $p:\{-1,1\}^{n\times d}\to\mathbb{R}$ such that if we divide the variables $x\in\{-1,1\}^{n\times d}$ in d blocks of n coordinates each, then the every of the monomials of p has at most one coordinate from each of the blocks. In other words, the block-multilinear polynomials of degree d are those that can be written as

$$p(x_1,\cdots,x_d)=\widehat{p}(\emptyset)+\sum_{s\in[d]}\sum_{\substack{\mathbf{b}\in[d]^s\\ b_1<\cdots<b_s}}\sum_{\mathbf{i}\in[n]^s}\widehat{p}(\{(b_1,i_1),\cdots,(b_s,i_s)\})x_{b_1}(i_1)\cdots x_{b_s}(i_s), \tag{4.1}$$

for every $(x_1,\cdots,x_d)\in(\{-1,1\}^n)^d$. For this kind of polynomials, there is a very natural way of evaluating them in matrix inputs,

$$p(A_1,\cdots,A_d)=\widehat{p}(\emptyset)\,\mathrm{Id}_m+\sum_{s\in[d]}\sum_{\substack{\mathbf{b}\in[d]^s\\ b_1<\cdots<b_s}}\sum_{\mathbf{i}\in[n]^s}\widehat{p}(\{(b_1,i_1),\cdots,(b_s,i_s)\})A_{b_1}(i_1)\cdots A_{b_s}(i_s), \tag{4.2}$$

for every $A_s\in(M_m)^n$, $s\in[d]$ and $m\in\mathbb{N}$. The *completely bounded norm* of a block-multilinear polynomial is defined as

$$\|p\|_{\mathrm{cb}}:=\sup\{\|p(A_1,\cdots,A_d)\|:\ m\in\mathbb{N},\ A_s\in(B_m)^n,\ s\in[d]\}. \tag{4.3}$$

Concerning these polynomials, we can show the following.

Theorem 1.8. *Let $d\in\mathbb{N}$. Let $p:\{-1,1\}^{n\times d}\to\mathbb{R}$ be a block-multilinear degree d polynomial with $\|p\|_{\mathrm{cb}}\le 1$. Then, p has a variable of influence at least $(\mathrm{Var}[p]/d)^2$. In addition, if p is homogeneous of degree d, then it has a variable of influence at least $\mathrm{Var}[p]^2$.*

Remark 4.1. With our proof of the homogeneous case of Theorem 1.8 we can show that for the case of $p:\{-1,1\}^{n\times d}\to\mathbb{R}$ being a homogeneous degree d block-multinear polynomial we have the following non-commutative root influence inequality

$$\|p\|_{\mathrm{cb}}\ge\sum_{i\in[n]}\sqrt{\mathrm{Inf}_{s,i}[p]}, \tag{4.4}$$

for any $s\in[d]$. This improves [9, Theorem 1.4] in two ways. First, we can allow s to be any number in $[d]$, while they only prove the result of $s\in\{1,d\}$. Second, they prove a weaker statement that depends on d, namely,

$$\|p\|_{\mathrm{cb}}\ge\sum_{i\in[n]}\frac{\sqrt{\mathrm{Inf}_{s,i}[p]}}{\sqrt{e(d+1)}},$$

for $s\in\{1,d\}$.

Remark 4.2. Given that $p(x_1,\cdots,x_d)=x_1(1)\ldots x_d(1)$ is a homogeneous degree d block-multilinear completely bounded polynomial with $\mathrm{Var}[p]^2=\mathrm{MaxInf}[p]=1$, we have that the homogeneous case of Theorem 1.8 is optimal.

Proof of the homogeneous degree d case of Theorem 1.8: Let p be a homogeneous degree d block-multilinear polynomial. Let $s \in [d]$. We label the coordinates by (r,i), where $r \in [d]$ indicates the block, and $i \in [n]$. Our goal is defining $A \in (B_m)^n$ and $f_\emptyset, e_\emptyset \in S^{m-1}$ such that

$$\langle f_\emptyset, A(i_1)\dots A(i_d)e_\emptyset\rangle = \frac{\widehat{p}(\{(1,i_1),\dots,(d,i_d)\})}{\sqrt{\mathrm{Inf}_{s,i_s}[p]}}. \tag{4.5}$$

Once we are there, we can prove the announced root-influence inequality Eq. (4.4). Indeed,

$$\begin{aligned}
\|p\|_{\mathrm{cb}} &\geq \sum_{i_1,\dots,i_d\in[n]} \widehat{p}(\{(1,i_1),\dots,(d,i_d)\})\langle f_\emptyset, A(i_1)\dots A(i_d)e_\emptyset\rangle \\
&= \sum_{i_1,\dots,i_d\in[n]} \widehat{p}(\{(1,i_1),\dots,(d,i_d)\})\frac{\widehat{p}(\{(1,i_1),\dots,(d,i_d)\})}{\sqrt{\mathrm{Inf}_{s,i_s}[p]}} \\
&= \sum_{i_s\in[n]} \frac{1}{\sqrt{\mathrm{Inf}_{s,i_s}[p]}} \underbrace{\sum_{i_1,\dots,i_{s-1},i_{s+1},i_d\in[n]} \widehat{p}(\{(1,i_1),\dots,(d,i_d)\})^2}_{\mathrm{Inf}_{s,i}[p]} \\
&= \sum_{i\in[n]} \sqrt{\mathrm{Inf}_{s,i}[p]}.
\end{aligned}$$

Finally, the statement about the maximal influence quickly follows from the root-influence inequality

$$\|p\|_{\mathrm{cb}} \geq \sum_{i\in[n]} \sqrt{\mathrm{Inf}_{s,i}[p]} \geq \sum_{i\in[n]} \frac{\mathrm{Inf}_{s,i}[p]}{\sqrt{\mathrm{MaxInf}[p]}} = \frac{\mathrm{Var}[p]}{\sqrt{\mathrm{MaxInf}[p]}},$$

which after rearranging yields

$$\mathrm{MaxInf}[p] \geq \left(\frac{\mathrm{Var}[p]}{\|p\|_{\mathrm{cb}}}\right)^2.$$

Hence, it suffices to design $(f_\emptyset, e_\emptyset, A) \in S^{m-1}\times S^{m-1}\times (B_m)^n$ satisfying Eq. (4.5). Let $\mathcal{S} := \{\{(r,i_r),\dots,(d,i_d)\} : i_r,\dots,i_d \in [n],\ s+1 \leq r \leq d\}$ and $\mathcal{S}' := \{\{(1,i_1),\dots,(r,i_r)\} : i_1,\dots,i_r \in [n],\ r \leq s-1\}$. Let $m := 2+|\mathcal{S}|+|\mathcal{S}'|$. Let $\{e_\emptyset, e_S, f_\emptyset, f_{S'} :\ S\in\mathcal{S},\ S'\in\mathcal{S}'\}$ be an orthonormal basis of $\mathbb{R}^m$, and define $A(i) \in M_m$ by

$$\begin{aligned}
A(i)e_S &:= e_{S\cup\{(d-|S|,i)\}},\ \text{for } 0\leq |S| \leq d-s-1,\ S\in\mathcal{S}, \\
A(i)e_S &:= \sum_{\substack{S'\in\mathcal{S}'\\ |S'|=s-1}} \frac{\widehat{p}(S'\cup S\cup\{(s,i)\})}{\sqrt{\mathrm{Inf}_{s,i}(p)}} f_{S'},\ \text{for } |S| = d-s,\ S\in\mathcal{S}, \\
A(i)f_{S'} &:= \delta_{(|S'|,i)\in S'} f_{S'-\{(|S'|,i)\}},\ S'\in\mathcal{S}'.
\end{aligned}$$

We claim that $(f_\emptyset, e_\emptyset, A(i))$ satisfies Eq. (4.5). This is because the first applications of the $A(i)$'s act like a *creation* operator and the last as *annihilation* operators. The first $d-s-1$ of the matrices on $e_\emptyset$ create a vector that stores the indices of these first $d-s-1$ applications, namely

$$A(s+1)\dots A(d)e_\emptyset = e_{\{((s+1,i_{s+1}),\dots,(d,i_d))\}}.$$

The $d-s$ application has a unique behavior, as it maps the previous vector to a superposition of $f_\cdot$ vectors, namely

$$A(i_s)e_{\{((s+1,i_{s+1}),\ldots,(d,i_d))\}} = \sum_{\substack{S'\in\mathcal{S}'\\|S'|=s-1}} \frac{\widehat{p}(S'\cup((s,i_s),\ldots,(d,i_d)))}{\sqrt{\mathrm{Inf}_{s,i}(p)}} f_{S'}.$$

Finally, the last $s-1$ applications of the matrices act like annihilation operators, meaning that

$$A(i_1)\ldots A(i_{s-1})f_{S'} = \delta_{S',((1,i_1),\ldots,(s-1,i_{s-1}))} f_\emptyset.$$

Putting everything together we conclude that indeed Eq. (4.5) is satisfied.

Finally, we claim that $A(i)$ are contractions. Given that $\{e_S:\ 0\le|S|\le d-s-1,\ S\in\mathcal{S}\}$, $\{e_S:\ |S|=d-s,\ S\in\mathcal{S}\}$ and $\{f_{S'}:\ S'\in\mathcal{S}'\}$ are mapped to orthogonal spaces, we just have to check than when $A(i)$ is a contraction when it is restricted to the span of each of these 3 sets. For the first and third sets of vectors that is clear. For the second is true because for any $\lambda\in[n]^{d-s}$

$$\begin{aligned}
\|A(i)\sum_{\substack{S\in\mathcal{S}\\|S|=d-s}}\lambda_S e_S\| &= \|\sum_{\substack{S\in\mathcal{S}\\|S|=d-s}}\sum_{\substack{S'\in\mathcal{S}'\\|S'|=s-1}}\frac{\widehat{p}(S'\cup S\cup\{(s,i)\})}{\sqrt{\mathrm{Inf}_{s,i}[p]}}\lambda_S f_{S'}\| \\
&= \sqrt{\frac{\sum_{\substack{S'\in\mathcal{S}'\\|S'|=s-1}}\left(\sum_{\substack{S\in\mathcal{S}\\|S|=d-s}}\widehat{p}(S'\cup S\cup\{(s,i)\})\lambda_S\right)^2}{\mathrm{Inf}_{s,i}[p]}} \\
&\le \sqrt{\frac{\sum_{\substack{S'\in\mathcal{S}'\\|S'|=s-1}}\left(\sum_{\substack{S\in\mathcal{S}\\|S|=d-s}}\widehat{p}(S'\cup S\cup\{(s,i)\})^2\right)\left(\sum_{\substack{S\in\mathcal{S}\\|S|=d-s}}\lambda_S^2\right)}{\mathrm{Inf}_{s,i}[p]}} \\
&= \sqrt{\frac{\mathrm{Inf}_{s,i}[p]}{\mathrm{Inf}_{s,i}[p]}}\sqrt{\sum_{\substack{S\in\mathcal{S}\\|S|=d-s}}\lambda_S^2} \\
&= \|\sum_{\substack{S\in\mathcal{S}\\|S|=d-s}}\lambda_S e_S\|,
\end{aligned}$$

where in the inequality we have used Cauchy-Schwarz. □

Proof of the general case of Theorem 1.8: Let $p:\{-1,1\}^{n\times d}\to\mathbb{R}$ be a block-multilinear degree d polynomial. For every $s\in[d]$, let $p_{=s}$ be its degree s part. Let $D\in[d]$ be such that $\mathrm{Var}[p_{=D}]\ge\mathrm{Var}[p]/d$, which exists because $\mathrm{Var}[p]=\sum_{s\in[d]}\mathrm{Var}[p_{=s}]$. We will now divide the proof in two parts. One is showing that

$$\|p_{=D}\|_{\mathrm{cb}}\le\|p\|_{\mathrm{cb}}, \tag{4.6}$$

and the other is proving that

$$\mathrm{MaxInf}(p_{=D})\ge\left(\frac{\mathrm{Var}[p_{=D}]}{\|p_{=D}\|_{\mathrm{cb}}}\right)^2. \tag{4.7}$$

Once we had done that, the result will easily follow:

$$\mathrm{MaxInf}(p) \geq \mathrm{MaxInf}(p_{=D}) \geq \left(\frac{\mathrm{Var}[p_{=D}]}{\|p_{=D}\|_{\mathrm{cb}}}\right)^2 \geq \left(\frac{\mathrm{Var}[p]}{d\|p\|_{\mathrm{cb}}}\right)^2,$$

where in the second inequality we have used Eq. (4.7), and in the third we have used Eq. (4.6) and that $\mathrm{Var}[p_{=D}] \geq \mathrm{Var}[p]/d$.

First, we prove Eq. (4.6). Let $B \in B_{d+1}$ be defined by $B := \sum_{s\in[D]} e_s e_{s+1}^T$, where $\{e_s\}_{s\in[D+1]}$ is an orthonormal basis of $\mathbb{R}^{D+1}$. Note that $\langle e_1, B^s e_{D+1}\rangle = \delta_{s,D}$ for all $s \in [d]_0$. Hence,

$$\begin{aligned}
\|p_{=D}\|_{\mathrm{cb}} &= \sup_{\substack{u,v\in S^{m-1},\, A\in(B_m)^n \\ m\in\mathbb{N}}} \sum_{\substack{\mathbf{b}\in[d]^D \\ b_1<\cdots<b_D}} \sum_{\mathbf{i}\in[n]^D} \widehat{p}_{=D}(\{(b_1,i_1),\ldots,(b_D,i_D)\})\langle u, A_{b_1}(i_1)\ldots A_{b_D}(i_D)v\rangle \\
&= \sup_{\substack{u,v\in S^{m-1},\, A\in(B_m)^n \\ m\in\mathbb{N}}} \sum_{s\in[d]} \sum_{\substack{\mathbf{b}\in[d]^s \\ b_1<\cdots<b_s}} \sum_{\mathbf{i}\in[n]^s} \widehat{p}(\{(b_1,i_1),\ldots,(b_s,i_s)\}) \\
&\qquad \cdot \langle u\otimes e_1, (A_{b_1}(i_1)\otimes B)\ldots(A_{b_s}(i_s)\otimes B)v\otimes e_{D+1}\rangle \\
&\leq \|p\|_{\mathrm{cb}}.
\end{aligned}$$

Second, we prove Eq. (4.7). Let $\mathcal{S} := \{\{(b_1,i_1),\ldots,(b_{D-1},i_{D-1})\} : b_s \in [d],\ b_1 < \cdots < b_{D-1},\ i_s \in [n],\ s \in [D-1]\}$. Let $m := 2 + |\mathcal{S}|$. Let $\{v, f_\emptyset, f_S : S \in \mathcal{S}\}$ be an orthonormal basis of $\mathbb{R}^m$. For $b \in [d],\ i \in [n]$, define $A_b(i) \in M_m$ by

$$\begin{aligned}
A_b(i)v &:= \sum_{\substack{S\in\mathcal{S} \\ |S|=D-1}} \frac{\widehat{p}_{=D}(S\cup\{(b,i)\})}{\sqrt{\mathrm{MaxInf}[p_{=D}]}} f_S, \\
A_b(i)f_S &:= \delta_{(b,i)\in S} f_{S-\{(b,i)\}}, \text{ for } S \in \mathcal{S}\cup\emptyset.
\end{aligned}$$

$A_b(i)$ are contractions because they map the vectors of an orthonormal basis to orthogonal vectors without increasing their norms. Note that for $b_1 < \cdots < b_D$ and $\mathbf{i} \in [n]^D$ we have that

$$\langle f_\emptyset, A_{b_1}(i_1)\ldots A_{b_D}(i_D)v\rangle = \frac{\widehat{p}_{=D}(\{(b_1,i_1),\ldots,(b_D,i_D)\})}{\sqrt{\mathrm{MaxInf}[p_{=D}]}}.$$

Thus,

$$\|p_{=D}\|_{\mathrm{cb}} \geq \sum_{\substack{\mathbf{b}\in[d]^D \\ b_1<\cdots<b_D}} \sum_{\mathbf{i}\in[n]^D} \widehat{p}_{=D}(\{(b_1,i_1),\ldots,(b_D,i_D)\})\langle f_\emptyset, p(A_1,\ldots,A_d)v\rangle = \frac{\mathrm{Var}[p_{=D}]}{\sqrt{\mathrm{MaxInf}[p_{=D}]}},$$

which after rearranging yields Eq. (4.7). □

4.2 AA conjecture for homogeneous Fourier completely bounded polynomials

Finally, we prove a new case of the AA conjecture.

Theorem 1.6. *Let $d \in \mathbb{N}$. Let $p : \{-1,1\}^n \to \mathbb{R}$ be a homogeneous polynomial of degree d and with $\|p\|_{\mathrm{fcb},d} \leq 1$. Then, the maximum influence of p is at least* $\mathrm{Var}[p]^2$.

Proof: Let $m := 1 + \binom{n}{0} + \cdots + \binom{n}{d-1}$. Let $\{v, f_\emptyset, f_S : S \subseteq [n],\ 1 \leq |S| \leq d-1\}$ be an orthonormal basis of $\mathbb{R}^m$. Define the matrices $A(i) \in M_m$ as

$$A(i)v := \sum_{\substack{S \ni i \\ |S|=d}} \frac{\widehat{p}(S)}{\sqrt{\mathrm{MaxInf}[p]}} f_{S-\{i\}},$$
$$A(i)f_S := \delta_{S\ni i} f_{S-\{i\}},\ \text{for } S \subseteq [n],\ 0 \leq |S| \leq d-1,$$

for $i \in [n]$ and $A(n+1) := 0$. We claim that $(f_\emptyset, v, A(i))$ has Boolean behavior of degree d. $A(n+1)$ is clearly a contraction. For $i \in [n]$, $A(i)$ is a contraction, as it maps vectors of the orthonormal basis to orthogonal vectors without increasing the norm, because

$$\|A(i)v\|^2 = \sum_{S \ni i} \frac{\widehat{p}(S)^2}{\mathrm{MaxInf}[p]} = \frac{\mathrm{Inf}_i[p]}{\mathrm{MaxInf}[p]} \leq 1.$$

On the other hand, if $S \subseteq [n]$ satisfies $|S| \leq d-1$, then any $\mathbf{i} \in [n+1]^d$ with $S_{\mathbf{i}} = S$ either has a repeated element of $[n]$ or has an appearance of the index $n+1$, which implies that $\langle f_\emptyset, A(i_1)\ldots A(i_d)\rangle = 0 = \widehat{p}(S)$. If $|S| = d$, then any $\mathbf{i} \in [n+1]^d$ with $S_{\mathbf{i}} = S$ has d different indices in $[n]$ (corresponding to the elements of S), so in that case

$$\langle f_\emptyset, A(i_1)\ldots A(i_d)v\rangle = \frac{\widehat{p}(S)}{\sqrt{\mathrm{MaxInf}[p]}}. \tag{4.8}$$

Putting everything together we conclude that $(f_\emptyset, v, A(i))$ has Boolean behavior of degree d, so

$$\|p\|_{\mathrm{fcb},d} \geq \sum_{S \subseteq [n]} \widehat{p}(S)\langle f_\emptyset, A(i_1)\ldots A(i_d)v\rangle = \sum_{S\subseteq[n]} \frac{\widehat{p}(S)^2}{\sqrt{\mathrm{MaxInf}[p]}}$$
$$= \frac{\mathrm{Var}[p]}{\sqrt{\mathrm{MaxInf}[p]}},$$

where in the first equality we have used Eq. (4.8). After rearranging, the above expression yields

$$\mathrm{MaxInf}[p] \geq \left(\frac{\mathrm{Var}[p]}{\|p\|_{\mathrm{fcb},d}}\right)^2.$$

□

Remark 4.3. Sadly, we could not extend the proof of Theorem 1.6 to the general case. Now, we aim to illustrate what would go wrong with our technique.

For example, consider a polynomial $p : \{-1,1\}^3 \to \mathbb{R}$ with $\deg(p) = 1$ and $\|p\|_{\mathrm{fcb},3} \leq 1$. Ideally, we would want to define unit vectors u and v and contractions $A(i)$ such that for every $S \subseteq [3]$ and every $\mathbf{i} \in [\mathbf{i}^S]$ they satisfied

$$\langle u, A(i_1)A(i_2)A(i_3)v\rangle = \frac{\widehat{p}(S)}{\sqrt{\mathrm{MaxInf}[p]}}. \tag{4.9}$$

If we emulated the strategy of the proof of Theorem 1.6, then $A(1)v$ should be a *normalized* superposition of orthogonal vectors whose amplitudes are all possible $\widehat{p}(S_{\mathbf{i}})$ that have $i_3 = 1$. In particular, all $\widehat{p}(S)$ with $|S| = 1$ must be included among these amplitudes, because if $S = \{i\}$, then $S = S_{(i,1,1)}$. Hence, the *normalizing* factor of $A(1)v$ should be $\sqrt{\mathrm{Var}\, p}$, instead of $\sqrt{\mathrm{MaxInf}(p)}$. Note that this extra normalization comes from the fact that given that given (i_1,i_2,i_3), it may happen that $i_3 \notin S_{(i_1,i_2,i_3)}$ and $\widehat{p}(S_{(i_1,i_2,i_3)}) \neq 0$, because p is not homogeneous of degree-3. If we mimic the rest of the proof after this first step that we were forced to modify, we would reach

$$\langle u, A(i_1)\ldots A(i_3)v\rangle = \frac{\widehat{p}(S)}{\sqrt{\mathrm{Var}[p]}}$$

instead of Eq. (4.9), which would lead to $\|p\|_{\mathrm{fcb},3} \geq \sqrt{\mathrm{Var}\, p}$, that is trivially true, because $\|p\|_{\mathrm{fcb},3} \geq \|p\|_\infty$ and $\|p\|_\infty \geq \sqrt{\mathrm{Var}\, p}$.

Remark 4.4. However, there might be a different way of, given a polynomial p of degree at most d, choosing (u, v, A) with Boolean behavior of degree d such that

$$\langle u, A(i_1)\ldots A(i_d)v\rangle = \frac{\widehat{p}(S_{\mathbf{i}})}{\mathrm{poly}(d, \mathrm{MaxInf}[p])},$$

for any $\mathbf{i} \in [n+1]^d$. If that was true, one could copy and paste the proof of Theorem 1.6 and conclude Theorem 1.5.

This reduces Theorem 1.5 to a question with flavor of tensor networks (see [13] for an introduction to the topic). In particular, the central questions in matrix product states theory is, given a t-tensor $T \in \mathbb{C}^{n\times\cdots\times n}$, to find matrices $A_1,\ldots,A_t$ of low dimension such that $T_{\mathbf{i}} = \mathrm{Tr}[A(i_1)\ldots A(i_t)]$ for every $\mathbf{i} \in [n]^t$. Thus, we are asking the same question, but with a different goal: to minimize the operator norm of the matrices, instead of their dimensions.

It also has the flavor of almost-quantum correlations [25]. Almost-quantum correlations are a model for multiparty quantum mechanics that eludes tensor products and commutativity of the observables: it only imposes the commutativity on the correlations. For example, in a bipartite scenario, valid correlations would be those determined by observables $\{A_x\}_{x\in\mathcal{X}}$ and $\{B_y\}_{y\in\mathcal{Y}}$ and a state $|\psi\rangle$ such that

$$\langle\psi|A_xB_y|\psi\rangle = \langle\psi|B_yA_x|\psi\rangle, \text{ for all } x \in \mathcal{X}, y \in \mathcal{Y}.$$

In other words, almost-quatum correlations impose the commutativity conditions with respect to the *sandwiches* with $|\psi\rangle$, instead of directly imposing them to the observables, Similarly, we would like to find matrices that satisfy certain Boolean relations with respect to the product with two vectors u and v.

Question 4.5. Given a polynomial p of degree at most d, is there $(u,v,A) \in \mathscr{B}\mathscr{B}^d$ such that

$$\langle u, A(i_1)\dots A(i_d)v\rangle = \frac{\widehat{p}(S_{\mathbf{i}})}{\mathrm{poly}(d, \mathrm{MaxInf}[p])},$$

for any $\mathbf{i} \in [n+1]^d$?

Acknowledgements. We want to thank Jop Briët, Sander Gribling and Carlos Palazuelos for useful comments, conversations and encouragement. We also want to thank the reviewers for helpful comments. This research was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement no. 945045, and by the NWO Gravitation project NETWORKS under grant no. 024.002.003.

References

[1] SCOTT AARONSON AND ANDRIS AMBAINIS: The need for structure in quantum speedups. *arXiv preprint arXiv:0911.0996*, 2009. 2

[2] SCOTT AARONSON AND ANDRIS AMBAINIS: Forrelation: A problem that optimally separates quantum from classical computing. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pp. 307–316, 2015. 2

[3] SCOTT AARONSON, ANDRIS AMBAINIS, JĀNIS IRAIDS, MARTINS KOKAINIS, AND JURIS SMOTROVS: Polynomials, quantum query complexity, and Grothendieck's inequality. In *31st Conference on Computational Complexity, CCC 2016*, pp. 25:1–25:19, 2016. arXiv:1511.08682. 10

[4] ANDRIS AMBAINIS: Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007. 2

[5] ANDRIS AMBAINIS: Understanding quantum algorithms via query complexity. In *Proceedings of the International Congress of Mathematicians: Rio de Janeiro 2018*, pp. 3265–3285. World Scientific, 2018. 1

[6] SRINIVASAN ARUNACHALAM, JOP BRIËT, AND CARLOS PALAZUELOS: Quantum query algorithms are completely bounded forms. *SIAM J. Comput*, 48(3):903–925, 2019. Preliminary version in ITCS'18. 3, 4, 10

[7] PER AUSTRIN, HAO CHUNG, KAI-MIN CHUNG, SHIUAN FU, YAO-TING LIN, AND MOHAMMAD MAHMOODY: On the impossibility of key agreements from quantum random oracles. In *Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*, pp. 165–194. Springer, 2022. 3

[8] NIKHIL BANSAL AND MAKRAND SINHA: K-forrelation optimally separates quantum and classical query complexity. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pp. 1303–1316, 2021. 2

[9] NIKHIL BANSAL, MAKRAND SINHA, AND RONALD DE WOLF: Influence in completely bounded block-multilinear forms and classical simulation of quantum algorithms. *arXiv preprint arXiv:2203.00212*, 2022. 3, 5, 12

[10] ROBERT BEALS, HARRY BUHRMAN, RICHARD CLEVE, MICHELE MOSCA, AND RONALD DE WOLF: Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. [doi:10.1145/502090.502097] 2

[11] SREEJATA KISHOR BHATTACHARYA: Aaronson-ambainis conjecture is true for random restrictions. *arXiv preprint arXiv:2402.13952*, 2024. 3

[12] JOP BRIËT AND CARLOS PALAZUELOS: Failure of the trilinear operator space Grothendieck inequality. *Discrete Analysis*, 2019. Paper No. 8. 4

[13] J. IGNACIO CIRAC, DAVID PÉREZ-GARCÍA, NORBERT SCHUCH, AND FRANK VERSTRAETE: Matrix product states and projected entangled pair states: Concepts, symmetries, theorems. *Rev. Mod. Phys.*, 93:045003, Dec 2021. [doi:10.1103/RevModPhys.93.045003] 17

[14] ANDREAS DEFANT, MIECZYSŁAW MASTYŁO, AND ANTONIO PÉREZ: On the fourier spectrum of functions on boolean cubes. *Mathematische Annalen*, 374(1):653–680, 2019. 3

[15] IRIT DINUR, EHUD FRIEDGUT, GUY KINDLER, AND RYAN O'DONNELL: On the fourier tails of bounded functions over the discrete cube. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pp. 437–446, 2006. 3

[16] EDWARD FARHI, JEFFREY GOLDSTONE, AND SAM GUTMANN: A quantum algorithm for the hamiltonian nand tree. *arXiv preprint quant-ph/0702144*, 2007. 2

[17] SANDER GRIBLING AND MONIQUE LAURENT: Semidefinite programming formulations for the completely bounded norm of a tensor. *arXiv preprint arXiv:1901.04921*, 2019. 4, 7, 10

[18] LOV K GROVER: A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996. 2

[19] PAATA IVANISHVILI: Aaronson-ambainis conjecture. `https://extremal010101.wordpress.com/2019/10/29/aaronson-ambainis-conjecture/`, 2019. 3

[20] RAHUL JAIN AND SHENGYU ZHANG: The influence lower bound via query elimination. *Electronic Colloquium on Computational Complexity - ECCC*, 7, 02 2011. [doi:10.4086/toc.2011.v007a010] 3

[21] MONIQUE LAURENT AND FRANZ RENDL: Semidefinite programming and integer programming. *Handbooks in Operations Research and Management Science*, 12:393–514, 2005. 7

[22] SHACHAR LOVETT AND JIAPENG ZHANG: Fractional certificates for bounded functions. *Electronic Colloquium on Computational Complexity - ECCC*, 107, 2022. 3

[23] GATIS MIDRIJANIS: On randomized and quantum query complexities. *arXiv preprint quant-ph/0501142*, 2005. 3

[24] ASHLEY MONTANARO: Some applications of hypercontractive inequalities in quantum information theory. *Journal of Mathematical Physics*, 53(12):122206, 2012. 3

[25] MIGUEL NAVASCUÉS, YELENA GURYANOVA, MATTY J HOBAN, AND ANTONIO ACÍN: Almost quantum correlations. *Nature communications*, 6(1):6288, 2015. 17

[26] RYAN O'DONNELL, MICHAEL SAKS, ODED SCHRAMM, AND ROCCO A SERVEDIO: Every decision tree has an influential variable. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*, pp. 31–39. IEEE, 2005. 3

[27] RYAN O'DONNELL AND YU ZHAO: Polynomial bounds for decoupling, with applications. *arXiv preprint arXiv:1512.01603*, 2015. 3

[28] VERN PAULSEN: *Completely Bounded Maps and Operator Algebras*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2003. 5

[29] ALEXANDER A SHERSTOV, ANDREY A STOROZHENKO, AND PEI WU: An optimal separation of randomized and quantum query complexity. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pp. 1289–1302, 2021. 2

[30] PETER W SHOR: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999. 2

[31] DANIEL R. SIMON: On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997. [doi:10.1137/S0097539796298637, doi.org10.1137S0097539796298637] 2

[32] AVISHAY TAL: Towards optimal separations between quantum and randomized query complexities. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 228–239. IEEE, 2020. 2

[33] N. TH. VAROPOULOS: On an inequality of von Neumann and an application of the metric theory of tensor products to operators theory. *J. Functional Analysis*, 16:83–100, 1974. [doi:10.1016/0022-1236(74)90071-8] 4, 11

[34] TAKASHI YAMAKAWA AND MARK ZHANDRY: Verifiable quantum advantage without structure. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 69–74. IEEE, 2022. 2

AUTHOR

Francisco Escudero Gutiérrez
PhD candidate
Centrum Wiskunde & Informatica, Science Park 123, 1098 Amsterdam
feg@cwi.nl
https://sites.google.com/view/francisco-escudero-gutierrez/