Quantum computing, norms and polynomials

Escudero Gutiérrez, F.

Chapter 4

Grothendieck inequalities characterizes converses to the polynomial method

4.1 Introduction

For a Boolean function $f : D \to \{-1, 1\}$ defined on a set $D \subseteq \{-1, 1\}^n$, the celebrated *polynomial method* of Beals, Buhrman, Cleve, Mosca and de Wolf [BBC+01], introduced in Chapter 3, gives a lower bound on the quantum query complexity of f in terms of the approximate degree. Using this method, many well-known quantum algorithms were proved to be optimal in terms of query complexity (see e.g., [BKT20] and references therein).

Since polynomials are simpler objects than quantum query algorithms, it is of interest to know how well approximate degree approximates quantum query complexity. There are total functions f that satisfy $Q(f) \geq \widetilde{\deg}(f)^c$ for some absolute constant $c > 1$ [Amb06, ABDK16]; the second reference gives an exponent $c = 4 - o(1)$, which was shown to be optimal in [ABDK16]. For partial functions it was recently shown that this separation can even be exponential [AB23]. These separations rule out a direct converse to the polynomial method, whereby a given bounded degree-$2t$ polynomial p can be computed by a t-query quantum algorithm $\mathcal{A}$. However, since these results concern functions whose approximate degree grows with n, they leave room for the possibility that such an $\mathcal{A}$ approximates p with some error that depends on t.

For bounded polynomials of degree at most 2, a *multiplicative converse* to the polynomial method was proved in [AAI+16], showing that up to an absolute constant scaling, quadratic polynomials can indeed be computed by 1-query quantum algorithms.

Theorem 4.1 (Quadratic multiplicative converse [AAI+16])**.** *There exists an absolute constant $C \in (0,1]$ such that $\mathcal{E}(Cp,1) = 0$ for every bounded polynomial p of degree at most 2.*

This result directly implies the following *additive* version.

Corollary 4.2 (Quadratic additive converse)**.** *There exists an absolute constant $\varepsilon \in (0,1)$ such that the following holds. For every bounded polynomial p of degree at most 2, we have $\mathcal{E}(p,1) \leq \varepsilon$. In particular, one can take $\varepsilon = 1 - C$ for the constant C appearing in Theorem 4.1.*

In light of the polynomial method, Corollary 4.2 shows that one-query quantum algorithms are roughly equivalent to bounded quadratic polynomials. The authors of [AAI+16] asked whether this result generalizes to higher degrees. Two ways to interpret this question are that for any k, any bounded degree-$2k$ polynomial p satisfies:

(a) Multiplicative converse: $\mathcal{E}(Cp,k) = 0$ for some $C = C(k) > 0$, or;

(b) Additive converse: $\mathcal{E}(p,k) \leq \varepsilon$ for some $\varepsilon = \varepsilon(k) < 1$.

The dependence on the degree k in these options is necessary due to the known separations between bounded-error quantum query complexity and approximate degree. Option (a), the higher-degree version of Theorem 4.1, was ruled out in [ABP19].

Theorem 4.3. *For any $C > 0$, there exist an $n \in \mathbb{N}$ and a bounded quartic n-variable polynomial p such that no two-query quantum algorithm $\mathcal{A}$ satisfies $\mathbb{E}[\mathcal{A}(x)] = Cp(x)$ for every $x \in \{-1,1\}^n$.*

Note that Option ((a)) with C implies Option ((b)) with $1 - C$, but Theorem 4.3 does not rule out Option ((a)).

Contributions of this chapter

Our first contribution concerns an error in the original proof of Theorem 4.3, which was based on a probabilistic example. Here, we show that Theorem 4.3 holds as stated, both by considering a slightly modified probabilistic example and by giving a completely explicit example. More importantly, we prove a stronger result that subsumes Theorem 4.3: we rule out the possibility of Option ((b)).

Theorem 4.4. *There is no constant $\varepsilon \in (0,1)$ such that for every bounded polynomial p of degree at most 4, we have $\mathcal{E}(p,2) \leq \varepsilon$.*

In the context of quantum query complexity of Boolean functions, this rules out arguably the most natural way to *upper* bound $Q(f)$ in terms of $\widetilde{\deg}(f)$: First, ε-approximate f by a degree-$2t$ polynomial p, then ε'-approximate p with a t-query quantum algorithm $\mathcal{A}$, with $\varepsilon + \varepsilon' < 1$, and finally boost the success probability of $\mathcal{A}$ so that it approximates f, for instance by taking the majority of independent runs of $\mathcal{A}$. Corollary 4.2 gives the only exceptional case where this is possible in general.

Our second contribution concerns 1-query quantum algorithms. For the case of bilinear forms, Theorem 4.1 was proved using a surprising application of the famous Grothendieck theorem (see Section 2.7.1). The general form of Theorem 4.1 follows from decoupling techniques. In this chapter, we show that the additive approximation implied by Theorem 4.1 is optimal.

Theorem 4.5. *The worst-case minimum error for one-query quantum algorithms satisfies*

$$\sup_p \mathcal{E}(p,1) = 1 - \frac{1}{K_G^{\mathbb{R}}},$$

where the supremum is taken over the set of bounded bilinear forms.

This complements another well-known characterization of $K_G^{\mathbb{R}}$ in terms of the largest-possible Bell-inequality violations in two-player XOR games [Tsi80].

The main technical result of this chapter

Both Theorems 4.3 and 4.4 are in fact corollaries of our main result (Theorem 4.13 below), which gives a formula for $\mathcal{E}(p,t)$ when p is a block-multilinear form. Block-multilinear forms already played an important role in other works related to quantum query complexity [OZ15, AAI+16, BSdW22], theoretical computer science [KN07, Lov10, KM13] and in the polarization theory of functional analysis [BH31, Har72].

The formula characterizes $\mathcal{E}(p,t)$ in terms of a ratio of norms appearing naturally in Grothendieck's theorem for bilinear forms (see Section 2.7.1). The dual formulation of Grothendieck's theorem asserts that for any bilinear form $A : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$,

$$\|A\|_{\infty,*} \leq K_G^{\mathbb{R}} \|A\|_{\mathrm{cb},*}.$$

Similar norms can be defined for block-multilinear forms of higher degree. Endowing the space of polynomials with the standard inner product of the coefficient vectors in

the monomial basis, our formula for $\mathcal{E}(p,t)$ is as follows.

Theorem 4.6 (Informal version of Theorem 4.13)**.** *For a block-multilinear form p of degree $2t$, we have*

$$\mathcal{E}(p,t) = \sup_q \frac{\langle p,q\rangle - \|q\|_{\mathrm{cb},*}}{\|q\|_{\infty,*}}.$$

where the supremum runs over all block-multilinear forms q of degree $2t$.

The proof of Theorem 4.6 uses a characterization of quantum query algorithms in terms of completely bounded polynomials [ABP19].

Theorems 4.4 and 4.5 follow from Theorem 4.6 by taking suprema over particular sequences of bounded degree-$2t$ block-multilinear forms. From Theorem 4.6 it follows that

$$\sup_p \mathcal{E}(p,t) = \sup_q \left[\left(\sup_p \frac{\langle p,q\rangle}{\|q\|_{\infty,*}}\right) - \frac{\|q\|_{\mathrm{cb},*}}{\|q\|_{\infty,*}}\right] = 1 - \inf_q \frac{\|q\|_{\mathrm{cb},*}}{\|q\|_{\infty,*}}. \tag{4.1}$$

Now, Theorem 4.5 follows from Eq. (4.1) and the dual version of Grothendieck's inequality (Section 4.1). Similarly, Theorem 4.4 is proven by using Eq. (4.1) and constructing a family of degree-4 polynomials $(p_n)_n$ that witnesses the failure of Grothendieck inequality. By this we mean that $(p_n)_n$ exhibit the separation

$$\frac{\|p_n\|_{\mathrm{cb}}}{\|p_n\|_\infty} \to \infty. \tag{4.2}$$

By duality this implies that there is a sequence $(r_n)_n$ with $\|r_n\|_{\mathrm{cb},*}/\|r_n\|_{\infty,*} \to 0$, which alongside Eq. (4.1) implies that $\sup_p \mathcal{E}(p,2) = 1$, as desired.

4.2 Preliminaries

Polynomials, norms and quantum query complexity

As usual we let $\mathbb{R}[x_1,\ldots,x_n]$ be the ring of n-variate polynomials with real coefficients, whose elements we write as

$$p(x) = \sum_{\alpha\in\mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha, \tag{4.3}$$

where $x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ and $c_\alpha \in \mathbb{R}$. We define the support of p by

$$\mathrm{supp}(p) = \{\alpha \in \mathbb{Z}^n_{\geq 0} \mid c_\alpha \neq 0\}.$$

For $\alpha \in \mathbb{Z}^n_{\geq 0}$, write $|\alpha| = \alpha_1 + \cdots + \alpha_n$, which is the degree of the monomial x^α. A form of degree d is a homogeneous polynomial of degree d, i.e., a polynomial whose support consists of α for which $|\alpha| = d$. Denote by $\mathbb{R}[x_1, \ldots, x_n]_{=d}$ the space of forms of degree d. For p as in Eq. (4.3), define its homogeneous degree-d part by

$$p_{=d}(x) = \sum_{|\alpha|=d} c_\alpha x^\alpha.$$

We endow $\mathbb{R}[x_1, \ldots, x_n]$ with the inner product given by

$$\langle p, q \rangle = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha c'_\alpha,$$

where c_α and c'_α are the coefficients of p and q, respectively.

We recall the definition of $\|\cdot\|_1$ and $\|\cdot\|_\infty$, which are seminorms of polynomials in $\mathbb{R}[x_1, \ldots, x_n]$, and norms on the space of multilinear polynomials.

$$\|p\|_\infty := \sup_{x \in \{-1,1\}^n} |p(x)|,$$
$$\|p\|_1 := \mathbb{E}_{x \in \{-1,1\}^n} |p(x)|,$$

where the expectation is taken with respect to the uniform probability measure.

We will work with a reformulation of the completely bounded polynomial method, Theorem 3.6. To state it, we define the completely bounded norm of a form p.

Definition 4.7. Let $p \in \mathbb{R}[x_1, \ldots, x_n]_{=t}$. Then, its completely bounded norm is defined by

$$\|p\|_{\mathrm{cb}} = \inf \Big\{ \|T\|_{\mathrm{cb}} \mid p(x) = T(x, \ldots, x) \ \forall x \in \mathbb{R}^n \Big\},$$

where the infimum runs over all t-linear forms $T : \mathbb{R}^n \times \cdots \times \mathbb{R}^n \to \mathbb{R}$.

Note that we are slightly abusing notation because we have introduced two notions of completely bounded norm for t-linear forms $T : \mathbb{R}^n \times \cdots \times \mathbb{R}^n \to \mathbb{R}$. The first one in Definition 2.17, where we regard T as a multilinear form. Furthermore, such T can also be regarded as a homogeneous polynomial in n^t variables, so we have defined a second notion of completely bounded norm for it in Definition 4.7. For the rest of the chapter, we will use the definition of Definition 4.7. However, to prove Theorem 4.5 we should show that for bilinear forms both norms are equal (see Proposition 4.25 below).

Now, we can restate Theorem 3.6.[1]

Theorem 4.8 (Completely bounded polynomial method)**.** *Let* $p : \{-1,1\}^n \to [-1,1]$ *and let* $t \in \mathbb{N}$*. Then,*

$$\begin{aligned}\mathcal{E}(p,t) = \inf \quad & \|p-q\|_\infty \\ \text{s.t.} \quad & h \in \mathbb{R}[x_1,\dots,x_{n+1}]_{=2t} \text{ with } \|h\|_{\text{cb}} \le 1 \\ & q : \{-1,1\}^n \to \mathbb{R}, \text{ with } q(x) = h(x,1) \ \forall\ x \in \{-1,1\}^n.\end{aligned}$$

Block-multilinear forms

Theorem 4.13 is stated for a special kind of polynomials, which are the block-multilinear forms.

Definition 4.9. Let $\mathcal{P} = \{I_1,\dots,I_t\}$ be a partition of $[n]$ into t (pairwise disjoint) non-empty subsets. Define the set of *block-multilinear polynomials with respect to* $\mathcal{P}$ to be the linear subspace

$$V_{\mathcal{P}} = \text{Span}\left\{x_{i_1}\cdots x_{i_t} \mid i_1 \in I_1,\dots,i_t \in I_t\right\}.$$

We also work with the larger space of polynomials spanned by monomials where in the above we replace linearity by odd degree.

Definition 4.10. For a family $\mathcal{Q} \subseteq 2^{[m]}$ of pairwise disjoint subsets, let $W_{\mathcal{Q}} \subseteq \mathbb{R}[x_1,\dots,x_m]$ be the subspace of polynomials spanned by monomials x^α with $\alpha \in \mathbb{Z}^m_{\ge 0}$ satisfying

$$\sum_{i\in I} \alpha_i \equiv 1 \bmod 2 \ \forall I \in \mathcal{Q}. \tag{4.4}$$

We use $\Pi_{\mathcal{Q}} : \mathbb{R}[x_1,\dots,x_m] \to W_{\mathcal{Q}}$ to refer to the projector onto $W_{\mathcal{Q}}$.

Remark 4.11. Given a partition $\mathcal{P}$ of $[n]$, we have $V_{\mathcal{P}} \subset W_{\mathcal{P}}$. In particular, $V_{\mathcal{P}}$ consists of precisely the multilinear polynomials in $W_{\mathcal{P}}$.

Although the projector $\Pi_{\mathcal{Q}}$ onto $W_{\mathcal{Q}}$ is properly defined on the space of polynomials of n variables, we will slightly abuse notation and let it act on a t-tensor $T \in \mathbb{R}^{n\times\cdots\times n}$ as follows. Define $\mathcal{I}_{\mathcal{Q}} \subseteq [n]^t$ to be the set of t-tuples that contain an odd number of

[1] A direct reformulation of Theorem 3.6 would be with the polynomial h below belonging to $\mathbb{R}[x_1,\dots,x_{2n}]_{=2t}$, instead of $\mathbb{R}[x_1,\dots,x_{n+1}]_{=2t}$, However, in [GL19] it was observed that only *one extra variable* is needed.

elements from each set in $\mathcal{Q}$. Then, we let $\Pi_{\mathcal{Q}} T$ be the tensor given by

$$(\Pi_{\mathcal{Q}} T)_{\mathbf{i}} := \begin{cases} T_{\mathbf{i}} & \text{if } \mathbf{i} \in \mathcal{I}_{\mathcal{Q}}, \\ 0 & \text{otherwise.} \end{cases} \tag{4.5}$$

It is not hard to see that if p is a polynomial satisfying $T(x, \dots, x) = p(x)$ for every $x \in \{-1, 1\}^n$, then $\Pi_{\mathcal{Q}} T(x, \dots, x) = \Pi_{\mathcal{Q}} p(x)$ for every $x \in \{-1, 1\}^n$.

We note that all the norms and seminorms we have mentioned are norms on the space $V_{\mathcal{P}}$ for any partition $\mathcal{P}$ of $[n]$. Hence, we can take the dual of these norms with respect to this subspace, so from now on $\|p\|_{\infty,*}$ and $\|p\|_{\mathrm{cb},*}$ will be the dual of $\|p\|_{\infty}$ and $\|p\|_{\mathrm{cb}}$ of $V_{\mathcal{P}}$, respectively. By contrast, when we write $\|R\|_{\mathrm{cb},*}$ for some t-tensor $\mathbb{R}^{n \times \cdots \times n}$ we refer to the dual norm of the completely bounded norm of R with respect to the whole space of t-tensors.

We stress that $\|\cdot\|_{\infty,*}$ need not be equal to $\|\cdot\|_1$. This is because we are taking the dual norms with respect to $V_{\mathcal{P}}$ and not with respect to the space of all multilinear maps, in which case the dual norm would be $\|p\|_1$. The following example shows that $\|p\|_{\infty,*} \neq \|p\|_1$ in general.

Example 4.12. Consider $n = 3$, $t = 1$ and $p = (x_1 + x_2 + x_3)/3$. Then, $\|p\|_1 > 1/3$, but $\|p\|_{\infty,*} \leq 1/3$. Indeed, as $|p(x)| \geq 1/3$ for every $x \in \{-1, 1\}^3$ and $|p(x)| > 1/3$ for some $x \in \{-1, 1\}^3$, we have that $\|p\|_1 > 1/3$. On the other hand, in this case $\mathcal{P} = \{[3]\}$ so $V_{\mathcal{P}}$ is the set of linear polynomials. Note that if q is linear, then $\|\hat{q}\|_1 = \|q\|_{\infty}$, where $\hat{q}$ is the Fourier transform of q. Hence

$$\|p\|_{\infty,*} = \sup_{q \in V_{\mathcal{P}}, \|q\|_{\infty} \leq 1} \langle p, q \rangle = \sup_{q \in V_{\mathcal{P}}, \|\hat{q}\|_1 \leq 1} \langle \hat{p}, \hat{q} \rangle \leq \sup_{\|\hat{q}\|_1 \leq 1} \|\hat{p}\|_{\infty} \|\hat{q}\|_1 = \frac{1}{3},$$

where in second equality we used Parseval's identity.

4.3 $\mathcal{E}(p, t)$ for block-multilinear forms

In this section we formally state and prove our main result:

Theorem 4.13. *Let $\mathcal{P}$ be a partition of $[n]$ in $2t$ subsets and $p \in V_{\mathcal{P}}$. Then,*

$$\mathcal{E}(p, t) = \sup \left\{ \langle p, r \rangle - \|r\|_{\mathrm{cb},*} \mid r \in V_{\mathcal{P}}, \ \|r\|_{\infty,*} \leq 1 \right\}.$$

For the proof, we use more convenient expressions for the completely bounded norms and the fact that the projector Π_Q is contractive under several norms.

Contractivity of the projector Π_Q.

A key element of the proof of Theorem 4.13 is that can restrict the infimum in Theorem 4.8 to the space of polynomials $W_{\mathcal{Q}}$ given in Definition 4.10. To do that, we prove that the orthogonal projector onto this space, $\Pi_{\mathcal{Q}}$ is contractive in several norms. This will follow from the fact that $\Pi_{\mathcal{Q}}$ has a particularly nice structure in the form of an averaging operator. Let $\mathcal{Q}$ be a family of disjoint subsets of $[n]$. For each $I \in \mathcal{Q}$ let z_I be a random variable that takes the values -1 and 1 with probability $1/2$ and let $z = (z_I)_{I\in\mathcal{Q}}$. For a bit string $x \in \{-1,1\}^n$, we define the random variable $x \cdot z \in \{-1,1\}^n$ as

$$(x \cdot z)(i) := \begin{cases} x_i z_I & \text{if } i \in I \text{ for some } I \in \mathcal{Q}, \\ x_i & \text{otherwise.} \end{cases}$$

For a matrix-valued map $A : [n] \to M(d)$ we define the random variable $A \cdot z$ in an analogous way.

Proposition 4.14. *For any $p \in \mathbb{R}[x_1, \ldots, x_n]$ and $x \in \mathbb{R}^n$, we have that*

$$\Pi_{\mathcal{Q}} p(x) = \mathbb{E}_z \Big[p(x \cdot z) \prod_{I\in\mathcal{Q}} z_I \Big].$$

Similarly, for any t-tensor $T \in \mathbb{R}^{n\times\cdots\times n}$, positive integer d and matrix-valued map $A\colon [n] \to M(d)$, we have that

$$\Pi_{\mathcal{Q}} T(A) = \mathbb{E}_z \left[T(A \cdot z) \prod_{I\in\mathcal{Q}} z_I \right].$$

Proof. By linearity, it suffices to prove the equality for monomials. Let $\alpha \in \mathbb{Z}^n_{\geq 0}$. Then we have

$$(x \cdot z)^\alpha \prod_{I\in\mathcal{Q}} z_I = x^\alpha \prod_{I\in\mathcal{Q}} z_I^{1+\sum_{i\in I}\alpha_i}.$$

It follows that

$$\mathbb{E}_z \Big[(x \cdot z)^\alpha \prod_{I\in\mathcal{Q}} z_I \Big] = \begin{cases} x^\alpha & \text{if } 1 + \sum_{i\in I} \alpha_i = 0 \bmod 2 \ \forall I \in \mathcal{Q}, \\ 0 & \text{otherwise.} \end{cases}$$

It remains to observe that this is precisely the projection of x^α on $W_{\mathcal{Q}}$. The statement for tensors follows analogously. □

Finally, we prove that $\Pi_{\mathcal{Q}}$ is contractive with respect to the relevant norms.

Lemma 4.15. *Let $\mathcal{Q}$ be a family of disjoint subsets of $[n]$ and $p \in \mathbb{R}[x_1, \ldots, x_n]$ and let* norm $\in \{\mathrm{cb}, \infty, 1\}$ *where for the* cb*-norm we moreover require p to be homogeneous. Then*

$$\|\Pi_{\mathcal{Q}} p\|_{\mathrm{norm}} \leq \|p\|_{\mathrm{norm}}.$$

Proof. First, we consider the $\|\cdot\|_\infty$ norm. For every $x \in \{-1,1\}^n$, we have that $x \cdot z \in \{-1,1\}^n$, so

$$|\Pi_{\mathcal{Q}} p(x)| \leq \mathbb{E}_z |p(x \cdot z) \prod_{I \in \mathcal{Q}} z_I| = \mathbb{E}_z |p(x \cdot z)| \leq \mathbb{E}_z \|p\|_\infty = \|p\|_\infty,$$

where in the first inequality we used Proposition 4.14 and the triangle inequality.

Second, we consider $\|\cdot\|_{\mathrm{cb}}$. Arguing as in the $\|\cdot\|_\infty$ case and using Definition 4.7, it follows that for any t-tensor $T \in \mathbb{R}^{n \times \cdots \times n}$ we have that $\|\Pi_{\mathcal{Q}} T\|_{\mathrm{cb}} \leq \|T\|_{\mathrm{cb}}$. Given that $\Pi_{\mathcal{Q}} p(x) = \Pi_{\mathcal{Q}} T(x)$ if $p(x) = T(x)$, it follows that

$$\|\Pi_{\mathcal{Q}} p\|_{\mathrm{cb}} \leq \|\Pi_{\mathcal{Q}} T\|_{\mathrm{cb}} \leq \|T\|_{\mathrm{cb}}$$

for every t-tensor $T \in \mathbb{R}^{n \times \cdots \times n}$ such that $T(x) = p(x)$. Taking the infimum over all those T we arrive at $\|\Pi_{\mathcal{Q}} p\|_{\mathrm{cb}} \leq \|p\|_{\mathrm{cb}}$.

Finally, for $\|\cdot\|_1$ we have

$$\|\Pi_{\mathcal{Q}} p\|_1 = \mathbb{E}_x |\mathbb{E}_z p(x \cdot z) \prod_{I \in \mathcal{Q}} z_I| \leq \mathbb{E}_x \mathbb{E}_z |p(x \cdot z)| = \mathbb{E}_z \mathbb{E}_x |p(x)| = \|p\|_1,$$

where in the first equality we have used Proposition 4.14 and in the third we have used the fact that the uniform measure is invariant under multiplication by $z \in \{-1,1\}^n$. □

Putting everything together

We are now ready to prove Theorem 4.13. To this end, we start from the expression given in Theorem 4.8 for $\mathcal{E}(p,t)$ and let $h \in \mathbb{R}[x_1, \ldots, x_{n+1}]_{=2t}$ with $\|h\|_{\mathrm{cb}} \leq 1$ and let $q : \{-1,1\}^n \to \mathbb{R}$ be defined by $q(x) = h(x,1)$ for every $x \in \{-1,1\}^n$.

We first show that we can project q (and h) onto $W_{\mathcal{P}}$ and obtain a feasible solution whose objective value is at least as good as q. Since $\mathcal{P}$ is a partition of $[n]$, it defines a family of disjoint subsets of $[n+1]$, so by Lemma 4.15, we have $\|\Pi_{\mathcal{P}} h\|_{\mathrm{cb}} \leq \|h\|_{\mathrm{cb}} \leq 1$. Since the degree of h is at most $2t$, the polynomial $\Pi_{\mathcal{P}} h$ has degree at most $2t$.

This shows that each monomial in its support contains exactly one variable from each of the $2t$ sets in $\mathcal{P}$. We can therefore observe that $\Pi_{\mathcal{P}}h$ does not depend on x_{n+1}. Since $h(x,1) = q(x)$, we have $\Pi_{\mathcal{P}}h(x,1) = \Pi_{\mathcal{P}}q(x)$ and therefore $\Pi_{\mathcal{P}}q \in V_{\mathcal{P}}$. From Definition 4.7 follows that $\|\Pi_{\mathcal{P}}q\|_{\mathrm{cb}} \leq 1$. Indeed, applying $\Pi_{\mathcal{P}}$ to a $2t$-tensor $T \in \mathbb{R}^{(n+1)\times\cdots(n+1)}$ that certifies $\|h\|_{\mathrm{cb}} \leq 1$ results in a tensor $\Pi_{\mathcal{P}}T$ that satisfies $\Pi_{\mathcal{P}}T(\mathbf{i}) = 0$ whenever $\mathbf{i}$ contains an index equal to $n+1$. So, $\Pi_{\mathcal{P}}T(x,1) = \Pi_{\mathcal{P}}q(x)$ for every $x \in \{-1,1\}^n$ and thus $\Pi_{\mathcal{P}}T$, viewed as a $2t$-tensor in $\mathbb{R}^{n\times\cdots\times n}$, certifies $\|\Pi_{\mathcal{P}}q\|_{\mathrm{cb}} \leq 1$. For the objective value of $\Pi_{\mathcal{P}}q$ we finally observe that

$$\|p - \Pi_{\mathcal{P}}q\|_\infty = \|\Pi_{\mathcal{P}}(p-q)\|_\infty \leq \|p-q\|_\infty,$$

where we used that $p \in V_{\mathcal{P}}$ in the equality and Lemma 4.15 in the inequality. This shows that

$$\mathcal{E}(p,t) \geq \inf\{\|p-q\|_\infty \mid q \in V_{\mathcal{P}} \text{ with } \|q\|_{\mathrm{cb}} \leq 1\}.$$

To show that the above inequality is in fact an equality it suffices to observe that given a polynomial $q \in V_{\mathcal{P}}$, we can define $h \in \mathbb{R}[x_1,\ldots,x_{n+1}]$ as $h(x,x_{n+1}) = q(x)$ and then we have $\|h\|_{\mathrm{cb}} \leq \|q\|_{\mathrm{cb}}$.

Finally, in the above reformulation of $\mathcal{E}(p,t)$, we can express $\|p-q\|_\infty$ in terms of its dual norm and obtain

$$\begin{aligned}\mathcal{E}(p,t) = \inf_q \sup_r \quad & \langle p-q, r\rangle \\ \text{s.t.} \quad & q \in V_{\mathcal{P}} \text{ with } \|q\|_{\mathrm{cb}} \leq 1, \\ & r \in V_{\mathcal{P}} \text{ with } \|r\|_{\infty,*} \leq 1.\end{aligned}$$

Finally, we need the von Neumann's minimax theorem (see [Nik54] for a proof).

Theorem 4.16 (Minimax)**.** *Let X and Y convex compact sets. Let $f : X \times Y \to \mathbb{R}$ such that f is concave in the first variable and convex in the second. Then,*

$$\sup_{x\in X}\inf_{y\in Y} f(x,y) = \inf_{y\in Y}\sup_{x\in X} f(x,y).$$

The desired result then follows by exchanging the infimum and supremum, which we are allowed to do by Theorem 4.16.

4.4 Separations between infinity and completely bounded norms

In this section we show that the completely bounded norm of a degree 4 bounded polynomial can be unbounded. In other words, we prove the following Theorem.

Theorem 4.17. *There is a sequence $p_n \in \mathbb{R}[x_1, \dots, x_n]_{=4}$ such that*

$$\frac{\|p_n\|_{\mathrm{cb}}}{\|p_n\|_\infty} \to \infty.$$

To prove Theorem 4.17 we first provide a framework to lower bound the completely bounded norm inspired on a technique due to Varopoulos [Var74].[2] Second, we construct two sequences of bounded polynomials, one random and one explicit, that fit in that framework and have unbounded completely bounded norm.

Lower bounding the completely bounded norm

We will first talk about general cubic forms, that is polynomials given by:

$$p(x) = \sum_{S \in \binom{[n]}{3}} c_S \prod_{i \in S} x_i, \tag{4.6}$$

where the c_S are some real coefficients. We will lower bound its completely bounded norm. Then, we will extent this lower bound to an associated quartic form, given by $x_0 p(x)$. For $i \in [n]$, define the ith *slice* of p 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

$$\Delta(p) = \max_{i \in [n]} \|M_i\|_{\mathrm{op}}.$$

Lemma 4.18 (tri-linear Varopoulos decomposition)**.** *Let p be an n-variate multilinear cubic form as in* (4.6)*. Then, for some $d \in \mathbb{N}$, there exist contractions $A(1), \dots, A(n) \in$*

[2] We use the same construction as the one proposed by Varopoulos, but we apply it to multilinear polynomials, which gives it the extra property displayed in Eq. (4.7)

M_d and orthogonal vectors $u, v \in S^{d-1}$ such that $[A(j), A(i)] = 0$, and

$$A(i)^2 = 0 \tag{4.7}$$

$$\langle u, A(i)v \rangle = 0 \tag{4.8}$$

$$\langle u, A(i)A(j)v \rangle = 0 \tag{4.9}$$

$$\langle u, A(i)A(j)A(k)v \rangle = \frac{c_{\{i,j,k\}}}{\Delta(p)} \tag{4.10}$$

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

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

$$A(i) = \left[\begin{array}{c|c|c|c} & & & \\ \hline e_i & & & \\ \hline & W_i^{\mathsf{T}} & & \\ \hline & & e_i^{\mathsf{T}} & \end{array}\right],$$

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 [BP19, Lemma 2.11], except for the property that $A(i)^2 = 0$. This follows from the fact that

$$A(i)^2 = \left[\begin{array}{c|c|c|c} & & & \\ \hline & & & \\ \hline W_i^{\mathsf{T}} e_i & & & \\ \hline & e_i^{\mathsf{T}} W_i^{\mathsf{T}} & & \end{array}\right]$$

and that the ith row and ith column of M_i (and hence W_i) are zero. □

Corollary 4.19. *Let p be an n-variate multilinear cubic form as in (4.6). Suppose that an $(n+2)$-variate quartic form $h \in \mathbb{R}[x_0, x_1, \ldots, x_n, z]$ satisfies $h(x, 1) = x_0 p(x_1, \ldots, x_n)$ for every $x \in \{-1, 1\}^{n+1}$. Then,*

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

Proof. From the orthonormality of the characters, it follows that h and $x_0 p$ 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 $A(1), \ldots, A(n) \in B_{M_d}$ and $u, v \in S^d$ be as in Lemma 4.18, and extend A by $A(0) = I, A(n+1) = 0$.

Commutativity and properties (4.7)–(4.9) imply that if a quartic monomial expression $A((i,j,k,l))$ with $i,j,k,l \in \{0,\dots,n+1\}$ has repeated indices or an index equal to $n+1$, then $\langle u, A((i,j,k,l))v\rangle = 0$. With this, it follows that, for every T_h such that $T_h(x,\dots,x) = h(x)$, we have

$$\|T_h\|_{\mathrm{cb}} \geq \sum_{\mathbf{i}\in(\{0\}\cup[n+1])^4} T_{\mathbf{i}}\Big\langle u, A(\mathbf{i})v\Big\rangle = \sum_{S\in\binom{[n]}{3}} c_S\Big\langle u,\, A(0)\prod_{i\in S} A(i)v\Big\rangle. \tag{4.11}$$

Finally, if we use that $A(0) = \mathrm{Id}$, property (4.10) and Parseval's identity, we obtain the desired result:

$$\|h\|_{\mathrm{cb}} = \inf\|T_h\|_{\mathrm{cb}} \geq \sum_{S\in\binom{[n]}{3}} c_S\langle u, \prod_{i\in S} A(i)v\rangle = \Delta(p)^{-1}\sum_{S\in\binom{[n]}{3}} c_S^2 = \frac{\|p\|_2^2}{\Delta(p)}.$$

□

A separation based on a random example

We begin by defining a random cubic form as in (4.6) where the coefficients c_S are chosen to be independent uniformly distributed random signs. Parseval's identity then gives $\|p\|_2^2 = \binom{n}{3}$. We now use a standard random-matrix inequality to upper bound $\Delta(p)$ (see [Tao12, Corollary 2.3.6] for a proof).

Lemma 4.20. *There exist absolute constants $C, c \in (0,\infty)$ such that the following holds. Let n be a positive integer and let M be a random $n\times n$ symmetric random matrix such that for $j \geq i$, the entries M_{ij} are independent random variables with mean zero and absolute value at most 1. Then, for any $\tau \geq C$, we have*

$$\Pr\big[\|M\|_{\mathrm{op}} > \tau\sqrt{n}\big] \leq Ce^{-c\tau n}.$$

Applying Lemma 4.20 to the slices M_i and the union bound then imply that $\Delta(p) \leq C\sqrt{n}$ with probability $1-\exp(-Cn)$. By Hoeffding's inequality [BLM13, Theorem 2.8] and the union bound, we have that $\|p\|_\infty \leq Cn^2$ with probability $1-\exp(-Cn)$. Rescaling p then gives that there exists a bounded multilinear cubic form such that $\|p\|_2^2/\Delta(p) \geq C\sqrt{n}$. Now Theorem 4.17 follows from Corollary 4.19.

A construction based on an explicit example

We also give an explicit construction using techniques from [BP19], which were used there to disprove a conjecture on a tri-linear version of Grothendieck's theorem. We do not exactly use the construction from that paper because it involves complex functions. Instead, we will use the Möbius function (defined below), which is real valued and has the desired properties.

The construction uses some notions from additive combinatorics. For a function $f : \mathbb{Z}_n \to [-1, 1]$ (on the cyclic group of order n), define the 3-linear form

$$p(x_1, x_2, x_3) = \sum_{a,b \in \mathbb{Z}_n} x_{1,a} x_{2,a+b} x_{3,a+2b} f(a + 3b).$$

where $x_1, x_2, x_3 \in \{-1, 1\}^n$ and the sums of a and b are done in $\mathbb{Z}_n$.

We begin by upper bounding $\Delta(p)$. The polynomial p 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 $f(a+3b)$ 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 $\|M_{1,a}\|_{\mathrm{op}} \leq 1$. Similarly, we get that $\|M_{i,a}\|_{\mathrm{op}} \leq 1$ for $i = 2, 3$. Hence,

$$\Delta(p) \leq 1. \tag{4.12}$$

for any choice of f.

Now we will choose a specific f for which we will be able to upper bound $\|p\|_\infty$ and lower bound $\|p\|_2^2$. Identify $\mathbb{Z}_n$ with $\{0, 1 \ldots, n-1\}$ in the standard way. We choose f to be the Möbius function restricted to this interval. That is, set $f(0) = 0$ and for $a > 0$, set

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

The infinity norm of p can be upper bounded in terms of the Gowers 3-uniformity

norm of f. This norm plays a central role in additive combinatorics and is defined by

$$\|f\|_{U^3} = \Big(\mathbb{E}_{a,b_1,b_2,b_3 \in \mathbb{Z}_n} \prod_{c \in \{0,1\}^3} f(a + c_1 b_1 + c_2 b_2 + c_3 b_3) \Big)^{\frac{1}{8}}.$$

The proof of the announced bound can be found in [Gre07, Proposition 1.11].

Lemma 4.21 (generalized von Neumann inequality)**.** *Suppose that n is coprime to 6. Then, for any $f : \mathbb{Z}_n \to [-1, 1]$, we have that*

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

A recent result by Tao and Teräväinen [TT23] given an upper bound to the Gowers 3-uniformity norm of the Möbius function.

Theorem 4.22. *Let $f : \mathbb{Z}_n \to \mathbb{R}$ be the Möbius function. Then,*

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

for some constant $C > 0$.

Combining Lemma 4.21 and Theorem 4.22 it follows that

$$\|p\|_\infty \leq \frac{n^2}{(\log \log n)^C} \tag{4.13}$$

for some constant $C > 0$.

To lower bound $\|p\|_2^2$ we begin using Parseval's identity, which implies that

$$\|p\|_2^2 = n \sum_{a \in \mathbb{Z}_n} f(a)^2. \tag{4.14}$$

Given that $|f(a)|^2$ is 1 if a is square-free and 0 otherwise, we can use a classical result of number theory to lower bound $\|p\|_2^2$ (see [HW+79, page 269] for a proof).

Proposition 4.23. *There are $\frac{6}{\pi^2} n - O(\sqrt{n})$ natural numbers between 1 and n that are square-free.*

From Eq. (4.14) and Proposition 4.23 follows that

$$\|p\|_2^2 = \frac{6}{\pi^2} n^2 - O(\sqrt{n^3}). \tag{4.15}$$

Finally, we substitute p by $p/(n^2/(\log\log n)^C)$, and it follows from Eqs. (4.12), (4.13) and (4.15) that p is bounded and

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

Again, Theorem 4.17 now follows from Corollary 4.19.

Remark 4.24. The *jointly completely bounded norm* of p is given by

$$\|p\|_{\text{jcb}} = \sup_{d\in\mathbb{N}} \| \sum_{a,b\in\mathbb{Z}_n} A(1,a)A(2,a+b)A(3,a+2b)f(a+3b)\|,$$

where the supremum is taken over maps $A : [3]\times[n] \to \mathbb{C}^{d\times d}$ such that $\|A(i,a)\|_{\text{op}} \leq 1$ and $[A(i,a), A(j,b)] = [A(i,a), A(j,b)^\dagger] = 0$ for all $i \neq j$ and $a, b \in \mathbb{Z}_n$. 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 [BBB+19] that Proposition 4.21 also holds for the jointly completely bounded norm, that is $\|p\|_{\text{jcb}} \leq n^2\|f\|_{U^3}$. The proof of Corollary 4.19 easily implies that $\|p\|_{\text{cb}} \geq \|p\|_2^2/\Delta(p)$. This was used in [BP19] to prove that the jcb and cb norms are inequivalent.

4.5 Grothendieck inequalities characterize converses to the polynomial method

In this section, we show, as a corollary of Theorem 4.13, that Grothendieck inequalities characterize converses to the polynomial method. By this we mean that: i) for 1-query algorithms an additive converse is possible and moreover this converse characterizes $K_G^{\mathbb{R}}$; and ii) for 2-query algorithms no additive converse is possible, because Grothendieck's inequality fails for 3-linear forms.

4.5.1 Characterizing $K_G^{\mathbb{R}}$ with 1-query quantum algorithms

Here we prove Theorem 4.5. Before doing that, we should prove Definition 2.17 and Definition 4.7 coincide for bilinear forms, so we can apply Grothendieck's Theorem, which uses Definition 2.17, into Theorem 4.13, which uses Definition 4.7.

Proposition 4.25. *For bilinear forms Definitons 2.17 and 4.7 coincide.*

Proof. Let $T : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ be a bilinear form. In this proof we will use $\|T\|_{\mathrm{cb}}$ to refer to the quantity defined in Definition 2.17, and we will write the quantity of Definition 4.7 as

$$\|T\|_{\tilde{\mathrm{cb}}} = \inf\Big\{\|R\|_{\mathrm{cb}} \mid T(x) = R(x,x)\ \forall\ x \in \mathbb{R}^n \times \mathbb{R}^n\Big\},$$

where the infimum runs over all bilinear forms $R : (\mathbb{R}^n \times \mathbb{R}^n) \times (\mathbb{R}^n \times \mathbb{R}^n) \to \mathbb{R}$.

We first prove that $\|T\|_{\tilde{\mathrm{cb}}} = \|T_{\mathrm{sym}}\|_{\mathrm{cb}}$, where $T_{\mathrm{sym}} : (\mathbb{R}^n \times \mathbb{R}^n) \times (\mathbb{R}^n \times \mathbb{R}^n) \to \mathbb{R}$ is the only symmetric bilinear form such that $T(x) = T_{\mathrm{sym}}(x,x)$ for every $x \in \mathbb{R}^n \times \mathbb{R}^n$. On the one hand, by definition, it follows that $\|T\|_{\tilde{\mathrm{cb}}} \leq \|T_{\mathrm{sym}}\|_{\mathrm{cb}}$. On the other hand, consider a bilinear form $R : (\mathbb{R}^n \times \mathbb{R}^n) \times (\mathbb{R}^n \times \mathbb{R}^n) \to \mathbb{R}$ such that $T(x) = R(x,x)$ for every $x \in \mathbb{R}^n \times \mathbb{R}^n$. We define $R^{\mathsf{T}} : (\mathbb{R}^n \times \mathbb{R}^n) \times (\mathbb{R}^n \times \mathbb{R}^n) \to \mathbb{R}$ as the bilinear form obtained by transposing the matrix associated to R as in Definition 2.14. We have that $T_{\mathrm{sym}} = (R + R^{\mathsf{T}})/2$ and that $T(x) = R^{\mathsf{T}}(x,x)$ for every $x \in \mathbb{R}^n \times \mathbb{R}^n$. Furthermore, it is satisfied that

$$\begin{aligned}
\|R^{\mathsf{T}}\|_{\mathrm{cb}} &= \sup\Big\{\|\sum_{i,j} R_{j,i} A(i) B(j)\| \mid A(i), B(j) \in B_{M_d}\Big\} \\
&= \sup\Big\{\|\sum_{i,j} R_{j,i} B(j)^{\mathsf{T}} A(i)^{\mathsf{T}}\| \mid A(i), B(j) \in B_{M_d}\Big\} \\
&= \|R\|_{\mathrm{cb}},
\end{aligned} \tag{4.16}$$

where we use (twice) that for any matrix M we have $\|M\| = \|M^{\mathsf{T}}\|$. Thus, we have that $\|R\|_{\mathrm{cb}} \geq \|T_{\mathrm{sym}}\|_{\mathrm{cb}}$, so $\|T\|_{\tilde{\mathrm{cb}}} \geq \|T_{\mathrm{sym}}\|_{\mathrm{cb}}$.

Second, we prove that $\|T\|_{\mathrm{cb}} = \|T_{\mathrm{sym}}\|_{\mathrm{cb}}$. We observe that $T_{\mathrm{sym}} = \frac{1}{2}\begin{pmatrix} 0 & T \\ T^{\mathsf{T}} & 0 \end{pmatrix}$. Thus, we immediately have that $\|T\|_{\mathrm{cb}} \leq \|T_{\mathrm{sym}}\|_{\mathrm{cb}}$. Also, it is satisfied that

$$\begin{aligned}
\|T_{\mathrm{sym}}\|_{\mathrm{cb}} &\leq \frac{1}{2}\left(\left\|\begin{pmatrix} 0 & T \\ 0 & 0 \end{pmatrix}\right\|_{\mathrm{cb}} + \left\|\begin{pmatrix} 0 & 0 \\ T^{\mathsf{T}} & 0 \end{pmatrix}\right\|_{\mathrm{cb}}\right) \\
&\leq \frac{1}{2}\left(\|T\|_{\mathrm{cb}} + \|T^{\mathsf{T}}\|_{\mathrm{cb}}\right) \\
&= \|T\|_{\mathrm{cb}},
\end{aligned}$$

where the last equality uses (4.16). □

We recall that it was shown in [AAI+16] that for every bilinear form there exists a 1-query quantum algorithm that makes additive error at most $1 - 1/K_G^{\mathbb{R}}$. It thus

remains to show the lower bound.

Theorem 4.5. *The worst-case minimum error for one-query quantum algorithms satisfies*

$$\sup_p \mathcal{E}(p,1) = 1 - \frac{1}{K_G^{\mathbb{R}}},$$

where the supremum is taken over the set of bounded bilinear forms.

Proof. Theorem 4.13 shows the following:

$$\begin{aligned} \sup_{p\in\mathcal{BB}} \mathcal{E}(p,1) &= \sup_{\|p\|_\infty\le 1} \sup_{\|r\|_{\infty,*}\le 1} \langle p, r\rangle - \|r\|_{\mathrm{cb},*} && (4.17)\\ &= \sup_{\|r\|_{\infty,*}\le 1} \|r\|_{\infty,*} - \|r\|_{\mathrm{cb},*} && (4.18)\\ &= \sup_{\|r\|_{\infty,*}=1} 1 - \|r\|_{\mathrm{cb},*}. \end{aligned}$$

It thus remains to show that for bilinear forms $\|r\|_{\infty,*} \le K_G^{\mathbb{R}}\|r\|_{\mathrm{cb},*}$. We do so starting from Grothendieck's theorem for matrices. It states that for $A \in \mathbb{R}^{n\times n}$ we have $\|A\|_{\mathrm{cb}} \le K_G^{\mathbb{R}}\|A\|_\infty$. Each bilinear form $q : \{-1,1\}^n \times \{-1,1\}^n \to \mathbb{R}$ uniquely corresponds to a matrix $A \in \mathbb{R}^{n\times n}$ such that $q(x,y) = x^{\mathsf{T}}Ay$. Moreover, for such q and A one has $\|q\|_\infty = \|A\|_\infty$ (immediate) and in Proposition 4.25 we showed $\|q\|_{\mathrm{cb}} = \|A\|_{\mathrm{cb}}$, so $\|q\|_{\mathrm{cb}} \le K_G^{\mathbb{R}}\|q\|_\infty$. A duality argument then concludes the proof:

$$\|r\|_{\infty,*} = \sup_{\|q\|_\infty\le 1} \langle r, q\rangle \le \sup_{\|q\|_{\mathrm{cb}}\le K_G^{\mathbb{R}}} \langle r, q\rangle = K_G^{\mathbb{R}}\|r\|_{\mathrm{cb},*}.$$

□

Remark 4.26. If in Theorem 4.5 we restrict the supremum to bilinear forms on $n+n$ variables, for a fixed n, then we obtain a characterization of $K_G^{\mathbb{R}}(n)$ instead of $K_G^{\mathbb{R}}$. Here, $K_G^{\mathbb{R}}(n) = \sup \|A\|_{\mathrm{cb}}/\|A\|_\infty$, where the supremum is taken over all non-zero $n\times n$ real matrices.

4.5.2 No converse for the polynomial method

In this section we show that there is no additive nor multiplicative converse for polynomials of degree 4 and 2-query algorithms. In other words, we will prove Theorems 4.3 and 4.4. Before doing that, we explain what was the error in the proof of Theorem 4.3 given in [ABP19].

Their proof arrives at the equation

$$\sum_{\alpha,\beta\in\{0,1,2,3,4\}^n:|\alpha|+|\beta|=4} d'_{\alpha,\beta}x^\alpha = C \sum_{\alpha\in\{0,1\}^n:|\alpha|=4} d_\alpha x^\alpha \quad \forall\, x\in\{-1,1\}^n, \tag{4.19}$$

where $d'_{\alpha,\beta}$, d_α and C are some real numbers, x^α stands for $\prod_{i=1}^n x_i^{\alpha_i}$ and $|\alpha|$ for $\sum_{i=1}^n \alpha_i$. It follows from the orthogonality of the characters 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 $n=1$, $C=1$ and $d'_{(2,0),(0,2)} = -d'_{(0,0),(4,0)} = 1$ and the rest of the coefficients set to 0, then (4.19) becomes $x^2-1=0,\ \forall\, x\in\{-1,1\}$.

We now prove that there is no additive converse, from which the non-multiplicative converse result quickly follows.

Theorem 4.4. *There is no constant $\varepsilon\in(0,1)$ such that for every bounded polynomial p of degree at most 4, we have $\mathcal{E}(p,2)\le\varepsilon$.*

Proof. For any partition $\mathcal{P}$ of $\{0\}\cup[3n]$ in $2t$ subsets, Theorem 4.13 shows that

$$\begin{aligned}\sup_{p\in V_\mathcal{P},\|p\|_\infty\le 1}\mathcal{E}(p,t) &= \sup_{p\in V_\mathcal{P},\|p\|_\infty\le 1}\sup_{r\in V_\mathcal{P},\|r\|_{\infty,*}\le 1}\langle p,r\rangle - \|r\|_{\mathrm{cb},*}\\ &= \sup_{r\in V_\mathcal{P},\|r\|_{\infty,*}\le 1}\|r\|_{\infty,*}-\|r\|_{\mathrm{cb},*}\\ &= \sup_{r\in V_\mathcal{P},\|r\|_{\infty,*}=1} 1-\|r\|_{\mathrm{cb},*}.\end{aligned}$$

Consider now the case $t=2$ and the partition $\mathcal{P}_n = \{\{0\},\{1,\dots,n\},\{n+1,\dots,2n\},\{2n+1,\dots,3n\}\}$ of $\{0\}\cup[3n]$. In Theorem 4.17 a sequence of forms $p_n\in V_{\mathcal{P}_n}$ was constructed with the property that

$$\frac{\|p_n\|_{\mathrm{cb}}}{\|p_n\|_\infty}\to\infty. \tag{4.20}$$

Hence, by a duality argument we get that there is a sequence $r_n\in V_{\mathcal{P}_n}$ such that $\|r_n\|_{\mathrm{cb},*}/\|r_n\|_{\infty,*}\to 0$. Indeed, suppose towards a contradiction that there is a $K>0$ such that for every $n\in\mathbb{N}$ and every $r\in V_{\mathcal{P}_n}$ we have that $\|r\|_{\mathrm{cb},*}\ge K\|r\|_{\infty,*}$. Then,

$$\|p\|_{\mathrm{cb}} = \sup_{\|r\|_{\mathrm{cb},*}\le 1}\langle r,p\rangle \le \frac{1}{K}\sup_{\|r\|_{\infty,*}\le 1}\langle r,p\rangle = \frac{1}{K}\|p\|_\infty,$$

which contradicts Eq. (4.20). The sequence r_n shows that

$$\sup_{p\in V_{\mathcal{P}_n}, \|p\|_\infty \leq 1, n\in\mathbb{N}} \mathcal{E}(p,2) = 1,$$

which implies the stated result. □

Theorem 4.3. *For any $C > 0$, there exist an $n \in \mathbb{N}$ and a bounded quartic n-variable polynomial p such that no two-query quantum algorithm $\mathcal{A}$ satisfies $\mathbb{E}[\mathcal{A}(x)] = Cp(x)$ for every $x \in \{-1,1\}^n$.*

Proof. First note that we can assume $C \leq 1$, because $|\mathbb{E}[\mathcal{A}(x)]| \leq 1$ for any algorithm $\mathcal{A}$ and any $x \in \{-1,1\}^n$. Assume that there exists $0 < C \leq 1$ such that for every bounded p of degree 4 there is a 2-query algorithm $\mathcal{A}$ with $\mathbb{E}[\mathcal{A}(x)] = p(x)$ for every $x \in \{-1,1\}^n$. We claim that that $\mathcal{A}$ approximates p up to an additive error $1 - 1/C$, which contradicts Theorem 4.4. Indeed,

$$|p(x) - \mathbb{E}[\mathcal{A}(x)]| = |p(x)(1-C)| \leq 1 - C.$$

□