On Converses to the Polynomial Method

Jop Briët
CWI & QuSoft, Amsterdam, The Netherlands

Francisco Escudero Gutiérrez
CWI & QuSoft, Amsterdam, The Netherlands

Abstract

A surprising "converse to the polynomial method" of Aaronson et al. (CCC'16) shows that any bounded quadratic polynomial can be computed exactly in expectation by a 1-query algorithm up to a universal multiplicative factor related to the famous Grothendieck constant. A natural question posed there asks if bounded quartic polynomials can be approximated by 2-query quantum algorithms. Arunachalam, Palazuelos and the first author showed that there is no direct analogue of the result of Aaronson et al. in this case. We improve on this result in the following ways: First, we point out and fix a small error in the construction that has to do with a translation from cubic to quartic polynomials. Second, we give a completely explicit example based on techniques from additive combinatorics. Third, we show that the result still holds when we allow for a small additive error. For this, we apply an SDP characterization of Gribling and Laurent (QIP'19) for the completely-bounded approximate degree.

2012 ACM Subject Classification Mathematics of computing → Functional analysis; Theory of computation → Quantum complexity theory

Keywords and phrases Quantum query complexity, polynomial method, completely bounded polynomials

Digital Object Identifier 10.4230/LIPIcs.TQC.2022.6

Related Version *Full Version*: https://arxiv.org/abs/2204.12303

Funding *Jop Briët*: 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.
Francisco Escudero Gutiérrez: 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.

Acknowledgements We want to thank Srinivasan Arunachalam, Sander Gribling and Carlos Palazuelos for useful discussions. We also want to thank the referees of TQC for their helpful comments.

1 Introduction

A celebrated result of Beals et al. [6], known as the *polynomial method* in quantum complexity theory, leverages the problem of lower bounding the quantum query complexity of a Boolean function to lower bounding the approximate degree. The method is based on the fact that for every t-query quantum algorithm $\mathcal{A}$ that takes an n-bit input and returns a sign, there is a real n-variable polynomial f of degree at most $2t$ such that $f(x) = \mathbb{E}[\mathcal{A}(x)]$ for every x. Here, the expectation is taken with respect to the randomness in the measurement done by $\mathcal{A}$.[1] In addition to many new lower bounds, this result led to a line of research on possible

[1] We identify a quantum query algorithm with the (random) function representing its output on a given input string.

converses, whereby a bounded polynomial f can be turned into a quantum query algorithm that approximates f and whose query complexity depends in some reasonably way on the degree of f. Here, f is *bounded* if it maps the Boolean hypercube to the interval $[-1, 1]$ and a quantum query algorithm $\mathcal{A}$ *approximates* f if for some constant error parameter $\varepsilon < 1$, we have that $|f(x) - \mathbb{E}[\mathcal{A}(x)]| \leq \varepsilon$ for every x. For bounded polynomials of degree at most 2, the following converse was proved in [2], using a surprising application of the Grothendieck inequality from Banach space theory (we refer to [14] for an extensive survey on Grothendieck-type inequalities).

▶ **Theorem 1** (Aaronson et al.). *There exists an absolute constant $C > 0$ such that the following holds. For every bounded polynomial f of degree at most 2, there exists a one-query quantum algorithm $\mathcal{A}$ such that $\mathbb{E}[\mathcal{A}(x)] = Cf(x)$ holds for every $x \in \{-1, 1\}^n$.*

This "multiplicative converse" implies an approximation with *additive* error at most $1 - C$. A natural question is if this result generalizes to quartic polynomials and two-query quantum algorithms [2, Section 5, Question 1]. Based on the probabilistic method and a new characterization of quantum query algorithms in terms of completely bounded polynomials, a counterexample to a direct analog of Theorem 1 was given for quartic polynomials in [3].

▶ **Theorem 2** (Arunachalam–Briët–Palazuelos). *For any $C > 0$, there exist an $n \in \mathbb{N}$ and a bounded quartic n-variable polynomial f such that no two-query quantum algorithm $\mathcal{A}$ satisfies $\mathbb{E}[\mathcal{A}(x)] = Cf(x)$ for every $x \in \{-1, 1\}^n$.*

However, this result does not exclude the possibility that all bounded quartic polynomials can be (additively) approximated by two-query quantum algorithms. Moreover, the result is not constructive, relying on results from random matrix theory to show the existence of such polynomials. Finally, the result was obtained by transforming a certain random *cubic* polynomial into a quartic polynomial with similar properties. As we will explain here, the argument given in [3] to show that there is such a transformation contains an error. Here, we address these issues as follows:

First, we correct the error in [3], showing that Theorem 2 holds as stated.

Second, we give a completely explicit example for Theorem 2 using ideas from the field of additive combinatorics that were applied to construct counterexamples to certain far-reaching generalizations of the Grothendieck inequality [8].

Third, we strengthen Theorem 2 by showing that it still holds with a small additive error:

▶ **Theorem 3.** *For any $C > 0$, there exist an $n \in \mathbb{N}$, an $\varepsilon > 0$ and a bounded quartic n-variable polynomial f such that no two-query algorithm $\mathcal{A}$ satisfies $|\mathbb{E}[\mathcal{A}(x)] - Cf(x)| < \varepsilon$ for every $x \in \{-1, 1\}^n$.*

This result is an application of a semidefinite-program (SDP) of Gribling and Laurent [11] for quantum query complexity. It can be interpreted as an analogue of results on approximate degree based on its linear-programming-based characterization (see for instance [9]). To the best of our knowledge, this is the first application of [11] to prove lower bounds on quantum query complexity. As such, we believe it can serve as a first step towards using this SDP to approach other problems such as proving large separations between approximate degree and quantum query complexity, for example [1].

In similar vein, we use a basic lower bound on the (real) Grothendieck constant, denoted K_G, based on the CHSH Bell inequality to give an impossibility result for one-query quantum algorithms. That is, we show that there exists a bounded quadratic polynomial f such that no one-query quantum algorithm approximates f with error less than $1 - 1/\sqrt{2}$.

Motivated by this, we pose as an open question whether this can be improved to $1 - 1/K_G$. Since the result of [2] achieves this for bounded bilinear forms, this would give yet another characterization of the Grothendieck constant. Tsirelson's characterization in the context of Bell inequalities [18] being a famous example in quantum information theory, for instance.

We would like to remark that the characterization of quantum query algorithms given in [3], that we use here, was regarded as a nice, but unnatural result. However, it has gained relevance in recent times, as it has been proved to be an appropriate tool to make progress in a relevant question such as the Aaronson-Ambainis conjecture [5].

2 Preliminaries

Unless stated otherwise, below C will stand for an absolute positive constant whose value may change from line to line. All polynomials are assumed to be real and multivariate. A homogeneous polynomial is referred to as a *form*. A polynomial is multilinear if each variable appears with degree at most 1. Given an n-variate polynomial f and $p \in [1, \infty)$, define

$$\|f\|_p = \left(\mathbb{E}_{x \in \{-1,1\}^n} f(x)^p\right)^{\frac{1}{p}}$$
$$\|f\|_\infty = \max_{x \in \{-1,1\}^n} |f(x)|.$$

We also define the following "commutative version" of a completely bounded norm:

$$\|f\|_{\text{iccb}} = \sup_{d \in \mathbb{N}} \left\{ \left\| f(A_1, \ldots, A_n) \right\| : A_i \in \mathbb{C}^{d \times d},\ \|A_i\| \leq 1,\ [A_i, A_j] = 0 \right\},$$

where the norms on the right-hand side are the usual operator norms.[2]

The following lemma [3, Theorem 1.3, Proposition 4.4] relates quantum query algorithms to completely bounded polynomials.

▶ **Lemma 4.** *Let $\mathcal{A}$ be a t-query quantum algorithm. Then, there exists an $(n+1)$-variate form f of degree $2t$ such that $\|f\|_{\text{iccb}} \leq 1$ and which satisfies $f(x, 1) = \mathbb{E}[\mathcal{A}(x)]$ for every $x \in \{-1, 1\}^n$.*

We will also use a quantity associated specifically with multilinear cubic forms, that is polynomials of the form:

$$f(x) = \sum_{S \in \binom{[n]}{3}} c_S \prod_{i \in S} x_i, \tag{1}$$

where the c_S are some real coefficients. For $i \in [n]$, define the ith *slice* of f to be the symmetric matrix $M_i \in \mathbb{R}^{n \times n}$ with (j, k)-coefficient equal to $c_{\{i,j,k\}}$ if i, j, k are pairwise distinct and 0 otherwise. Then, define

$$\Delta(f) = \max_{i \in [n]} \|M_i\|.$$

The following is a slight variant of a decomposition due to Varopoulos [19].

[2] The notation iccb stands for "identical commutative completely bounded", where the word identical distinguishes it from another natural variant of the completely bounded norm of a polynomial.

▶ **Lemma 5** (tri-linear Varopoulos decomposition). *Let f be an n-variate multilinear cubic form as in* (1)*. Then, for some $d \in \mathbb{N}$, there exist pairwise commuting matrices $A_1, \ldots, A_n \in \mathbb{R}^{d\times d}$ and orthogonal unit vectors $u, v \in \mathbb{R}^d$ such that $\|A_i\| \leq 1$, $[A_i, A_j] = 0$ and*

$$A_i^2 = 0 \tag{2}$$
$$\langle u, A_i v\rangle = 0 \tag{3}$$
$$\langle u, A_i A_j v\rangle = 0 \tag{4}$$
$$\langle u, A_i A_j A_k v\rangle = \frac{c_{\{i,j,k\}}}{\Delta(f)} \tag{5}$$

for all pairwise distinct $i, j, k \in [n]$.

Proof. For each $i \in [n]$, define M_i as above. Define $W_i = \Delta(f)^{-1} M_i$ and note that this has operator norm at most 1. For each $i \in [n]$, define the $(2n+2) \times (2n+2)$ block matrix

$$A_i = \left[\begin{array}{c|c|c|c} & & & \\ \hline e_i & & & \\ \hline & W_i^\intercal & & \\ \hline & & e_i^\intercal & \end{array}\right],$$

where the first and last rows and columns have size 1, the second and third have size n and where the empty blocks are filled with zeros. Define $u = e_{2n+1}$ and $v = e_1$. The rest of the proof is identical to the proof of [8, Lemma 2.11], except for the property that $A_i^2 = 0$. This follows from the fact that

$$A_i^2 = \left[\begin{array}{c|c|c|c} & & & \\ \hline & & & \\ \hline W_i^\intercal e_i & & & \\ \hline & e_i^\intercal W_i^\intercal & & \end{array}\right].$$

and since the ith row and ith column of M_i are zero. ◀

▶ **Corollary 6.** *Let f be an n-variate multilinear cubic form as in* (1)*. Suppose that an $(n+2)$-variate quartic form $h \in \mathbb{R}[x_0, x_1, \ldots, x_n, z]$ satisfies $h(x, 1) = x_0 f(x_1, \ldots, x_n)$ for every $x \in \{-1, 1\}^{n+1}$. Then,*

$$\|h\|_{\mathrm{iccb}} \geq \frac{\|f\|_2^2}{\Delta(f)}.$$

Proof. The multilinear monomials $\chi_S(x) = \prod_{i\in S} x_i$ with $S \subseteq \{0, \ldots, n\}$ satisfy the orthogonality relations

$$\mathbb{E}_{x\in\{-1,1\}^{n+1}} \chi_S(x)\chi_T(x) = \delta_{S,T}. \tag{6}$$

It follows that h and $x_0 f$ have equal coefficients for each quartic multilinear monomial in the variables $x_0, \ldots, x_n$, which are c_S for $x_0\chi_S$ with $S \in \binom{[n]}{3}$ and 0 otherwise. Let $A_1, \ldots, A_n \in \mathbb{R}^{d\times d}$ and $u, v \in \mathbb{R}^d$ be as in Lemma 5 and let $A_0 = I, A_{n+1} = 0$. Commutativity and properties (2)–(4) imply that if a quartic monomial expression $A_i A_j A_k A_l$ with $i, j, k, l \in \{0, \ldots, n+1\}$ has repeated indices or an index equal to $n+1$, then $\langle u, A_i A_j A_k A_l v\rangle = 0$.

With this, it follows from property (5) that

$$\begin{aligned}\langle u, h(A_0,\dots,A_{n+1})v\rangle &= \Big\langle u, \sum_{S\in\binom{[n]}{3}} c_S\, A_0\chi_S(A_1,\dots,A_n)v\Big\rangle \\ &= \sum_{S\in\binom{[n]}{3}} c_S\langle u, \chi_S(A_1,\dots,A_n)v\rangle \\ &= \Delta(f)^{-1}\sum_{S\in\binom{[n]}{3}} c_S^2 \\ &= \Delta(f)^{-1}\|f\|_2^2,\end{aligned} \tag{7}$$

where the last line is Parseval's identity [13, Chapter 1]. ◀

3 Counterexamples

Here, we prove Theorems 2 and 3. But first we discuss the error in [3, pp. 920]. The proof there uses the equation

$$\sum_{\alpha,\beta\in\{0,1,2,3,4\}^n:|\alpha|+|\beta|=4} d'_{\alpha,\beta}x^\alpha = C\sum_{\alpha\in\{0,1\}^n:|\alpha|=4} d_\alpha x^\alpha \quad \forall\, x\in\{-1,1\}^n, \tag{8}$$

where $d'_{\alpha,\beta}$, d_α and C are real numbers and $|\alpha|$ stands for $\sum_{i=1}^n \alpha_i$. It follows from (6) that $d'_{\alpha,0} = Cd_\alpha$ for all $\alpha\in\{0,1\}^n$ such that $|\alpha|=4$. What is used, however, is that $d'_{\alpha,0} = Cd_\alpha$ for all $\alpha\in\{0,1,2,3,4\}^n$ such that $|\alpha|=4$, which is not true in general. For instance if $n=2$, $C=1$ and $d'_{(2,2),(0,0)} = d'_{(0,0),(4,0)} = -d'_{(2,0),(2,0)} = -d'_{(0,2),(2,0)} = 1$ and the rest of the coefficients set to 0, then (8) becomes $x_1^2x_2^2 - x_1^2 - x_2^2 + 1 = 0$.

Corollary 6 gets around this issue by using a multilinear cubic form instead of just a cubic form. This results in matrices A_i in Lemma 5 that square to zero and has the effect that terms other than quartic multilinear monomials vanish in the left-hand side of (7).

3.1 A random example

The probabilistic proof of Theorem 2 uses a random cubic form as in (1) where the coefficients c_S are chosen to be independent uniformly distributed random signs. Parseval's identity then gives $\|f\|_2^2 = \binom{n}{3}$. Each of the slices M_i of f is a random symmetric matrix with independent mean-zero entries of absolute value at most 1. A standard random-matrix inequality and the union bound then imply that $\Delta(f)\le C\sqrt{n}$ with probability $1-\exp(-Cn)$ [15, Corollary 2.3.6]. By Hoeffding's inequality [7, Theorem 2.8] and the union bound, we have that $\|f\|_\infty \le Cn^2$ with probability $1-\exp(-Cn)$. Rescaling f then gives that there exists a bounded multilinear cubic form such that $\|f\|_2^2/\Delta(f)\ge C\sqrt{n}$. It now follows from Lemma 4 with Corollary 6 that the $(n+1)$-variable quartic polynomial $x_0f(x_1,\dots,x_n)$ satisfies the requirements of Theorem 2.

3.2 An explicit example

We also give a constructive proof of Theorem 2 using techniques from [8], which were used there to disprove a conjecture of Pisier on certain far-reaching generalizations of the Grothendieck inequality. We do not exactly use the construction from that paper because it involves complex functions. Instead, we will the Möbius function (defined below), which is real valued and has the desired properties.

Let n be a positive integer to be set later and let $f_0 : \mathbb{Z}_n \to [-1, 1]$ be a function to be set later (where as usual $\mathbb{Z}_n$ denotes the group of integers modulo n). Define f to be the cubic multilinear form on $3n$ variables given by

$$f(x) = \sum_{a,b \in \mathbb{Z}_n} x(1, a)x(2, a + b)x(3, a + 2b)f_0(a + 3b), \tag{9}$$

where we indexed the variables by $[3] \times \mathbb{Z}_n$.

We claim that for some choice of f_0, the quartic polynomial $x_0 f$, where x_0 is an additional variable, meets the requirements of Theorem 2. The generalized von Neumann inequality [17, Lemma 11.4] allows us to bound the ∞-norm of f. For a function $g : \mathbb{Z}_n \to \mathbb{R}$ and $b \in \mathbb{Z}_n$, define its multiplicative derivative $\Delta_b g : \mathbb{Z}_n \to \mathbb{R}$ to be the function $\Delta_b g(a) = g(a + b)g(a)$. The Gowers 3-uniformity norm of g is then defined as

$$\|g\|_{U^3} = \left(\mathbb{E}_{a,b,c,d \in \mathbb{Z}_n} \Delta_b \Delta_c \Delta_d g(a)\right)^{\frac{1}{8}}.$$

▶ **Lemma 7** (generalized von Neumann inequality)**.** *Suppose that n is coprime to 6. Then, for any function of the form* (9)*, we have that*

$$\|f\|_\infty \leq n^2 \|f_0\|_{U^3}.$$

The polynomial f has $3n$ slices, $M_{i,a} \in \mathbb{R}^{[3] \times \mathbb{Z}_n}$ for each $i \in [3]$ and $a \in \mathbb{Z}_n$, which we view as 3×3 block-matrices with blocks indexed by $\mathbb{Z}_n$. The slice $M_{1,a}$ is supported only on the $(2, 3)$ and $(3, 2)$ blocks, which are each others' transposes. On its $(2, 3)$ block it has value $f_0(a + 3b)$ on coordinate $(a + b, a + 2b)$ for each b. In particular, this matrix has at most one nonzero entry in each row and column. It follows that a relabeling of the rows turns $M_{1,a}$ into a diagonal matrix with diagonal entries in $[-1, 1]$, and therefore $\|M_{1,a}\| \leq 1$. Similarly, we get that $\|M_{i,a}\| \leq 1$ for $i = 2, 3$. Hence, $\Delta(f) \leq 1$. Parseval's identity implies that

$$\|f\|_2^2 = n \sum_{a \in \mathbb{Z}_n} f_0(a)^2.$$

Identify $\mathbb{Z}_n$ with $\{0, 1 \ldots, n - 1\}$ in the standard way. We choose f_0 to be the Möbius function restricted to this interval. That is, set $f_0(0) = 0$ and for $a > 0$, set

$$f_0(a) = \begin{cases} 1 & \text{if } a \text{ is square-free with an even number of prime factors} \\ -1 & \text{if } a \text{ is square-free with an odd number of prime factors} \\ 0 & \text{otherwise.} \end{cases}$$

Tao and Teräväinen [16] recently proved that

$$\|f_0\|_{U^3} \leq \frac{1}{(\log \log n)^C}$$

for some absolute constant $C > 0$. It is also well-known that there are $\frac{6}{\pi^2} n - O(\sqrt{n})$ integers in $[n]$ that are square-free [12, page 269]. Normalizing f by $(\log \log n)^C / n^2$ and taking n coprime to 6 then gives a bounded multilinear cubic polynomial satisfying

$$\frac{\|f\|_2^2}{\Delta(f)} \geq \frac{6}{\pi^2} (\log \log n)^C - o(1).$$

This proves Theorem 2 as before.

▶ Remark 8. The *jointly completely bounded norm* of f is given by

$$\|f\|_{\mathrm{jcb}} = \sup_{d\in\mathbb{N}} \|f(A_1, A_2, A_3)\|,$$

where the supremum is taken over maps $A_1, A_2, A_3 : \mathbb{Z}_n \to \mathbb{C}^{d\times d}$ such that $\|A_i(a)\| \leq 1$ and $[A_i(a), A_j(b)] = [A_i(a), A_j(b)^*] = 0$ for all $i \neq j$ and $a, b \in \mathbb{Z}_n$. Note that the only difference with the iccb norm defined in Section 2 is the second commutation relation involving the complex conjugates. This norm can also be stated in terms of tensor products and the supremum is attained by observable-valued maps. As such, this norm appears naturally in the context of non-local games. It was shown in [4] that Proposition 7 also holds for the jointly completely bounded norm, that is $\|f\|_{\mathrm{jcb}} \leq n^2\|f_0\|_{U^3}$. The proof of Corollary 6 easily implies that $\|f\|_{\mathrm{iccb}} \geq \|f\|_2^2/\Delta(f)$. This was used in [8] to prove that the jcb and iccb norms are inequivalent.

3.3 SDPs for quantum query complexity

Theorem 3 is based on an SDP for the completely bounded approximate degree of Gribling and Laurent [11]. The following notation will be convenient to state the SDP. Let $\mathcal{F}(n,t)$ be the set of functions $f : [n]^t \to \mathbb{R}$ of the form

$$f(\mathbf{i}) = \langle u, A_1(i_1)\cdots A_t(i_t)v\rangle,$$

where $u, v \in S^{d-1}$ and $A_1, \ldots, A_t : [n] \to \{M \in \mathbb{R}^{d\times d} : \|M\| \leq 1\}$ for some $d \in \mathbb{N}$. A basic linear algebra argument shows that any such function can be obtained by setting $d = n^t$. Given a function $\phi : \{-1,1\}^n \to \mathbb{R}$, a sequence $\mathbf{i} \in [n+1]^t$ and setting $x_{n+1} = 1$, define

$$\hat{\phi}(\mathbf{i}) = \mathbb{E}_{x\in\{-1,1\}^n}\phi(x)\prod_{j=1}^{t} x_{i_j}.$$

Note that if

$$\phi(x) = \sum_{S\in\binom{[n]}{t}} c_S\chi_S(x)$$

is a multilinear form of degree t, then

$$\hat{\phi}(\mathbf{i}) = \begin{cases} c_S & \text{if } \{i_1, \ldots, i_t\} = S \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

Given $f : \{-1,1\}^n \to [-1,1]$ and $t \in \mathbb{N}$, define

$$\begin{aligned} \mathrm{SDP}(f,t) = \max\ & \mathbb{E}_{x\in\{-1,1\}^n}\phi(x)f(x) - w \\ \text{s.t.}\ & \phi : \{-1,1\}^n \to \mathbb{R},\ w \in \mathbb{R} \\ & \|\phi\|_1 = 1 \\ & (1/w)\hat{\phi} \in \mathcal{F}(n+1,t). \end{aligned} \tag{11}$$

Program (11) corresponds to the optimization problem (24) of [11] for total functions and is written in a more convenient way for our purposes. There, f is considered to take values in $\{-1,1\}$, but their results still hold if f is allowed to take values in $\mathbb{R}$, as we do here. Also, we must point out that the $A_i(i_s)$ used in the program (24) of [11] are unitaries, but there is no problem if we substitute them by contractions, thanks to the fact that every contraction can be seen as the top left corner of an unitary matrix [2, Lemma 7].

▶ **Theorem 9** (Gribling-Laurent). *If the optimal value of program* (11) *is stricly larger than* ε*, then there is no* $\lfloor t/2\rfloor$*-query algorithm* $\mathcal{A}$ *such that* $|\mathbb{E}(\mathcal{A}(x)) - f(x)| \leq \varepsilon$.

3.4 Approximation of quadratic forms

Theorem 1 implies that bounded quadratic polynomials can be approximated by one-query quantum algorithms with error at most $1 - C$. Moreover, for $2n$-variate bounded bilinear forms $f(x, y) = x^{\mathsf{T}} A y$ for $A \in \mathbb{R}^{n \times n}$, we can C to be $1/K_G(n)$, where $K_G(n)$ is the real Grothendieck constant of dimension n (see [3] for a short proof). Then, bounded bilinear forms can be approximated with an additive error of at most $1 - 1/K_G(n)$. Using Theorem 9, we show that this is optimal for $n = 2$, in which case $K_G(2) = \sqrt{2}$ [10].

▶ **Proposition 10.** *There exists a bilinear form $f \in \mathbb{R}[x_1, x_2, x_3, x_4]$ such that there is no one-query quantum algorithm that approximates f on every $x \in \{-1, 1\}^4$ with an additive error smaller than $1 - 1/\sqrt{2}$.*

Proof. We use the bilinear form that attains the Grothendieck constant of dimension 2, which is captured by the CHSH game. This form $f \in \mathbb{R}[x_1, x_2, x_3, x_4]$ is given by

$$f(x) = \frac{1}{2}\big(x_1(x_3 + x_4) + x_2(x_3 - x_4)\big).$$

Clearly f maps $\{-1, 1\}^4$ to $\{-1, 1\}$, and so $\|f\|_1 = \|f\|_2^2 = 1$. We now emulate the construction from Lemma 5. Writing the coefficients of f as c_S for $S \in \binom{[4]}{2}$, for each $i \in [4]$ define the unit vector $w_i \in \mathbb{R}^4$ by

$$w_i = \frac{1}{\sqrt{2}} \sum_{j \in [4] \setminus \{i\}} c_{\{i,j\}} e_j.$$

Now define the matrices $A_i \in \mathbb{R}^{6 \times 6}$ by

$$A(i) = \begin{pmatrix} 0 & 0 & 0 \\ w_i & 0 & 0 \\ 0 & e_i^{\mathsf{T}} & 0 \end{pmatrix}.$$

It is easily verified that $A(i)^2 = 0$ and that the $(6, 1)$-coordinate of $A(i)A(j)$ equals $c_{\{i,j\}}/\sqrt{2}$ if $i \neq j$, from which it also follows that these matrices commute. Setting $A(5) = 0$, we get that

$$\langle e_6, A(i)A(j)e_1 \rangle = \begin{cases} \frac{c_{\{i,j\}}}{\sqrt{2}} & \text{if } \{i, j\} \in \binom{[4]}{2} \\ 0 & \text{otherwise.} \end{cases}$$

Setting $\phi = f$ then gives that $\sqrt{2}\phi \in \mathcal{F}(5, 2)$ and $\|\phi\|_1 = 1$. This shows that $\mathrm{SDP}(f, 2) \geq 1 - 1/\sqrt{2}$. ◀

Proposition 10 leads to a following natural question:

▶ **Question 1.** *Is it true that for any $\varepsilon > 0$ there are an integer n and a bounded bilinear form $f \in \mathbb{R}[x_1, \ldots, x_{2n}]$ such that there is no one-query quantum algorithm that approximates f on every $x \in \{-1, 1\}^{2n}$ with an error smaller than $1 - \frac{1}{K_G} - \epsilon$?*

3.5 Approximation of cubic forms

Given that a generalization of Theorem 1 has been ruled out for quartic polynomials, one may wonder if a weaker converse for the polynomial method is possible:

▶ **Question 2.** *Are there constants $C > 0$ and $\varepsilon > 0$ such that for every bounded polynomial f of degree 4 there is a 2-query algorithm $\mathcal{A}$ such that $|\mathbb{E}(\mathcal{A}(x)) - Cf(x)| < \varepsilon$ for every $x \in \{-1,1\}^n$?*

An affirmative answer to this question would imply that every polynomial of degree 4 could be approximated by a 2-query algorithm with additive error $1 - C + \varepsilon$. This would be the converse for the polynomial method that motivated Theorem 1 in [2]. Theorem 3 means that the ε appearing in Question 2 cannot be arbitrarily small. In other words, Theorem 3 says that there is no multiplicative converse even if we allow an (arbitrarily) small additive error.

Proof of Theorem 3. Let $f \in \mathbb{R}[x_1, \dots, x_n]$ be a bounded multilinear cubic form as in (1). As shown in the proof of Corollary 6, there exist unit vectors $u, v \in \mathbb{R}^d$ and mappings $A : \{0, 1, \dots, n+1\} \to \mathbb{R}^{d \times d}$ such that $\|A(i)\| \leq 1$ for each i and

$$\big\langle u, A(i)A(j)A(k)A(l)v \big\rangle = \begin{cases} \frac{c_S}{\Delta(f)} & \text{if } \{i,j,k,l\} = \{0\} \cup S \text{ for } S \in \binom{[n]}{3} \\ 0 & \text{otherwise.} \end{cases}$$

Let $g = x_0 f / \|f\|_\infty$. Then, the function $\phi = x_0 f / \|f\|_1$ meets the criteria of (11) with $w = \Delta(f)/\|f\|_1$ and shows that

$$\begin{aligned} \mathrm{SDP}(g, 4) &\geq \frac{\|f\|_2^2}{\|f\|_1 \|f\|_\infty} - \frac{\Delta(f)}{\|f\|_1} \\ &\geq \frac{\|f\|_2^2}{\|f\|_1 \|f\|_\infty} \Big(1 - \frac{\Delta(f)\|f\|_\infty}{\|f\|_2^2} \Big). \end{aligned}$$

If f is the random example from Section 3.1, then $\|f\|_2^2 = \binom{n}{3}$ and $\Delta(f)\|f\|_\infty \leq Cn^{5/2}$ with high probability. In particular, the above is positive for sufficiently large n. Similarly, for any $C \in (0,1)$ we get that $\mathrm{SDP}(Cg, 4) > 0$ for sufficiently large n. The result now follows from Theorem 9. ◀

References

1. Scott Aaronson. Open problems related to quantum query complexity. *ACM Transactions on Quantum Computing*, 2(4):1–9, 2021.
2. 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*, pages 25:1–25:19, 2016. arXiv:1511.08682.
3. 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.
4. Tom Bannink, Jop Briët, Harry Buhrman, Farrokh Labib, and Troy Lee. Bounding Quantum-Classical Separations for Classes of Nonlocal Games. In *36th International Symposium on Theoretical Aspects of Computer Science (STACS 2019)*, volume 126 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 12:1–12:11, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. Available at arXiv:1811.11068. doi:10.4230/LIPIcs.STACS.2019.12.
5. Nikhil Bansal, Makrand Sinha, and Ronald de Wolf. Influence in completely bounded block-multilinear forms and classical simulation of quantum algorithms. *arXiv preprint*, 2022. arXiv:2203.00212.
6. 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.

7 S. Boucheron, G. Lugosi, and P. Massart. *Concentration inequalities: A nonasymptotic theory of independence*. Oxford university press, 2013.

8 Jop Briët and Carlos Palazuelos. Failure of the trilinear operator space Grothendieck inequality. *Discrete Analysis*, 2019. Paper No. 8.

9 Mark Bun, Robin Kothari, and Justin Thaler. The polynomial method strikes back: Tight quantum query bounds via dual polynomials. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC'18)*, pages 297–310, 2018.

10 Peter C Fishburn and James A Reeds. Bell inequalities, Grothendieck's constant, and root two. *SIAM Journal on Discrete Mathematics*, 7(1):48–56, 1994.

11 Sander Gribling and Monique Laurent. Semidefinite programming formulations for the completely bounded norm of a tensor. *arXiv preprint*, 2019. arXiv:1901.04921.

12 Godfrey Harold Hardy, Edward Maitland Wright, et al. *An introduction to the theory of numbers*. Oxford university press, 1979.

13 Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2009. doi:10.1017/cbo9781139814782.

14 Gilles Pisier. Grothendieck's theorem, past and present. *Bulletin of the American Mathematical Society*, 49(2):237–323, 2012.

15 T. Tao. *Topics in Random Matrix Theory*. Graduate studies in mathematics. American Mathematical Society, 2012. URL: https://books.google.nl/books?id=L51VAwAAQBAJ.

16 Terence Tao and Joni Teräväinen. Quantitative bounds for Gowers uniformity of the Möbius and von Mangoldt functions. *arXiv preprint*, 2021. arXiv:2107.02158.

17 Terence Tao and Van H Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006.

18 B. S. Tsirelson. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 1980. doi:10.1007/BF00417500.

19 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.