GROTHENDIECK INEQUALITIES CHARACTERIZE CONVERSES TO THE POLYNOMIAL METHOD

JOP BRIËT, FRANCISCO ESCUDERO GUTIÉRREZ, AND SANDER GRIBLING

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. Here we show that such a result does not generalize to quartic polynomials and 2-query algorithms, even when we allow for additive approximations. We also show that the additive approximation implied by their result is tight for bounded bilinear forms, which gives a new characterization of the Grothendieck constant in terms of 1-query quantum algorithms. Along the way we provide reformulations of the completely bounded norm of a form, and its dual norm.

1. Introduction

Quantum query complexity is one of the few models of computation in which the strengths and weaknesses of quantum computers can be rigorously studied with currently-available techniques (see e.g., [Amb18, Aar21] for recent surveys). On the one hand, many of quantum computing's best-known algorithms, such as for unstructured search [Gro96], period finding (the core of Shor's algorithm for integer factoring) [Sho97] and element distinctness [Amb07], are most naturally described in the query model. On the other hand, it admits powerful lower-bound techniques.

For a (possibly partial) 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] gives a lower bound on the quantum query complexity of f, denoted $Q(f)$, in terms of the minimal degree of an approximating polynomial for f, or approximate degree, $\widetilde{\deg}(f)$. The method relies on the basic fact that for any t-query quantum algorithm $\mathcal{A}$ that takes an n-bit input and returns a sign, there is a real n-variable polynomial p of degree at most $2t$

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.

such that $p(x) = \mathbb{E}[\mathcal{A}(x)]$ for every x. Here, the expectation is taken with respect to the randomness in the measurement done by $\mathcal{A}$.[1] 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 [ABDK+21].[2] These separations rule out a direct converse to the polynomial method, whereby a given bounded degree-$2t$ polynomial p is implemented with 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 of an "approximate converse," where $\mathcal{A}$ approximates p with some error that depends on t.

Here, p is *bounded* if it maps the Boolean hypercube to the interval $[-1, 1]$ and $\mathcal{A}$ *approximates* p if for some constant *additive* error parameter $\varepsilon < 1$, we have that $|p(x) - \mathbb{E}[\mathcal{A}(x)]| \leq \varepsilon$ for every x. Note that an additive error of 1 can trivially be achieved with a uniformly random coin flip. For a function $f : \{-1, 1\}^n \to \mathbb{R}$ and and positive integer t, we denote the smallest additive error that a t-query quantum algorithm can achieve by

$$\mathcal{E}(f, t) := \inf \big\{ \varepsilon \geq 0 \mid \exists\ t\text{-query quantum algorithm } \mathcal{A} \text{ with } |f(x) - \mathbb{E}[\mathcal{A}(x)]| \leq \varepsilon \quad \forall x \in \{-1, 1\}^n \big\}. \tag{1}$$

For bounded polynomials of degree at most 2, the following "multiplicative converse" to the polynomial method was proved by Aaronson, Ambainis, Iraids, Kokainis and Smotrovs [AAI+16].

Theorem 1.1 (Quadratic multiplicative converse)**.** *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.*

Up to an absolute constant scaling, quadratic polynomials can thus be computed exactly by 1-query quantum algorithms. This result directly implies the following additive version.

Corollary 1.2 (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 1.1.*

[1] We identify quantum query algorithms with the (random) functions giving their outputs.

[2] It is open whether partial functions admit exponential separations [Aar21, Problem 5].

In light of the polynomial method, Corollary 1.2 thus shows that in an approximate sense, one-query quantum algorithms are equivalent to bounded quadratic polynomials.

1.1. **Generalizations to higher degrees.** The authors of [AAI+16] asked whether their results generalize to higher degrees. Two ways to interpret this question are that for any k, any degree-$2k$ polynomial p satisfies:

(1) $\mathcal{E}(Cp, k) = 0$ for some $C = C(k) > 0$, or;
(2) $\mathcal{E}(p, k) \leq \varepsilon$ 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 (1), the higher-degree version of Theorem 1.1, was ruled out by Arunachalam, Palazuelos and the first author [ABP19] and the first two authors [BEG22]. In particular, in terms of the notation above, the hoped-for constant scaling $C(4) > 0$ does not exist. In the additive-error setting it was also proved in [BEG22] that for some absolute constant $\varepsilon_0 > 0$, we necessarily have that $\varepsilon(4) > \varepsilon_0$, thus placing a lower bound on the error required in any quartic generalization of Corollary 1.2.

These negative results do not exclude the possibility of option (2), namely that Corollary 1.2 generalizes to higher degrees, in particular that it holds for some $\varepsilon(4) \in (\varepsilon_0, 1)$. Our first result shows that it does not.

Theorem 1.3. *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 $\widetilde{\deg}(f)$: 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 then boost the success probability of $\mathcal{A}$ so that it approximates f. Corollary 1.2 gives the only exceptional case where this is possible in general.

1.2. **Best constants.** Theorem 1.1 was proved using a surprising application of the famous Grothendieck inequality from Banach space theory [Gro53]. For bounded bilinear forms, $p(x, y) = x^{\mathsf{T}} A y$ given by a matrix $A \in \mathbb{R}^{n \times n}$, the result holds with $1/C$ equal to the Grothendieck constant K_G (see [ABP19, Section 5] for a short proof). Determining the precise value of K_G is a notorious open problem posed originally in [Gro53]; the best-known lower and upper bounds place it in the interval $(1.676, 1.782)$ [Dav84, Ree91, BMMN13]. The general form of Theorem 1.1 then follows from decoupling techniques. It is not difficult to show that $1/K_G$ is the optimal constant in the bilinear case for the

multiplicative setting of Theorem 1.1. Here we show that the additive $1-1/K_G$ approximation implied by the multiplicative setting is also optimal.

Theorem 1.4. *Let $\mathcal{BB}$ the set of bounded bilinear forms. Then,*

$$\sup_{p\in\mathcal{BB}} \mathcal{E}(p,1) = 1 - \frac{1}{K_G}.$$

Theorem 1.4 may open a new route to determine the value of K_G by studying the power and limitations of 1-query quantum algorithms. This complements another well-known characterization of K_G in terms of the largest-possible Bell-inequality violations in two-player XOR games [Tsi80].

1.3. **Techniques.** The starting point for this work is a characterization of quantum query algorithms with completely bounded polynomials [ABP19]. Recently, this characterization was also used to make progress on the problem to determine "the need for structure in quantum speed-ups" by Bansal, Sinha and de Wolf [BSdW22] and in the above-mentioned work [BEG22]. In addition, it led to a new exact SDP-based formulation for quantum query complexity, due to Laurent and the third author [GL19].

Using this, we show that for any "block-multilinear" polynomial p of degree $2t$, the parameter $\mathcal{E}(p,t)$ can be written in terms of a ratio of norms related to norms appearing naturally in the Grothendieck inequality. Block-multilinear forms appear naturally in the polynomial method and play an important role for instance in [AAI+16, BSdW22]. Here we will give an informal explanation of our main technical contribution and refer to the sequel for further details.

For a partition $\mathcal{P}$ of $[n]$ into $2t$ parts, we let $V_{\mathcal{P}}$ denote the space of real n-variable degree-$2t$ polynomials that are block-multilinear with respect to $\mathcal{P}$. In Theorem 4.1 below we show that for any $p \in V_{\mathcal{P}}$, we can express $\mathcal{E}(p,t)$ as a supremum of the form

$$\sup_{r\in V_{\mathcal{P}}} \frac{\langle p, r\rangle - \|r\|_{\mathrm{cb},*}}{\|r\|_{\infty,*}}, \tag{2}$$

where the inner product is as usual for functions on the Boolean hypercube.

The connection with the Grothendieck theorem emerges in the bilinear case, where $t=1$, $n=2k$ and, say, $\mathcal{P} = \{1,\dots,k\}\cup\{k+1,\dots,2k\}$. In this case, $V_{\mathcal{P}}$ consists of polynomials of the form $p(x,y) = x^{\mathsf{T}}Ay$ for some matrix $A\in\mathbb{R}^{k\times k}$. Then, $\|p\|_{\infty,*}$ and $\|p\|_{\mathrm{cb},*}$ are the *dual norms* associated to respectively the

$\infty \to 1$-norm and completely bounded norm of A:

$$\|A\|_{\infty\to 1} = \max_{x,y\in\{-1,1\}^k} x^{\mathsf{T}} A y,$$

$$\|A\|_{\mathrm{cb}} = \sup_{d\in\mathbb{N},u,v:[k]\to S^{d-1}} \sum_{i,j=1}^{k} A_{i,j}\langle u(i), v(j)\rangle,$$

where S^{d-1} denotes the real $(d-1)$-dimensional Euclidean unit sphere. The expression (2) then simplifies to

$$\sup_{B\in\mathbb{R}^{k\times k}} \frac{\langle A, B\rangle - \|B\|_{\mathrm{cb},*}}{\|B\|_{\infty\to 1,*}}, \tag{3}$$

where the inner product is now the usual trace inner product on matrices. Grothendieck's theorem asserts that the above norms are in fact closely related.

Theorem 1.5 (Grothendieck's theorem)**.** *There exists a constant $K < \infty$ such that for any $k \in \mathbb{N}$ and $A \in \mathbb{R}^{k\times k}$, we have*

$$\|A\|_{\infty\to 1} \le \|A\|_{\mathrm{cb}} \le K\|A\|_{\infty\to 1}. \tag{4}$$

The non-trivial part of this result is the second inequality in (4) and the smallest K for which it holds is the above-mentioned Grothendieck constant K_G. The dual formulation of this fact asserts that $\|A\|_{\infty\to 1,*} \le K_G\|A\|_{\mathrm{cb},*}$ holds for any matrix A. Theorem 1.4 then follows from the expression (3) for $\mathcal{E}(p, 1)$ by minimizing $\|B\|_{\mathrm{cb},*}/\|B\|_{\infty\to 1,*}$ while maximizing $\langle A, B\rangle$ over all nonzero B.

Theorem 1.3 follows similarly from the expression (2) for the case $t = 2$. For this, we use a construction from [BEG22] which gives a sequence $(p_n)_{n\in\mathbb{N}}$ of block-multilinear polynomials of degree 4 satisfying

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

as $n \to \infty$. By duality, this implies the existence of a sequence of block-multilinear polynomials r_n of degree 4 such that $\|r_n\|_{\mathrm{cb},*}/\|r_n\|_{\infty,*} \to 0$. This sequence $(r_n)_{n\in\mathbb{N}}$ can be explicitly described, as we do in Appendix A.

We give two proofs of Theorem 4.1, one based directly on the formulation of $\mathcal{E}(f, t)$ that follows from [ABP19], and a second proof that uses a semidefinite programming formulation of the completely bounded norm from [GL19].

2. Preliminaries

First, we establish some notation. Given $n \in \mathbb{N}$, write $[n] := \{1, \dots, n\}$. Given $d \in \mathbb{N}$, we use the standard inner product of vectors $x, y \in \mathbb{R}^d$ defined as $\langle x, y\rangle = \sum_{i\in[d]} x_i y_i$, and the associated norm $\|x\| = \sqrt{\langle x, x\rangle}$. We denote the set of unit vectors of $\mathbb{R}^d$ by S^{d-1}. For matrices $A \in \mathbb{R}^{d\times d}$ we use the operator

norm that corresponds to viewing A as a linear map from $\mathbb{R}^d$ to $\mathbb{R}^d$. We write $M(d) = \mathbb{R}^{d\times d}$ and let $B_{M(d)}$ denote the unit ball in $M(d)$ with respect to the operator norm (i.e., the set of contractions).

We write $\mathbf{i}$ for a t-tuple $\mathbf{i} = (i_t, \ldots, i_t) \in [n]^t$ of indices. Given variables $x_1, \ldots, x_n$ and a t-tuple $\mathbf{i} \in [n]^t$, we use $x(\mathbf{i})$ to denote the monomial $x_{i_1} x_{i_2} \cdots x_{i_t}$. Similarly, given a matrix-valued map $A\colon [n] \to \mathbb{R}^{d\times d}$, we write $A(\mathbf{i}) := A(i_1)A(i_2)\ldots A(i_t)$. We let $\mathcal{S}_n$ be the symmetric group on n elements.

2.1. **Norms of polynomials.** 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

$$p(x) = \sum_{\alpha\in\mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha, \tag{5}$$

where $x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ and $c_\alpha \in \mathbb{R}$. The support of p is given 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 gives the degree of the monomial x^α. A form of degree d is a homogeneous polynomial of degree d. Denote by $\mathbb{R}[x_1, \ldots, x_n]_{=d}$ the space spanned by forms of degree d. For p as in Eq. (5), define its homogeneous degree-d part by

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

When when we only evaluate polynomials on the hypercube it is natural to consider the space of multilinear polynomials, which are those polynomials with support in $\{0,1\}^n$. We write $r : \{-1,1\}^n \to \mathbb{R}$ for a multilinear polynomial r. The inner product in $\mathbb{R}[x_1, \ldots, x_n]$ is 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.

Toward defining the completely bounded norm, we restrict our attention to forms only. For every $p \in \mathbb{R}[x_1, \ldots, x_n]_{=t}$ there are many t-tensors $T \in \mathbb{R}^{n\times\cdots\times n}$ such that $T(x) = p(x)$ for every $x \in \mathbb{R}^n$, where

$$T(x) := \sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} x(\mathbf{i}).$$

These tensors only have to satisfy

$$\sum_{\mathbf{i}\in\mathcal{I}_\alpha} T_{\mathbf{i}} = c_\alpha \quad \forall \alpha \in \mathbb{Z}^n_{\geq 0}, \tag{6}$$

where $\mathcal{I}_\alpha$ is the set of elements $\mathbf{i}$ of $[n]^t$ such that the element $m \in [n]$ occurs α_m times in $\mathbf{i}$. Each of these tensors gives a way of evaluating p in matrices, namely for every matrix-valued map $A : [n] \to \mathbb{R}^{d\times d}$,

$$T(A) := \sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} A(\mathbf{i}) = \sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} A(i_1)\dots A(i_t).$$

We will use the following inner product for tensors:

$$\langle T, R\rangle = \sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} R_{\mathbf{i}}.$$

It is also important to consider the unique symmetric t-tensor $T_p \in \mathbb{R}^{n\times\cdots\times n}$ such that

$$p(x) = T_p(x).$$

For a tensor $T = (T_{\mathbf{i}})_{\mathbf{i}\in[n]^t}$ and permutation $\sigma \in \mathcal{S}_t$ we define $T\circ\sigma := (T_{\sigma(\mathbf{i})})_{\mathbf{i}\in[n]^t}$, and we say that T symmetric if $T = T\circ\sigma$ for all $\sigma \in \mathcal{S}_t$. The entries of this T_p are given by

$$(T_p)_{\mathbf{i}} = \frac{c_{e_{i_1}+\cdots+e_{i_t}}}{\tau(i_1,\dots,i_t)} \text{ for } \mathbf{i} \in [n]^t, \tag{7}$$

where $\tau(i_1,\dots,i_t)$ is the number of distinct permutations of the sequence $(i_1,\dots,i_t)$. The completely bounded norm of a tensor T is given by[3]

$$\|T\|_{\mathrm{cb}} = \sup\{\|\sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} A_1(i_1)\dots A_t(i_t)\| \;\mid\; A_s\colon [n] \to B_{M(d)},\ s\in[t],\ d\in\mathbb{N}\},$$

and the norm of a form p is

$$\|p\|_{\mathrm{cb}} = \inf\{\sum_{\sigma\in\mathcal{S}_t} \|T_\sigma\|_{\mathrm{cb}} \;\mid\; \sum_{\sigma\in\mathcal{S}_t} T_\sigma\circ\sigma = T_p\}. \tag{8}$$

In Section 3 we provide easier expressions for both $\|T\|_{\mathrm{cb}}$ (showing that a single matrix-valued map $A\colon [n] \to \mathbb{R}^{d\times d}$ suffices) and $\|p\|_{\mathrm{cb}}$.

[3]This is the completely bounded norm of T when regarded as an element of $\ell^1_n \otimes_h \cdots \otimes_h \ell^1_n$, where h stands for the Haagerup tensor product, which determines a well-studied tensor norm. See for instance [Pau03, Chapter 17].

2.2. **Block-multilinear forms.** Our main result Theorem 4.1 is stated for a special kind of polynomials, which are the block-multilinear forms.

Definition 2.1. 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

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

We also work with the larger space of polynomials spanned by monomials where in the above we replace degree-1 with respect to a set by odd degree, formally defined as follows.

Definition 2.2. 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 $\alpha \in \mathbb{Z}^m_{\geq 0}$ satisfying

$$\sum_{i \in I} \alpha_i \equiv 1 \bmod 2 \ \forall I \in \mathcal{Q}. \tag{9}$$

Remark 2.3. 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 $W_{\mathcal{P}}$.

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. On the other hand, when we say $\|R\|_{\mathrm{cb},*}$ 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 2.4. 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 (see [O'D14, Chapter 1] for an introduction to Fourier analysis in the Boolean hypercube).

It will be convenient to work with $W_{\mathcal{Q}}$ because the projector onto this subspace has a nice structure. To state this formally we introduce some notation. Let $\Pi_{\mathcal{Q}} : \mathbb{R}[x_1, \ldots, x_n] \to W_{\mathcal{Q}}$ be the projector onto $W_{\mathcal{Q}}$. Given a t-tensor $T \in \mathbb{R}^{n \times \cdots \times n}$, we define $\Pi_{\mathcal{Q}} T$ as

$$(\Pi_{\mathcal{Q}} T)_{\mathbf{i}} := \begin{cases} T_{\mathbf{i}} & \text{if } \mathbf{i} \in \mathcal{I}_{\mathcal{Q}}, \\ 0 & \text{else,} \end{cases} \tag{10}$$

where $\mathcal{I}_{\mathcal{Q}}$ is the subset of indices $\mathbf{i}$ such that for every set of $\mathcal{Q}$, the number of indices in $\mathbf{i}$ that belong to that set is odd. Here we abuse notation since T is a tensor and not a polynomial, however, this is consistent in the following way: if $T(x) = p(x)$ for every $x \in \{-1, 1\}^n$, then $\Pi_{\mathcal{Q}} T(x) = \Pi_{\mathcal{Q}} p(x)$ for every $x \in \{-1, 1\}^n$, where on the left-hand side we use Eq. (10) and on the right-hand side $\Pi_{\mathcal{Q}}$ is the projection onto $W_{\mathcal{Q}}$. For every $I \in \mathcal{Q}$ let z_I be a random variable that takes the values -1 and 1 with probability $1/2$, let $z = (\sigma_I)_{I \in \mathcal{Q}}$ and for every $A \colon [n] \to \mathbb{R}^{d \times d}$ we define the random variable $A \cdot z$ by

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

Proposition 2.5. *Let $\mathcal{Q}$ be a family of disjoint subsets of $[n]$. If $p \in \mathbb{R}[x_1, \ldots, x_n]$, then*

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

for every $x \in \mathbb{R}^n$. Moreover, if $T \in \mathbb{R}^{n \times \cdots \times n}$ is a t-tensor, then

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

for every $A \colon [n] \to \mathbb{R}^{d \times d}$ and every $d \in \mathbb{N}$.

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

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

and hence

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

which equals the projection of x^α on $W_{\mathcal{Q}}$. The statement for tensors follows analogously. □

2.3. **Completely bounded forms and quantum query algorithms.** In [ABP19] the outputs of quantum query algorithms were fully characterized in terms of completely bounded forms.

Theorem 2.6 (Quantum query algorithms are completely bounded forms)**.** *Let $f : \{-1,1\}^n \to [-1,1]$ and let $t \in \mathbb{N}$. Then,*

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

3. Reformulation of the completely bounded norm of a form

In this section we prove a few general results regarding the completely bounded norms of tensors and polynomials. We provide simplifications of these norms that are not only helpful to develop our results, but also might facilitate the use of completely bounded polynomials to prove results in quantum query complexity. After this section, we will implicitly use the formulas of Propositions 3.1 and 3.2 as definitions for $\|p\|_{\mathrm{cb}}$ and $\|T\|_{\mathrm{cb}}$, respectively.

First, we provide a simpler expression (compared to Eq. (8)) for $\|p\|_{\mathrm{cb}}$.

Proposition 3.1. *Let $p \in \mathbb{R}[x_1,\dots,x_n]_{=t}$ be a form of degree t. Then,*

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

Proof: We first observe that for any t-tensor T and permutation $\sigma \in \mathcal{S}_t$ we have

$$(T \circ \sigma)(x) = \sum_{\mathbf{i} \in [n]^t} T_{\mathbf{i}\circ\sigma} x(\mathbf{i}) = \sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}\circ\sigma} x(\mathbf{i}\circ\sigma) = T(x).$$

We then show the first inequality: $\|p\|_{\mathrm{cb}} \le \inf\big\{\|T\|_{\mathrm{cb}} \mid p(x) = T(x)\ \forall x \in \mathbb{R}^n\big\}$. By restricting in (8) to decompositions where $T^\sigma = T/t!$ for all σ, we have

$$\begin{aligned} \|p\|_{\mathrm{cb}} &= \inf\Big\{ \sum_{\sigma\in\mathcal{S}_t} \|T^\sigma\|_{\mathrm{cb}} \mid T_p = \sum_\sigma T^\sigma \circ \sigma \Big\} \\ &\le \inf\Big\{ \|T\|_{\mathrm{cb}} \mid T_p = \frac{1}{t!}\sum_\sigma T\circ\sigma \Big\} \\ &= \inf\Big\{ \|T\|_{\mathrm{cb}} \mid p(x) = T(x) \Big\}. \end{aligned}$$

Here to see the last equality we require two observations: first, we have $p(x) = T_p(x) = \frac{1}{t!}\sum_\sigma T\circ\sigma(x) = \frac{1}{t!}\sum T(x) = T(x)$, and second, if $p(x) = T(x)$, then $T_p = \frac{1}{t!}\sum_\sigma T\circ\sigma$ since T_p is the *unique* symmetric t-tensor with $T_p(x) = p(x)$.

Now for the reverse inequality, let T^σ ($\sigma \in \mathcal{S}_t$) be such that $T_p = \sum_\sigma T^\sigma \circ \sigma$ and define $T = \sum_\sigma T^\sigma$. Then we have

$$p(x) = T_p(x) = \sum_\sigma T^\sigma \circ \sigma(x) = \sum_\sigma T^\sigma(x) = T(x),$$

and $\|T\|_{\mathrm{cb}} \leq \sum_\sigma \|T^\sigma\|_{\mathrm{cb}}$ by the triangle inequality. This shows that also $\|p\|_{\mathrm{cb}} \geq \inf\Big\{\|T\|_{\mathrm{cb}} \mid p(x) = T(x)\Big\}$. □

Second, we show that the contraction-valued maps A_s in the definition of $\|T\|_{\mathrm{cb}}$ can be taken to be the same. This result can be understood as the fact that the polarization constant of completely bounded multilinear maps is 1.[4]

Proposition 3.2. *Let $T \in \mathbb{R}^{n\times\cdots\times n}$ be a t-tensor. Then,*

$$\|T\|_{\mathrm{cb}} = \sup\Big\{\|\sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} A(\mathbf{i})\| \mid A\colon [n] \to B_{M(d)},\ d \in \mathbb{N}\Big\}.$$

Proof: Let $|||T|||$ be the expression in the right-hand side of the statement. Note that it is the same as the expression of $\|T\|_{\mathrm{cb}}$, but now the contraction-valued maps $A_1, \ldots, A_t$ are all equal. This shows that $|||T||| \leq \|T\|_{\mathrm{cb}}$. To prove the other inequality, let $A_1, \ldots, A_t\colon [n] \to B_{M(d)}$ and $u, v \in S^{d-1}$. Now, define the contraction-valued map A by $A(i) := \sum_{s\in[t]} e_s e_{s+1}^{\mathsf{T}} \otimes A_s(i)$ for $i \in [n]$, and define the unit vectors $u' := e_1 \otimes u$ and $v' := e_{t+1} \otimes v$. They satisfy

$$\langle u, A_1(i_1) \ldots A_t(i_t) v\rangle = \langle u', A(\mathbf{i}) v'\rangle \quad \text{for all } \mathbf{i} \in [n]^t,$$

so in particular

$$\sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} \langle u, A_1(i_1) \ldots A_t(i_t) v\rangle = \sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} \langle u', A(\mathbf{i}) v'\rangle.$$

Taking the supremum over all A_s and u, v shows that $\|T\|_{\mathrm{cb}} \leq |||T|||$, which concludes the proof. □

Third, we give a convenient formula for the dual of the completely bounded norm of a tensor. To state it in an elegant way, we introduce the following subset of t-tensors in $\mathbb{R}^{n\times\cdots\times n}$:

$$K(n,t) := \{\langle u, A(\mathbf{i}) v\rangle_{\mathbf{i}\in[n]^t} \mid d \in \mathbb{N},\ u, v \in S^{d-1},\ A\colon [n] \to B_{M(d)}\}. \tag{11}$$

Proposition 3.3. *Let $R \in \mathbb{R}^{n\times\cdots\times n}$ be a t-tensor. Then,*

$$\|R\|_{\mathrm{cb},*} = \inf\{w > 0 \mid R \in wK(n,t)\}. \tag{12}$$

[4] In Banach space theory a multilinear map $T : X \times \cdots \times X \to Y$ determines a polynomial $P : X \to Y : A \to T(A, \ldots, A)$. The operator norms of T and P are equivalent if T is symmetric: $\|T\| \leq \|P\| \leq K\|T\|$, where K is the polarization constant of T. For a survey on the topic see, e.g., [MMFPSS22, Section 5.1].

Remark 3.4. Note that Proposition 3.3 states that $\|R\|_{\mathrm{cb},*}$ is the Minkowski norm defined by $K(n,t)$, so $K(n,t)$ is the unit ball of $(\mathbb{R}^{n\times\cdots\times n}, \|\cdot\|_{\mathrm{cb},*})$.

Proof: Let $|||R|||$ be the expression in the right-hand side of Eq. (12). First, we show that $|||\cdot|||$ is a norm. We should check that $|||R|||$ is well-defined, i.e., that every tensor can be decomposed as $\langle u, A(\mathbf{i})v\rangle$. We observe that the standard basis elements for the space of t-tensors are contained in $K(n,t)$. Indeed, let $u := e_1$, $v := e_{t+1}$ and $A(i) = \sum_{s\in\mathbf{i}^{-1}(i)} e_s e_{s+1}^{\mathsf{T}}$ then

$$\langle u, A(\mathbf{j})v\rangle = \begin{cases} 1 & \text{if } \mathbf{j} = \mathbf{i}, \\ 0 & \text{otherwise.} \end{cases}$$

To conclude that $|||R|||$ is well-defined it then suffices to observe that the set of scalar multiples of elements in $K(n,t)$ is closed under addition. Indeed, if

$$R_{\mathbf{i}} = \langle u, A(\mathbf{i})v\rangle \text{ and } \tilde{R}_{\mathbf{i}} = \langle \tilde{u}, \tilde{A}(\mathbf{i})\tilde{v}\rangle,$$

for some $u, v, \tilde{u}, \tilde{v} \in \mathbb{R}^d$ with $\|u\|^2 = \|v\|^2 = w$, $\|\tilde{u}\|^2 = \|\tilde{v}\|^2 = \tilde{w}$ and maps $A, \tilde{A}\colon [n] \to B_{M(d)}$, then

$$R_{\mathbf{i}} + \tilde{R}_{\mathbf{i}} = \langle \hat{u}, \hat{A}(\mathbf{i})\hat{v}\rangle,$$

where $\hat{u}, \hat{v} \in \mathbb{R}^{2d}$ are the vectors with $\|\hat{u}\|^2 = \|\hat{v}\|^2 = w+\tilde{w}$ defined by $\hat{u} := u\oplus\tilde{u}$, $v := v \oplus \tilde{v}$ and the map $\hat{A}\colon [n] \to B_{M(2d)}$ is defined via

$$\hat{A}(i) = \begin{pmatrix} A(i) & 0 \\ 0 & \tilde{A}(i) \end{pmatrix}.$$

This construction also shows that $|||\cdot|||$ satisfies the triangle inequality. It is also clear that $|||\cdot|||$ is homogeneous and that $|||R||| = 0$ if and only if $R = 0$, so $|||\cdot|||$ is a norm.

Finally, note that the completely bounded norm of a t-tensor $R \in \mathbb{R}^{n\times\cdots\times n}$ is given by

$$\|T\|_{\mathrm{cb}} = \sup\Big\{ \Big| \sum_{\mathbf{i}\in[n]^t} T_{\mathbf{i}} \langle u, A(\mathbf{i})v\rangle \Big| \;\Big|\; d \in \mathbb{N},\ u, v \in S^{d-1},\ A\colon [n] \to B_{M(d)} \Big\},$$

so $\|T\|_{\mathrm{cb}} = |||T|||_*$, and by the fact that the dual of the dual norm is the primal norm for finite-dimensional normed spaces, we conclude that

$$|||\cdot||| = |||\cdot|||_{**} = \|\cdot\|_{\mathrm{cb},*}.$$

□

As was observed in [ABP19], in general $\|T\|_{\mathrm{cb}}$ need not be equal to $\|T\circ\sigma\|_{\mathrm{cb}}$. It is not hard to show however, that when T is a matrix (i.e. a 2-tensor) we have $\|T^{\mathsf{T}}\|_{\mathrm{cb}} = \|T\|_{\mathrm{cb}}$. This is equivalent to $\|T \circ \sigma\|_{\mathrm{cb}} = \|T\|_{\mathrm{cb}}$ for the only

non-trivial permutation in $\mathcal{S}_2$. Doing so, this gives the following reformulation of the completely bounded norm of forms of degree 2.

Proposition 3.5. *Let $p \in \mathbb{R}[x_1, \ldots, x_n]_{=2}$ be a quadratic form and let T_p be the unique symmetric matrix associated to p via (7). Then $\|p\|_{\mathrm{cb}} = \|T_p\|_{\mathrm{cb}}$.*

Proof: Let $T \in \mathbb{R}^{n\times n}$ be a matrix. First, we have

$$\begin{aligned} \|T^{\mathsf{T}}\|_{\mathrm{cb}} &= \sup\Big\{\|\sum_{i,j} T_{j,i}A(i)B(j)\| \;\mid\; A, B\colon [n] \to B_{M(d)}\Big\} \\ &= \sup\Big\{\|\sum_{i,j} T_{j,i}B(j)^{\mathsf{T}}A(i)^{\mathsf{T}}\| \;\mid\; A, B\colon [n] \to B_{M(d)}\Big\} \\ &= \|T\|_{\mathrm{cb}}, \end{aligned} \tag{13}$$

where we use (twice) that for any matrix M we have $\|M\| = \|M^{\mathsf{T}}\|$.

Let $T \in \mathbb{R}^{n\times n}$ be a matrix with $p(x) = T(x)$. Then, $T_p = (T + T^{\mathsf{T}})/2$, so from the above and the triangle inequality it follows that

$$\|T_p\|_{\mathrm{cb}} = \frac{1}{2}\|T + T^{\mathsf{T}}\|_{\mathrm{cb}} \leq \frac{1}{2}(\|T\|_{\mathrm{cb}} + \|T^{\mathsf{T}}\|_{\mathrm{cb}}) = \|T\|_{\mathrm{cb}}.$$

Using Proposition 3.1 we conclude that $\|p\|_{\mathrm{cb}} = \|T_p\|_{\mathrm{cb}}$. □

Considering only bilinear forms gives the following corollary.

Corollary 3.6. *Let $p : \{-1,1\}^n \times \{-1,1\}^n \to \mathbb{R}$ be a bilinear form and let $A \in \mathbb{R}^{n\times n}$ be such that $p(x,y) = x^{\mathsf{T}}Ay$ for all $x, y \in \mathbb{R}^n$. Then, $\|A\|_{\mathrm{cb}} = \|p\|_{\mathrm{cb}}$.*

Proof: By Proposition 3.5 we have $\|p\|_{\mathrm{cb}} = \|T_p\|_{\mathrm{cb}}$. Now observe that $T_p = \frac{1}{2}\begin{pmatrix} 0 & A \\ A^{\mathsf{T}} & 0 \end{pmatrix}$ and hence

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

where the last equality uses (13).

Conversely, let $A, B\colon [n] \to B_{M(d)}$. Note that $\|\sum_{i,j\in[n]} A_{i,j}A(i)B(j)\| = \|\sum_{i,j\in[n]} A_{i,j}A(i)B(j)U\|$ for any unitary matrix U. We may therefore assume without loss of generality that

$$\|\sum_{i,j\in[n]} A_{i,j}A(i)B(j)\| = \Big|\sum_{i,j\in[n]} A_{i,j}\langle u, A(i)B(j)u\rangle\Big|,$$

for a single unit vector u. For every $i \in [n]$, define the following contractions:

$$Q_1(i) = A(i) = Q_2^{\mathsf{T}}(i), \qquad Q_2(n+i) = B(i) = Q_1^{\mathsf{T}}(n+i).$$

Then,

$$\begin{aligned}\|T_p\|_{\mathrm{cb}} &\geq \Big\| \sum_{i,j\in[n]} \frac{1}{2}\big(A_{i,j}Q_1(i)Q_2(n+j) + A_{j,i}Q_1(n+i)Q_2(j)\big)\Big\| \\ &= \Big| \sum_{i,j\in[n]} A_{i,j}\langle u, \frac{A(i)B(j) + B^{\mathsf{T}}(j)A^{\mathsf{T}}(i)}{2} u\rangle\Big| \\ &= \Big| \sum_{i,j\in[n]} A_{i,j}\langle u, A(i)B(j)u\rangle\Big|\end{aligned}$$

Taking the supremum over $A, B\colon [n] \to B_{M(d)}$ shows that $\|T_p\|_{\mathrm{cb}} \geq \|A\|_{\mathrm{cb}}$. □

We finally record the following useful property of $\Pi_{\mathcal{Q}}$.

Lemma 3.7. *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: We will use Proposition 2.5 throughout the 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 Lemma 3.7 and the triangle inequality. Similarly, 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 $\|\Pi_{\mathcal{Q}} p\|_{\mathrm{cb}} \leq \|p\|_{\mathrm{cb}}$. 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 Lemma 3.7 and in the third we have used the fact that the uniform measure is invariant under products of $z \in \{-1,1\}^n$. □

4. $\mathcal{E}(p,t)$ FOR BLOCK-MULTILINEAR FORMS

4.1. **Proof of main result.** In this subsection we will prove and formally state our main result.

Theorem 4.1. *Let $\mathcal{P}$ be a partition of $[n]$ in $2t$ subsets and $p \in V_{\mathcal{P}}$. Then,*

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

Proof: We start from the expression given in Theorem 2.6 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 3.7, 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 $\Pi_{\mathcal{P}} q \in V_{\mathcal{P}}$. We then use Proposition 3.1 to show 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 we use Lemma 3.7 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

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

The desired result then follows by exchanging the infimum and supremum, which we are allowed to do by von Neumann's minimax theorem (see, e.g., [Nik54] for a simple statement and proof) and the definition of $\|r\|_{\mathrm{cb},*}$. □

4.2. **How to compute the dual norms.** Theorem 4.1 provides a formula for $\mathcal{E}(p,t)$ when $p \in V_{\mathcal{P}}$ that is easier to work with than the one of Theorem 2.6, as we will see in the next sections. However, it is not clear yet how to compute the dual norms appearing in Theorem 4.1. Now, we will give expressions for both norms.

Proposition 4.2. *Let $\mathcal{P}$ be a partition of $[n]$ in t subsets and $p \in V_{\mathcal{P}}$. Then,*

$$\|p\|_{\infty,*} = \inf\{\|r\|_1 \mid r : \{-1,1\}^n \to \mathbb{R},\, r \in W_{\mathcal{P}},\, r_{=t} = p\}. \tag{14}$$

Proof: First, by Lagrange duality (cf. [BV04, Sec. 5.1.6]), we have

$$\begin{aligned} &\inf\left\{\|r\|_1 \mid r : \{-1,1\}^n \to \mathbb{R},\, r_{=t} = p\right\} \\ &= \sup\left\{\langle p, q\rangle \mid q \in \mathbb{R}[x_1,\ldots,x_n]_{=t},\, \|q\|_\infty \leq 1\right\} \\ &= \sup\left\{\langle p, q\rangle \mid q \in V_{\mathcal{P}},\, \|q\|_\infty \leq 1\right\} = \|p\|_{\infty,*}, \end{aligned} \tag{15}$$

where for the second equality we use that $p \in V_{\mathcal{P}}$ and we replace q by $\Pi_{\mathcal{P}} q$ (which does not increase its infinity-norm by Lemma 3.7). Second, we show that the right-hand side of Eq. (14) equals (15). The lower bound follows from inclusion of the feasible region, while the upper bound follows from Lemma 3.7 for $\|\cdot\|_1$. □

We have already seen in Example 2.4 that $\|p\|_{\infty,*} \neq \|p\|_1$ in general, because we are taking the dual norm with respect to $V_{\mathcal{P}}$. For completeness we give an alternative proof of the separation using Proposition 4.2.

Example 4.3. The upper bound $\|p\|_{\infty,*} \leq 1/3$ of Example 2.4 follows from Proposition 4.2 by considering the multilinear map $r(x) = (x_1 + x_2 + x_3 + x_1x_2x_3)/3$ that belongs to $W_{\mathcal{P}}$, satisfies $r_{=1}(x) = p(x) = (x_1 + x_2 + x_3)/3$ and $\|r\|_1 = 1/3$.

Proposition 4.4. *Let $\mathcal{P}$ be a partition of $[n]$ in t subsets and let $p \in V_{\mathcal{P}}$. Then,*

$$\|p\|_{\mathrm{cb},*} = t!\|T_p\|_{\mathrm{cb},*}. \tag{16}$$

Proof: By duality and definition of $\|\cdot\|_{\mathrm{cb}}$, we have that

$$\begin{aligned} \|p\|_{\mathrm{cb},*} &= \sup\{\sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha c'_\alpha : q \in V_{\mathcal{P}}, \|q\|_{\mathrm{cb}} \leq 1\} \\ &= \sup\{\sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha \sum_{\mathbf{i} \in \mathcal{I}_\alpha} T_{\mathbf{i}} : q \in V_{\mathcal{P}}, T(x) = q(x), \|T\|_{\mathrm{cb}} \leq 1\}, \end{aligned}$$

where c_α and c'_α are the coefficients of p and q, respectively. Now, let $R \in \mathbb{R}^{n\times\cdots\times n}$ be a t-tensor such that $R(x) = p(x)$ for every $x \in \mathbb{R}^n$. Then we have, using Eq. (6), that

$$\|p\|_{\mathrm{cb},*} = \sup\{ \sum_{\alpha\in\mathbb{Z}^n_{\geq 0}} \sum_{\mathbf{j}\in\mathcal{I}_\alpha} R_{\mathbf{j}} \sum_{\mathbf{i}\in\mathcal{I}_\alpha} T_{\mathbf{i}} : q \in V_{\mathcal{P}}, T(x) = q(x), \|T\|_{\mathrm{cb}} \leq 1\}.$$

In particular, if we choose R to be T_p, then we have

$$\begin{aligned}\|p\|_{\mathrm{cb},*} &= t! \sup\{ \sum_{\alpha\in\mathbb{Z}^n_{\geq 0}} \sum_{\mathbf{i}\in\mathcal{I}_\alpha} (T_p)_{\mathbf{i}} T_{\mathbf{i}} : q \in V_{\mathcal{P}}, T(x) = q(x), \|T\|_{\mathrm{cb}} \leq 1\} \\ &= t! \sup\{\langle T_p, T\rangle : q \in V_{\mathcal{P}}, T(x) = q(x), \|T\|_{\mathrm{cb}} \leq 1\}.\end{aligned}$$

We now show that the expression on the right equals $t!$ times $\|T_p\|_{\mathrm{cb},*}$, which we recall can be written as

$$\|T_p\|_{\mathrm{cb},*} = \sup\{\langle T_p, T\rangle : \|T\|_{\mathrm{cb}} \leq 1\}. \tag{17}$$

By inclusion of the feasible region we have that $\|p\|_{\mathrm{cb},*} \leq t!\|T_p\|_{\mathrm{cb},*}$. For the other inequality, let $T \in \mathbb{R}^{n\times\cdots\times n}$ be a t-tensor and consider $\Pi_{\mathcal{P}} T$ as in Eq. (10). By Proposition 2.5 we have $\|\Pi_{\mathcal{P}} T\|_{\mathrm{cb}} \leq \|T\|_{\mathrm{cb}} \leq 1$. Also note that the polynomial $\Pi_{\mathcal{P}} T(x)$ belongs to $V_{\mathcal{P}}$, because $(\Pi_{\mathcal{P}} T)_{\mathbf{i}} = 0$ unless $\mathbf{i}$ contains exactly one index from each set in the partition $\mathcal{P}$. It remains to observe that $(\Pi_{\mathcal{P}} T)_{\mathbf{i}} = T_{\mathbf{i}}$ for all indices $\mathbf{i} \in [n]^t$ for which $(T_p)_{\mathbf{i}} \neq 0$ and therefore

$$\langle T_p, T\rangle = \langle T_p, \Pi_{\mathcal{P}} T\rangle.$$

This shows that $\|p\|_{\mathrm{cb},*} \geq t!\|T_p\|_{\mathrm{cb},*}$. □

5. No additive converse for the polynomial method

In this section we will show that there is no analogue of Corollary 1.2 for polynomials of degree 4. In other words, we will prove Theorem 1.3.

Theorem 1.3. *There is no constant $\varepsilon \in (0,1)$ such that for every bounded polynomial p of degree at most 4 we have $\mathcal{E}(p,2) \leq \varepsilon$.*

Proof: For any partition $\mathcal{P}$ of $[n]$ in $2t$ subsets, Theorem 4.1 shows that

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

Consider now the case $t = 2$ and the partition $\mathcal{P}_n = \{\{1, \ldots, n\}, \{n+1, \ldots, 2n\}, \{2n+1, \ldots, 3n\}, \{3n+1\}\}$ of $[3n+1]$. In [BEG22, Sec. 3.2] a sequence of forms $p_n \in V_{\mathcal{P}_n}$ was constructed with the property that

$$\frac{\|p_n\|_{\mathrm{cb}}}{\|p_n\|_\infty} \to \infty. \tag{18}$$

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 $\|r\|_{\mathrm{cb},*} \geq K\|r\|_{\infty,*}$. Then,

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

which contradicts Eq. (18). 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. □

Remark 5.1. In the above proof we used the fact that a sequence of forms $(p_n)_{n\in\mathbb{N}}$ with $\|p_n\|_{\mathrm{cb}}/\|p_n\|_\infty \to \infty$ implies the *existence* of a sequence $r_n \in V_{\mathcal{P}_n}$ with $\|r_n\|_{\mathrm{cb},*}/\|r_n\|_{\infty,*} \to 0$. In [BEG22, Sec. 3.2] such a sequence p_n was constructed. Let us point out that their construction in fact allows for an explicit description of a sequence r_n as well, for the details see Appendix A.

6. Characterizing K_G with 1-query quantum algorithms

In this section we show the best additive error up to which 1-query quantum algorithms can compute bounded bilinear forms is exactly $1 - 1/K_G$, where K_G is the real Grothendieck constant. 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 $1 - 1/K_G$. It thus remains to show the lower bound.

Theorem 1.4. *Let $\mathcal{BB}$ the set of bounded bilinear forms. Then,*

$$\sup_{p \in \mathcal{BB}} \mathcal{E}(p, 1) = 1 - \frac{1}{K_G}.$$

Proof: Theorem 4.1 shows the following:

$$\sup_{p\in\mathcal{BB}} \mathcal{E}(p,1) = \sup_{\|p\|_\infty\le 1} \sup_{\|r\|_{\infty,*}\le 1} \langle p, r\rangle - \|r\|_{\mathrm{cb},*} \tag{19}$$

$$= \sup_{\|r\|_{\infty,*}\le 1} \|r\|_{\infty,*} - \|r\|_{\mathrm{cb},*} \tag{20}$$

$$= \sup_{\|r\|_{\infty,*}=1} 1 - \|r\|_{\mathrm{cb},*}.$$

It thus remains to show that for bilinear forms there exists a constant $K > 0$ such that $\|p\|_{\infty,*} \le K\|p\|_{\mathrm{cb},*}$, and K_G is the smallest such constant. We do so starting from Grothendieck's theorem for matrices. It states that for $A \in \mathbb{R}^{n\times n}$ we have $\|A\|_{\mathrm{cb}} \le K\|A\|_\infty$, and K_G is the smallest such constant. Each bilinear form $p : \{-1,1\}^n \times \{-1,1\}^n \to \mathbb{R}$ uniquely corresponds to a matrix $A \in \mathbb{R}^{n\times n}$ such that $p(x,y) = x^{\mathsf{T}}Ay$. Moreover, for such p and A one has $\|p\|_\infty = \|A\|_\infty$ (immediate) and in Corollary 3.6 we showed $\|p\|_{\mathrm{cb}} = \|A\|_{\mathrm{cb}}$. A duality argument then concludes the proof: if $K > 0$ is such that $\|p\|_{\mathrm{cb}} \le K\|p\|_\infty$, then

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

□

7. Alternative proof of the main result via semidefinite programming

First of all, we will state Theorem 7.1 (which corresponds, after some reformulation, to equation (20) of [GL19]), that gives an optimization problem equivalent to the dual of the SDP $\mathcal{E}(f,t)$. Before that, we introduce the following notation. Given $\mathbf{i} \in [n+1]^{2t}$, $\alpha(\mathbf{i}) \in \{0,1\}^n$ is defined as

$$(\alpha(\mathbf{i}))_m := \begin{cases} 1 & \text{if } m \in [n] \text{ and } m \text{ occurs an odd number of times in } \mathbf{i}, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 7.1 ([GL19]). *Let $f : \{-1,1\}^n \to \mathbb{R}$ and $t \in \mathbb{N}$. Then,*

$$\mathcal{E}(f,t) = \sup\ (\langle f, r\rangle - w)/\|r\|_1 \tag{21}$$
$$\text{s.t. } r : \{-1,1\}^n \to \mathbb{R},\ d \in \mathbb{R}$$
$$A_s \colon [n+1] \to B_{M(d)} \text{ for all } s \in [2t]$$
$$u, v \in \mathbb{R}^d,\ w = \|u\|^2 = \|v\|^2$$
$$c_{\alpha(\mathbf{i})} = \langle u, A_1(i_1)\dots A_t(i_t)v\rangle \text{ for all } \mathbf{i} \in [n+1]^{2t},$$

where c_α are the coefficients of r.[5]

Second, we show that in the case of f belonging to $W_{\mathcal{P}}$, we can restrict r to belong to $W_{\mathcal{P}}$. As before, we also show that a single contraction-valued map A suffices.[6]

Lemma 7.2. *Let $\mathcal{P}$ be a partition of $[n]$ in $2t$ subsets and let $p \in W_{\mathcal{P}}$. Then,*

$$\begin{aligned} \mathcal{E}(p,t) = \sup\ & (\langle p, r\rangle - w)/\|r\|_1 \\ \text{s.t. } & r : \{-1,1\}^n \to \mathbb{R},\ r \in W_{\mathcal{P}}, d \in \mathbb{R} \\ & A\colon [n+1] \to B_{M(d)},\ \text{for } s \in [2t] \\ & u, v \in \mathbb{R}^d,\ w = \|u\|^2 = \|v\|^2 \\ & c_{\alpha(\mathbf{i})} = \langle u, A(\mathbf{i})v\rangle \text{ for all } \mathbf{i} \in [n+1]^{2t}\ , \end{aligned} \tag{22}$$

where c_α are the coefficients of r.

Proof: Let $\mathcal{E}^*(p,t)$ be the expression in the right-hand side of Eq. (22). By inclusion of the feasible region, $\mathcal{E}(p,t) \geq \mathcal{E}^*(p,t)$. To prove the other inequality, consider a feasible instance (u, v, w, A_s, r) for the SDP (21). Consider the contraction-valued map $\tilde{A}(i) := \sum_{s\in[2t]} e_s e_{s+1}^{\mathsf{T}} \otimes \hat{A}_s(i)$ for $i \in [n]$, where $\hat{A}_s(i)$ is a $d2^{2t} \times d2^{2t}$ matrix defined by

$$\hat{A}_s(i) = \bigoplus_{z\in\{-1,1\}^{2t}} (A_s \cdot z)(i).$$

We also define $\tilde{A}(n+1) := 0$ and the vectors $\tilde{u} = e_1 \otimes \hat{u}$ and $\tilde{v} = e_{2t+1} \otimes \hat{v}$, where $\hat{u}$ is the $2^t d$-dimensional vector defined as the (normalized) direct sum of 2^t copies of u, i.e.,

$$\hat{u} = \frac{1}{\sqrt{2^{2t}}} \bigoplus_{z\in\{-1,1\}^{2t}} u,$$

and the same for $\hat{v}$, but with an appropriate sign in each of the copies

$$\hat{v} = \frac{1}{\sqrt{2^{2t}}} \bigoplus_{z\in\{-1,1\}^{2t}} v \prod_{I\in\mathcal{P}} z_I.$$

This way, $(\tilde{u}, \tilde{v}, w, \tilde{A}, \Pi_{\mathcal{P}} r)$ is a feasible instance of $\mathcal{E}^*(p,t)$. Indeed, if $\mathbf{i}$ takes the value $n+1$ at least once or has any repeated indices, then $\alpha(\mathbf{i})_1 + \cdots + \alpha(\mathbf{i})_n < 2t$,

[5]Following [GL19] one obtains Theorem 7.1, but with the A_s being unitary-valued maps. Every contraction-valued map can be turned into an equivalent unitary-valued map by block-encoding contractions into the top-left corner of unitaries.

[6]In fact, all of the contraction-valued maps A_s can be taken to be the same regardless f belongs to $W_{\mathcal{P}}$ or not, similarly to what is done in Proposition 3.2.

so $(\Pi_{\mathcal{P}} r)_{\alpha(\mathbf{i})} = 0$ because $\Pi_{\mathcal{P}} r \in W_{\mathcal{P}}$, and $\langle \tilde{u}, \tilde{A}(\mathbf{i})\tilde{v}\rangle = 0$ by construction. If $\mathbf{i} \in [n]^{2t}$ and has no repeated indices, we get that

$$\langle \tilde{u}, \tilde{A}(\mathbf{i})\tilde{v}\rangle = \frac{1}{2^{2t}} \sum_{z\in\{-1,1\}^{2t}} \langle u, A_1(i_1)\dots A_{2t}(i_{2t})v\rangle \prod_{I\in\mathcal{P}} z_I^{1+\sum_{j\in I}\alpha(\mathbf{i})_j}.$$

Now, reasoning as in Proposition 2.5, we get that

$$\langle \tilde{u}, \tilde{A}(\mathbf{i})\tilde{v}\rangle = \begin{cases} \langle u, A_1(i_1)\dots A_{2t}(i_{2t})v\rangle & \text{if } \mathbf{i} \text{ takes one value in each } I \in \mathcal{P}, \\ 0 & \text{otherwise,} \end{cases}$$

so putting everything together we get that

$$\tilde{c}_{\alpha(\mathbf{i})} = \langle \tilde{u}, \tilde{A}(\mathbf{i})\tilde{v}\rangle,$$

where $\tilde{c}_\alpha$ are the coefficients of $\Pi_{\mathcal{P}} r$. Since $\tilde{A}$ is contraction-valued and both $\|\tilde{u}\|^2 = \frac{1}{2^{2t}} \sum_{z\in\{-1,1\}^{2t}} \|u\|^2 = \|u\|^2 = w$ and $\|\tilde{v}\|^2 = w$, we conclude that $(\tilde{u}, \tilde{v}, w, \tilde{A}, \Pi_{\mathcal{P}} r)$ is a feasible instance of Eq. (22).

Finally, the value of $(\tilde{u}, \tilde{v}, w, \tilde{A}, \Pi_{\mathcal{P}} r)$ is at least as large as the one of (u, v, w, A, r):

$$\frac{\langle p, \Pi_{\mathcal{P}} r\rangle - w}{\|\Pi_{\mathcal{P}} r\|_1} = \frac{\langle p, r\rangle - w}{\|\Pi_{\mathcal{P}} r\|_1} \geq \frac{\langle p, r\rangle - w}{\|r\|_1},$$

where in the equality we have used that that p belongs to $W_{\mathcal{P}}$ and in the inequality we have used Lemma 3.7. □

Now, we are ready to prove Theorem 4.1, again.

Proof of Theorem 4.1: First note that given a feasible instance (u, v, w, A, r) for Eq. (22) we clearly have that $r_{=2t} \in V_{\mathcal{P}}$. We show that also $w \geq \|r_{=2t}\|_{\mathrm{cb},*}$. By Propositions 3.3 and 4.4, this requires us to show that $t!$ times the unique symmetric $2t$-tensor $T_{r_{=2t}}$ associated to $r_{=2t}$ belongs to $wK(n, t)$. To do so, we show that $t!T_{r_{=2t}} = (\langle u, A(\mathbf{i})v\rangle)_{\mathbf{i}\in[n]^{2t}}$. Let $\mathbf{i} \in [n]^{2t}$. If $\mathbf{i}$ has repeated indices then $(T_{r_{=2t}})_{\mathbf{i}} = 0$ because $r_{=2t}$ is multilinear, and also $\langle u, A(\mathbf{i})v\rangle = 0$, because r is a feasible instance of Eq. (22). If $\mathbf{i}$ does not have repeated indices, then $t!(T_{r_{=2t}})_{\mathbf{i}} = c_{\alpha(\mathbf{i})}$, and also $\langle u, A(\mathbf{i})v\rangle = c_{\alpha(\mathbf{i})}$ because r is a feasible solution for Eq. (22).

On the other hand, given $r \in W_{\mathcal{P}}$ there is an instance (u, v, w, A, r) with $w = \|r_{=2t}\|_{\mathrm{cb},*}$. Indeed, by Proposition 4.4 there is a map $A\colon [n] \to B_{M(d)}$ and vectors u, v whose norm squared is $\|r_{=2t}\|_{\mathrm{cb},*}$ such that $c_\alpha(r_{=2t}) = \langle u, A(\mathbf{i})v\rangle$ for every $\mathbf{i} \in \mathcal{I}_\alpha$ and every $\alpha \in \mathbb{Z}^n_{\geq 0}$. Note that in order to have a feasible instance for Eq. (22) we need to satisfy its last condition, and with these contractions we can only satisfy it for α such that $\alpha_1 + \cdots + \alpha_n = 2t$. To satisfy it for every α with $\alpha_1 + \cdots + \alpha_n \leq 2t$, we just have to change the contractions and the vectors by $\hat{A}(i) := \sum_{s\in[2t]} e_s e_{s+1}^{\mathsf{T}} \otimes A_s(i)$ and $\hat{u} := e_1 \otimes u$ and $\hat{v} := e_{t+1} \otimes v$ and

define the extra contraction as $\hat{A}(n+1) = 0$. This, way $(\hat{u}, \hat{v}, \|r_{=2t}\|_{\mathrm{cb},*}, \hat{A}, r)$ is a feasible instance. To sum up, so far we have proved that

$$\begin{aligned}\mathcal{E}(p,t) = \sup\ & (\langle p, r\rangle - \|r_{=2t}\|_{\mathrm{cb},*})/\|r\|_1 \\ & \text{s.t. } r : \{-1,1\}^n \to \mathbb{R},\ r \in W_{\mathcal{P}}.\end{aligned}$$

We finally reformulate the above in terms of $r_{=2t}$ using the following two observations. Since $p \in V_{\mathcal{P}}$ we have $\langle p, r\rangle = \langle p, r_{=2t}\rangle$. Moreover, by Proposition 4.2, we have $\|r_{=2t}\|_{\infty,*} = \inf\{\|r_{=2t}\|_1 \mid r : \{-1,1\}^n \to \mathbb{R},\ r \in W_{\mathcal{P}}\}$. Hence,

$$\begin{aligned}\mathcal{E}(p,t) = \sup\ & (\langle p, r_{=2t}\rangle - \|r_{=2t}\|_{\mathrm{cb},*})/\|r_{=2t}\|_{\infty,*} \\ & \text{s.t. } r_{=2t} \in V_{\mathcal{P}},\end{aligned}$$

which concludes the proof. □

8. An open question

Let $\mathcal{P}$ be a partition of of $[n]$ in $2t$ subsets and let $p \in V_{\mathcal{P}}$ with $\|p\|_\infty \leq 1$. From the characterization of quantum t-query algorithms of [ABP19] we know that there is a quantum query algorithm $\mathcal{A}$ that outputs $p/\|p\|_{\mathrm{cb}}$ on expectation. In particular,

$$|\mathbb{E}[\mathcal{A}(x)] - p(x)| = \left|\frac{p(x)}{\|p\|_{\mathrm{cb}}} - p(x)\right| \leq \|p\|_\infty\Big(1 - \frac{1}{\|p\|_{\mathrm{cb}}}\Big).$$

As a consequence, one has that

$$\mathcal{E}(p,t) \leq \|p\|_\infty\Big(1 - \frac{1}{\|p\|_{\mathrm{cb}}}\Big). \tag{23}$$

Our Theorem 4.1 implies that both sides of Equation (23) are equal when you take the supremum over all $p \in V_{\mathcal{P}}$. We wonder if that is true for every $p \in V_{\mathcal{P}}$.

Question 8.1. *Let $\mathcal{P}$ be a partition of $[n]$ in $2t$ subsets and let $p \in V_{\mathcal{P}}$. Is it true that*

$$\mathcal{E}(p,t) = \|p\|_\infty\Big(1 - \frac{1}{\|p\|_{\mathrm{cb}}}\Big)?$$

A positive answer to this question would strengthen our main technical contribution, Theorem 4.1. Also, if we focus on the case $t = 1$, it would imply that the method proposed in [AAI+16] to give an algorithm that computes $p/\|p\|_{\mathrm{cb}}$ with 1 query, provides the best 1 query approximation for every p (here the best means the one that minimizes $\mathcal{E}(p,1)$). The analogue would be true with the following method to the case $t \geq 1$: take the algorithm that outputs $p/\|p\|_{\mathrm{cb}}$, whose existence is ensured by the main result of [ABP19]. Finally, for the case $t = 1$, it would imply a clean link between the biases of two player XOR games

and quantum query algorithms. Indeed, given a matrix $A \in \mathbb{R}^{n\times n}$ it both defines a bounded bilinear form $p_A(x,y) = x^{\mathsf{T}}Ay$ and a two player XOR game G_A, where the referee asks the pair of questions (i,j) with probability

$$\pi(i,j) = \frac{|A_{i,j}|}{\sum_{i,j\in[n]} |A_{i,j}|}$$

and the payoff is given by

$$\mu(i,j,a,b) = \frac{1 + ab\cdot \operatorname{sgn}[A_{i,j}]}{2}.$$

Corollary 3.6 states that

$$\|p_A\|_\infty = \|A\|_\infty \text{ and } \|p_A\|_{\mathrm{cb}} = \|A\|_{\mathrm{cb}},$$

while Tsirelson's work [Tsi80] implies that the classical and quantum biases of G_A are

$$\beta(G_A) = \|A\|_\infty \text{ and } \beta^*(G_A) = \|A\|_{\mathrm{cb}}.$$

Thus, a positive answer to Question 8.1 would imply that

$$\mathcal{E}(p_A,1) = \beta(G_A)\Big(1 - \frac{1}{\beta^*(G_A)}\Big).$$

Acknowledgments. We thank anonymous referees for their helpful feedback.

References

[AAI+16] S. Aaronson, A. Ambainis, J. Iraids, M. Kokainis, and J. 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.

[Aar21] S. Aaronson. Open problems related to quantum query complexity. *ACM Transactions on Quantum Computing*, 2(4), 2021. ISSN 2643-6809. doi: 10.1145/3488559.

[ABDK16] S. Aaronson, S. Ben-David, and R. Kothari. Separations in query complexity using cheat sheets. STOC '16. Association for Computing Machinery, New York, NY, USA, 2016. ISBN 9781450341325. doi:10.1145/2897518.2897644.

[ABDK+21] S. Aaronson, S. Ben-David, R. Kothari, S. Rao, and A. Tal. Degree vs. approximate degree and quantum implications of huang's sensitivity theorem. STOC 2021. Association for Computing Machinery, New York, NY, USA, 2021. ISBN 9781450380539. doi:10.1145/3406325.3451047.

[ABP19] S. Arunachalam, J. Briët, and C. Palazuelos. Quantum query algorithms are completely bounded forms. *SIAM J. Comput*, 48(3):903–925, 2019. Preliminary version in ITCS'18.

[Amb06] A. Ambainis. Polynomial degree vs. quantum query complexity. *J. Comput. System Sci.*, 72(2):220–238, 2006. Earlier version in FOCS'03. quant-ph/0305028.

[Amb07] A. Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007. Earlier version in FOCS'04. arXiv:quant-ph/0311001.

[Amb18] A. Ambainis. Understanding quantum algorithms via query complexity. In *Proceedings of the International Congress of Mathematicians (ICM 2018)*, pages 3265–3285. 2018. doi:10.1142/9789813272880_0181.

[BBC+01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. ISSN 0004-5411. doi: 10.1145/502090.502097.

[BEG22] J. Briët and F. Escudero Gutiérrez. On Converses to the Polynomial Method. In *17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022)*, volume 232 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 6:1–6:10. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. ISBN 978-3-95977-237-2. ISSN 1868-8969. doi: 10.4230/LIPIcs.TQC.2022.6.

[BKT20] M. Bun, R. Kothari, and J. Thaler. The polynomial method strikes back: Tight quantum query bounds via dual polynomials. *Theory of Computing*, 16(10):1–71, 2020. doi:10.4086/toc.2020.v016a010.

[BMMN13] M. Braverman, K. Makarychev, Y. Makarychev, and A. Naor. The Grothendieck constant is strictly smaller than Krivine's bound. *Forum Math. Pi*, 1:453–462, 2013. Preliminary version in FOCS'11. arXiv:1103.6161.

[BSdW22] N. Bansal, M. Sinha, and R. de Wolf. Influence in Completely Bounded Block-Multilinear Forms and Classical Simulation of Quantum Algorithms. In *37th Computational Complexity Conference (CCC 2022)*, volume 234, pages 28:1–28:21. 2022. doi:10.4230/LIPIcs.CCC.2022.28.

[BV04] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004. doi:10.1017/CBO9780511804441.

[Dav84] A. Davie. Lower bound for K_G, 1984. Unpublished.

[GL19] S. Gribling and M. Laurent. Semidefinite programming formulations for the completely bounded norm of a tensor. *arXiv preprint arXiv:1901.04921*, 2019.

[Gro53] A. Grothendieck. *Résumé de la théorie métrique des produits tensoriels topologiques*. Soc. de Matemática de São Paulo, 1953.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.

[HW+79] G. H. Hardy, E. M. Wright, et al. *An introduction to the theory of numbers*. Oxford university press, 1979.

[MMFPSS22] M. S. Moslehian, G. Muñoz-Fernández, A. Peralta, and J. Seoane-Sepúlveda. Similarities and differences between real and complex banach spaces: an overview and recent developments. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 116(2):1–80, 2022.

[Nik54] H. Nikaidô. On von Neumann's minimax theorem. *Pacific Journal of Mathematics*, 4:65–72, 1954.

[O'D14] R. O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014.

[Pau03] V. Paulsen. *Completely Bounded Maps and Operator Algebras*. 02 2003. ISBN 9780521816694. doi:10.1017/CBO9780511546631.

[Ree91] J. Reeds. A new lower bound on the real Grothendieck constant, 1991. Manuscript (`http://www.dtc.umn.edu/~reedsj/bound2.dvi`).

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computing*, 26(5):1484–1509, 1997. Earlier version in FOCS'94.

[Tsi80] B. S. Tsirelson. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 1980. doi:https://doi.org/10.1007/BF00417500.

[TT21] T. Tao and J. Teräväinen. Quantitative bounds for Gowers uniformity of the Möbius and von Mangoldt functions. *arXiv preprint arXiv:2107.02158*, 2021.

[TV06] T. Tao and V. H. Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006.

[Var74] N. Varopoulos. On an inequality of von Neumann and an application of the metric theory of tensor products to operators theory. *Journal of Functional Analysis*, 16(1):83–100, 1974. ISSN 0022-1236. doi:https://doi.org/10.1016/0022-1236(74)90071-8.

Appendix A. Explicit witnesses for Theorem 1.3

Here we show how the ideas from [BEG22], combined with Propositions 3.3 and 4.4, can be used to explicitly describe a sequence of polynomials $r_n \in V_{\mathcal{P}_n}$ that satisfies

$$\frac{\|r_n\|_{\mathrm{cb},*}}{\|r_n\|_{\infty,*}} \to 0,$$

where $\mathcal{P}_n = \{\{1,\dots,n\},\{n+1,\dots,2n\},\{2n+1,\dots,3n\},\{3n+1\}\}$. Below, C will denote an absolute positive constant whose value may be different at each occurrence.

We begin by introducing the Möbius function $f_0 : \mathbb{N} \to \{-1,0,1\}$. An integer $a \in \mathbb{N}$ has a unique prime-factorization $a = p_1^{n_1}\cdots p_t^{n_t}$ for distinct primes $p_1 < p_2 < \cdots < p_t$ and positive integers $n_1,\dots,n_t$. We say that a is square-free if all n_is equal 1. Define

$$f_0(a) := \begin{cases} 1 & \text{if } a \text{ is square-free and has an even number of prime factors} \\ -1 & \text{if } a \text{ is square-free and has an odd number of prime factors} \\ 0 & \text{if } a \text{ is not square-free.} \end{cases}$$

Then, we define $q_n \in \mathbb{R}[x_1,\dots,x_{3n}]$ by

$$q_n(x) := \sum_{a,b\in\mathbb{Z}_n} x_{[a]_n} x_{n+[a+b]_n} x_{2n+[a+2b]_n} f_0([a+3b]_n), \tag{24}$$

where $[a]_n$ is the only integer belonging to $[n]$ that is congruent with a mod n. A basic bound on the number of square-free integers [HW+79, page 269] shows that

$$\|q_n\|_2^2 \geq Cn^2. \tag{25}$$

Moreover, a recent result of Tao and Teräväinen [TT21] on the Gowers 3-uniformity norm of q_n and the generalized von Neumann inequality from additive combinatorics [TV06, Lemma 11.4] give that

$$\|q_n\|_\infty \leq \frac{n^2}{(\log\log n)^C}. \tag{26}$$

Now define $p_n, r_n \in V_{\mathcal{P}_n}$ by

$$p_n(x, x_{3n+1}) := \frac{q(x)x_{3n+1}}{\|q_n\|_\infty},$$
$$r_n(x, x_{3n+1}) := q(x)x_{3n+1}.$$

Since $\|p_n\|_\infty = 1$, it follows from (25) and (26) that

$$\|r_n\|_{\infty,*} \geq \langle r_n, p_n\rangle = \frac{\|q_n\|_2^2}{\|q_n\|_\infty} \geq C(\log\log n)^C. \tag{27}$$

To upper bound $\|r_n\|_{\mathrm{cb},*}$, one can use the following lemma proved in [BEG22], which is a basic variant of an idea of Varopoulos [Var74].

Lemma A.1 (tri-linear Varopoulos decomposition)**.** *For q_n as in (24), there exist $d \in \mathbb{N}$, $A : [3n] \to B_{M_d}$ and $u, v \in S^{d-1}$ such that*[7]

$$\begin{aligned} 0 &= \langle u, A(i)A(j)A(k)A(l)v\rangle \\ 3!(T_{q_n})_{ijk} &= \langle u, A(i)A(j)A(k)v\rangle \\ 0 &= \langle u, A(i)A(j)v\rangle \\ 0 &= \langle u, A(i)v\rangle, \end{aligned}$$

for all $i, j, k, l \in [3n]$.

If we extend the operator-valued map $A : [3n] \to B_{M_d}$ from the above lemma by defining $A(3n+1) := \mathrm{Id}$, then, for all $i, j, k, l \in [3n+1]$, we have

$$4!(T_{r_n})_{ijkl} = \langle u, A(i)A(j)A(k)A(l)v\rangle.$$

Thus, from Propositions 3.3 and 4.4 it follows that $\|r_n\|_{\mathrm{cb},*} \leq 1$. Combining with (27), we obtain the desired result

$$\frac{\|r_n\|_{\mathrm{cb},*}}{\|r_n\|_{\infty,*}} \leq \frac{1}{C(\log\log n)^C} \to 0.$$

[7]Strictly speaking, $0 = \langle u, A(i)A(j)A(k)A(l)v\rangle$ is not proven in Lemma 5 of [BEG22], but the matrices defined in the proof of that lemma are easily verified to satisfy this.

CWI & QuSoft, Science Park 123, 1098 XG Amsterdam, The Netherlands
Email address: j.briet@cwi.nl

CWI & QuSoft, Science Park 123, 1098 XG Amsterdam, The Netherlands
Email address: feg@cwi.nl

Université Paris Cité, CNRS, IRIF, F-75013, Paris, France
Email address: gribling@irif.fr