2018 IEEE 59th Annual Symposium on Foundations of Computer Science

Classical lower bounds from quantum upper bounds

Shalev Ben-David*, Adam Bouland†, Ankit Garg‡ and Robin Kothari§
*University of Waterloo, Waterloo, Canada, Email: shalev.b@uwaterloo.ca
†University of California at Berkeley, Berkeley, CA, USA, Email: abouland@berkeley.edu
‡Microsoft Research India, Bangalore, India, Email: garga@microsoft.com
§Microsoft Research, Redmond, WA, USA, Email: robin.kothari@microsoft.com

***Abstract*—We prove lower bounds on complexity measures, such as the approximate degree of a Boolean function and the approximate rank of a Boolean matrix, using quantum arguments. We prove these lower bounds using a quantum query algorithm for the combinatorial group testing problem. We show that for any function f, the approximate degree of computing the OR of n copies of f is Omega(sqrtn) times the approximate degree of f, which is optimal. No such general result was known prior to our work, and even the lower bound for the OR of ANDs function was only resolved in 2013.**

We then prove an analogous result in communication complexity, showing that the logarithm of the approximate rank (or more precisely, the approximate gamma-2 norm) of F: X x Y to 0,1 grows by a factor of Omega (sqrtn) when we take the OR of n copies of F, which is also essentially optimal. As a corollary, we give a new proof of Razborov's celebrated Omega(sqrtn) lower bound on the quantum communication complexity of the disjointness problem.

Finally, we generalize both these results from composition with the OR function to composition with arbitrary symmetric functions, yielding nearly optimal lower bounds in this setting as well.

***Keywords*-quantum computing; computational complexity;**

I. Introduction

Quantum computing promises to allow the efficient solution of certain problems believed to be intractable for classical computers, and is therefore of great practical interest. From a mathematical perspective, another important contribution of quantum computing is the rise of the "quantum method" as a proof technique. That is, often one can prove purely classical (i.e., not quantum) mathematical statements using techniques from quantum information for which no classical proof is known, or where the quantum proof is substantially simpler than its classical counterpart.[1] For example, the non-existence of efficient 2-locally-decodable codes was first proven using quantum arguments [2]. The closure of the classical complexity class PP under intersection was first shown using classical techniques by Beigel, Reingold, and Spielman [3], but Aaronson showed it could be reproven using quantum techniques in a simpler way [4]. The survey by Drucker and de Wolf provides more examples of this proof technique [5].

1) OR composition: In this work, we apply the quantum method to resolve several composition questions for classical complexity measures in query complexity and communication complexity. A quintessential example of this type of question is the OR-composition question, which asks the following: Given a function f, how hard is it to compute the function $\mathsf{OR}_n \circ f$, the OR of n copies of f? One particular strategy for computing $\mathsf{OR}_n \circ f$ is to compose the best algorithms for OR_n and f in the given model of computation. For many complexity measures (including all the measures studied in this paper), the product of the complexities of OR_n and f will yield an upper bound on the complexity of $\mathsf{OR}_n \circ f$. Typically, we conjecture that this upper bound is optimal, but it is not obvious that this must be the case, and hence establishing such a lower bound is usually difficult (or possibly even false for some complexity measures). For example, it is known that this upper bound is optimal for deterministic [6], [7] and quantum query complexity [8], [9], but was only recently established for randomized query complexity [10].

In this paper we show an optimal OR-composition result for approximate degree, a complexity measure in query complexity first studied by Nisan and Szegedy [11], which lower bounds quantum query complexity [12], and a nearly optimal OR-composition theorem for approximate rank (or approximate γ_2-norm or generalized discrepancy), a measure in communication complexity which lower bounds quantum communication complexity [13], [14].

Our results significantly generalize previous OR-composition results for these measures. For instance, OR-composition for approximate degree was open for close to 20 years *just for the special case that f is the* AND *function*! After several incremental improvements (see Table I) by Shi [15], Ambainis [16], and Sherstov [17], the problem was recently resolved by Sherstov [18] and Bun and Thaler [19] using a linear programming characterization of approximate degree.

In contrast, we show a tight OR-composition theorem for approximate degree for *arbitrary* functions f, generalizing these works and newer results on constant-depth compositions of the AND and OR functions [20]. (In fact, we also

[1]This is analogous to how it is sometimes easier to prove a statement about real numbers using complex numbers, as expressed in the following quote usually attributed to Jacques Hadamard [1]: "The shortest path between two truths in the real domain passes through the complex domain".

2575-8454/18/$31.00 ©2018 IEEE
DOI 10.1109/FOCS.2018.00040

Bound	Citation
$O(n)$	Høyer, Mosca and de Wolf [23]
$\Omega\left(\sqrt{n}\right)$	Nisan and Szegedy [11]
$\Omega\left(\sqrt{n \log n}\right)$	Shi [15]
$\Omega\left(n^{0.66\ldots}\right)$	Ambainis [16]
$\Omega\left(n^{0.75}\right)$	Sherstov [17]
$\Omega(n)$	Sherstov [18] and Bun and Thaler [19]

Table I
HISTORY OF LOWER BOUNDS ON THE APPROXIMATE DEGREE OF $\mathsf{OR}_n \circ \mathsf{AND}_n$ (FROM [18])

provide an optimal lower bound on the approximate degree of the OR of possibly different functions f_i.)

In communication complexity, to the best of our knowledge no OR-composition result was known for approximate rank. Indeed, such a result would directly imply Razborov's celebrated $\Omega(\sqrt{n})$ lower bound on the quantum communication complexity of the disjointness function [21]. To highlight the power of our techniques, we provide a short proof of the $\Omega(\sqrt{n})$ lower bound for disjointness. We also provide a more direct proof of the recent lower bound on the quantum information complexity of disjointness [22].

2) Symmetric function composition: We then generalize our OR-composition results to hold for compositions with arbitrary symmetric functions, which are functions that only depend on the Hamming weight of the input. Other than OR, compositions with symmetric functions like parity and majority have been studied in complexity theory. For instance, the question of how difficult it is to compute $\mathsf{XOR}_n \circ f$ was already studied in 1982 in Yao's seminal paper on the XOR lemma [24] (see [25] for a general composition theorem for $g \circ f$ in this setting.). Since the class of symmetric functions includes the OR function, proving composition theorems for arbitrary symmetric functions is even harder. Such composition theorems are known for deterministic [6], [7] and quantum query complexity [8], [9]. But it remains open to show a similar theorem for randomized query complexity, where only partial results are known [26], [27].

3) Techniques: Although the final results for approximate degree and approximate rank are purely classical, our proofs use quantum algorithms in a crucial way, and there is no known classical proof of these results. We therefore believe this to be a powerful example of the "quantum method" [5]. However, we only use quantum algorithms in a black-box manner and the reader is not required to be familiar with quantum query complexity. We only use its relationship with polynomials due to Beals et al. [12] and the existence of a quantum algorithm for the combinatorial group testing problem due to Belovs [28].

Another salient feature of our proofs is that our lower bounds on various measures like approximate degree are proven using the existence of very fast quantum *algorithms* for related problems. This is part of a recent trend in complexity theory, sometimes called "ironic complexity theory" [29], in which lower bounds are proven using upper bounds. For instance, Williams' celebrated circuit lower bound for ACC uses this approach [30].

Our approach of using a fast quantum algorithm (by Belovs [28]) to prove lower bounds is inspired by the recent work of Hoza [31], who showed that fast quantum algorithms for certain query problems imply lower bounds in communication complexity. Hoza's work was, in turn, inspired by work of Cleve, van Dam, Nielsen, and Tapp [32], who used the Bernstein–Vazirani algorithm [33] to prove the first lower bound on the quantum communication complexity (with unlimited shared entanglement) of the inner product function. Similar proof techniques were also used by Buhrman and de Wolf [34] to show a lower bound on the quantum query complexity of searching a sorted list by a reduction to the hardness of computing parity.

II. OUR RESULTS

We now describe our results in more detail.

A. Approximate degree

For any Boolean function $f : \{0,1\}^n \to \{0,1\}$, the approximate degree of f, denoted $\widetilde{\deg}(f)$, is the minimum degree of any real polynomial p over the variables $x_1, \ldots, x_n$, such that $|f(x) - p(x)| \leq 1/3$ for all $x \in \{0,1\}^n$. Note that $\widetilde{\deg}(f) \leq n$ for all Boolean functions since any Boolean function can be represented exactly with a polynomial of degree n. Also note that negating the output of a function does not change its approximate degree, and neither does negating input bits. Hence $\widetilde{\deg}(\mathsf{OR}_n) = \widetilde{\deg}(\mathsf{AND}_n) = \widetilde{\deg}(\mathsf{NAND}_n)$ and results for one function carry over to the others.

Approximate degree was first studied by Nisan and Szegedy [11]. Since then, it has been used to prove oracle separations, design learning algorithms, and show lower bounds on quantum query complexity, formulas size, and communication complexity. (See [18], [19], [35] and the references therein for more information.) It can be used to prove lower bounds on quantum query complexity because for all (total or partial) functions f, we have $\mathrm{Q}(f) \geq \frac{1}{2}\widetilde{\deg}(f)$ [12], where $\mathrm{Q}(f)$ denotes the bounded-error quantum query complexity of f.

Although approximate degree has a simple definition in terms of polynomials, several simple questions about this measure remain open. Surprisingly, even the approximate degree of the depth-2 AND-OR tree $\mathsf{AND}_n \circ \mathsf{OR}_m$ remained open for close to 20 years! In 2013, after several incremental improvements (described in Table I), Sherstov [18] and Bun and Thaler [19] showed that

$$\widetilde{\deg}(\mathsf{AND}_n \circ \mathsf{OR}_m) = \Omega(\sqrt{nm}), \tag{1}$$

which is optimal [23]. These lower bounds were proved using a linear programming formulation of approximate degree, and exploited certain properties of the dual polynomial

for the OR function. In contrast to these approaches using dual polynomials, our OR-composition result for approximate degree uses completely different techniques and is more general:

Theorem 1: For any Boolean function $f : \{0,1\}^m \to \{0,1\}$, we have

$$\widetilde{\deg}(\mathsf{OR}_n \circ f) = \Omega(\sqrt{n}\,\widetilde{\deg}(f)). \tag{2}$$

This lower bound is tight due to a matching upper bound of Sherstov [35]. This resolves the OR-composition question for approximate degree. As an example, this now allows us to show the optimal bound $\widetilde{\deg}(\mathsf{OR}_n \circ \mathsf{MAJ}_n) = \Omega(n^{3/2})$, where MAJ is the majority function. Prior to our work, the best lower bound that could be proved with known techniques was $\widetilde{\deg}(\mathsf{OR}_n \circ \mathsf{MAJ}_n) = \Omega(n)$.

After characterizing the approximate degree of the depth-2 AND-OR tree, Bun and Thaler [20] also proved that the approximate degree of the depth-d AND-OR tree on n inputs is $\Omega(\sqrt{n}/\log^{d/2-1} n)$. Theorem 1 straightforwardly implies the optimal bound of $\Omega(\sqrt{n})$.

We then generalize Theorem 1 to a composition theorem for arbitrary symmetric functions g. Our OR-composition theorem plays a central role in the proof of our symmetric-function composition theorem, which we discuss in Section III.

Theorem 2: For any symmetric Boolean function $g : \{0,1\}^n \to \{0,1\}$ and any Boolean function $f : \{0,1\}^m \to \{0,1\}$, we have

$$\widetilde{\deg}(g \circ f) = \widetilde{\Omega}(\widetilde{\deg}(g)\,\widetilde{\deg}(f)). \tag{3}$$

This lower bound is also tight up to log factors due to a matching upper bound of Sherstov [35]. This resolves the symmetric-composition question for approximate degree.

B. Approximate rank or γ_2 norm

In communication complexity, we have two players Alice and Bob, who hold inputs $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ respectively. Their goal is to compute a function $F : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ on their inputs while minimizing the communication between them. One of the most studied functions in communication complexity is the set disjointness problem $\mathsf{DISJ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, defined as $\mathsf{DISJ}_n(x,y) = \bigvee_{i=1}^n (x_i \wedge y_i)$ for all $x, y \in \{0,1\}^n$.

The quantum communication complexity of the disjointness problem was one of the early open problems in quantum communication complexity. Let $\mathrm{Q}^*_{\mathrm{CC}}(F)$ denote the bounded-error quantum communication complexity of a function F with unlimited preshared entanglement. Then it follows from Grover's algorithm [36] and the query-to-communication simulation algorithm of Buhrman, Cleve, and Wigderson [37] that $\mathrm{Q}^*_{\mathrm{CC}}(\mathsf{DISJ}_n) = O(\sqrt{n}\log n)$, which was later improved to $\mathrm{Q}^*_{\mathrm{CC}}(\mathsf{DISJ}_n) = O(\sqrt{n})$ [38]. However the lower bound remained open until a breakthrough by Razborov [21], who showed that $\mathrm{Q}^*_{\mathrm{CC}}(\mathsf{DISJ}_n) = \Omega(\sqrt{n})$.

Razborov's result actually lower bounds a smaller complexity measure. With any communication problem $F : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, we can associate a $\{-1,+1\}$ matrix, called the sign matrix of F, whose (x,y) entry is $(-1)^{F(x,y)}$. Informally, the approximate rank of F, denoted $\widetilde{\mathrm{rank}}(F)$ is the least rank of any matrix that is entry-wise close to the sign matrix of F. (See the full version of this paper [39] for a more precise definition.) Another measure that is essentially equivalent to approximate rank is the approximate γ_2-norm of the sign matrix of F, which we denote $\widetilde{\gamma}_2(F)$, also defined in [39]. For any function F, $\log \widetilde{\gamma}_2(F)$ lower bounds its quantum communication complexity, and Razborov's result proves the stronger statement that $\log \widetilde{\gamma}_2(\mathsf{DISJ}_n) = \Omega(\sqrt{n})$.

We first show that our techniques yield a new proof of Razborov's celebrated $\Omega(\sqrt{n})$ lower bound for disjointness.

Theorem 3: Let $\mathsf{DISJ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be the set disjointness function defined as $\mathsf{DISJ}_n(x,y) = \bigvee_{i=1}^n (x_i \wedge y_i)$ for all $x, y \in \{0,1\}^n$. Then

$$\log \widetilde{\mathrm{rank}}(\mathsf{DISJ}_n) = \Omega(\sqrt{n}) \tag{4}$$

and

$$\log \widetilde{\gamma}_2(\mathsf{DISJ}_n) = \Omega(\sqrt{n}). \tag{5}$$

Note that this lower bound is tight due to the matching quantum algorithm of Aaronson and Ambainis [38]. Building on this, we generalize our result to an OR-composition theorem.[2]

Theorem 4: For any function $F : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, we have $\log \widetilde{\gamma}_2(\mathsf{OR}_n \circ F) = \widetilde{\Omega}\left(\sqrt{n} \log \widetilde{\gamma}_2(F)\right)$.

We then generalize this proof to show a nearly optimal composition theorem for an arbitrary symmetric function g and an arbitrary communication problem F.

Theorem 5: For any Boolean function $F : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, and any symmetric function $g : \{0,1\}^n \to \{0,1\}$, we have

$$\log \widetilde{\gamma}_2(g \circ F) \geq \widetilde{\deg}(g)^{1-o(1)} \log \widetilde{\gamma}_2(F). \tag{6}$$

Note that these lower bounds are also essentially tight, as a matching upper bound of $\log \widetilde{\gamma}_2(g \circ F) = \widetilde{O}(\widetilde{\deg}(g) \log \widetilde{\gamma}_2(F))$ can be proved by composing a polynomial for g with a matrix for F. (For details, see the full version of our paper [39]).

C. Further Extensions

We also prove two further extensions of our result. First, we generalize our tight OR-composition theorem for $\widetilde{\deg}(\mathsf{OR}_n \circ f)$ to the case of different functions f_i. We show

[2] An astute reader may worry that an OR-composition theorem cannot possibly hold in communication complexity because some functions do not become harder as we take the OR of many copies of the function. For example, the function $\overline{\mathsf{EQ}}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, defined as $\overline{\mathsf{EQ}}_n(x,y) = 0$ if and only if $x = y$, can be solved with $O(1)$ communication using a randomized or quantum protocol. Taking the OR of many copies of $\overline{\mathsf{EQ}}_n$ only yields a larger instance of $\overline{\mathsf{EQ}}$, which is no harder than before. However, Theorem 4 still holds because $\log \widetilde{\gamma}_2(\overline{\mathsf{EQ}}_n) \leq 0$.

a tight lower bound on the approximate degree of the OR of n possibly different functions f_i (which may possibly even have different input sizes). This completely characterizes the approximate degree of this function, and furthermore implies that the approximate degree of any constant-depth read-once formula is $\Omega(\sqrt{n})$. This lower bound is optimal, since an upper bound of $O(\sqrt{n})$ is known for the approximate degree of arbitrary read-once formulas (not just constant-depth) via the $O(\sqrt{n})$ upper bound on quantum query complexity [8] and it is an interesting open question if this upper bound is tight for arbitrary read-once formulas. For details see the full version of our paper [39].

Second, we show a lower bound on the quantum information complexity of the disjointness function. Quantum information complexity [40] is a information relaxation of quantum communication complexity, in the same sense that information complexity is a relaxation of communication complexity. Intuitively, instead of charging for the number of bits (or qubits) of communication if a protocol, information complexity only charges for the information transmitted by these bits (or qubits). We use our techniques to reprove the $\Omega(\sqrt{n})$ lower bound on the quantum information complexity of disjointness [22] up to log factors. This lower bound is already known, but the known proof uses an alternate characterization of quantum information complexity as amortized quantum communication complexity. In contrast, our proof is more direct and works with the information theoretic definition of quantum information complexity. For details see the full version of our paper [39].

III. High-level overview of techniques

While we prove several different lower bounds against measures in query and communication complexity, our proofs share several common techniques. In particular, all our proofs use Belovs' algorithm for the combinatorial group testing problem [28], which we now describe. Combinatorial group testing has a long history originating in the testing of World War II draftees for Syphilis [41], where the goal was to minimize the number of tests used to screen recruits. The basic idea was to pool multiple blood samples together before testing them; the blood test then reveals if anyone in the pool has the disease. In other words the test reveals the OR of the draftee's disease statuses within the group. One can easily see that if only one person has the disease, then one can use binary search to use only $\log n$ tests to identify which of n people has the disease; similarly one can show that if k people have the disease then $k \log n$ tests suffice.

More formally, in this problem there is a hidden string $x \in \{0,1\}^n$. One is allowed to query any subset $S \subseteq [n]$, and querying a subset S returns the OR of the bits of x in the subset, i.e., $\bigvee_{i \in S} x_i$. The goal is to use these subset queries to learn all of the bits of x. Clearly this can be achieved with n queries in almost any reasonable measure of query complexity, by querying each bit of the input separately, i.e., by querying the subsets $\{1\}, \ldots, \{n\}$. And as previously mentioned, for sparse inputs one can use fewer than n queries. But for worst-case inputs this trivial $O(n)$ query algorithm is optimal for classical (deterministic or randomized) query complexity. This is because if the string x contains a single 0, then this problem reduces to search. Therefore even a quantum algorithm for this query problem would require $\Omega(\sqrt{n})$ queries by the lower bound for Grover search [42]. Surprisingly, Belovs [28] showed that the quantum query complexity of this problem is at most $O(\sqrt{n})$ as well. This algorithm will play a key role in our proofs.

1) Approximate degree OR*-composition:* We first describe the ideas required to lower bound the approximate degree of functions of the form $\mathsf{OR}_n \circ f$, making note of the parts of the proof that fail in communication complexity.

Suppose by way of contradiction that $\widetilde{\deg}(\mathsf{OR}_n \circ f) = T$, where T is smaller than expected. This means we can compute the OR of n copies of a function f more easily than expected. But this also implies we can compute the OR of any subset $S \subseteq [n]$ of these n copies of f, since we can apply this algorithm to any subset S of our choice. (This argument already does not work in communication complexity when only one player knows the subset S, since that player would have to communicate S to the other player.)

Now we view the n outputs to the functions f as the hidden string $x \in \{0,1\}^n$ in the combinatorial group testing problem. In the combinatorial group testing problem, we assume we have the ability to query the OR of any subset of the bits, which is exactly what the assumed polynomial for $\mathsf{OR}_n \circ f$ gives us. From Belovs' quantum algorithm, we can construct an approximating polynomial for combinatorial group testing using the results of Beals et al. [12]. More precisely, since combinatorial group testing has an n-bit output, which is the hidden string $x \in \{0,1\}^n$, we use a decision version of this problem that simply outputs the parity of all the bits. We would now like to compose this polynomial with the assumed polynomials that allow us to compute the OR of a subset of the functions f. However, since the polynomials we wish to compose are approximating polynomials, they do not straightforwardly compose as expected, and to make this work, we use Sherstov's robust polynomial construction [35]. Finally, by composing these polynomials of degree T and degree $O(\sqrt{n})$, we get a polynomial of degree $O(T\sqrt{n})$ for computing the parity of all the functions f, i.e., we have shown that $\widetilde{\deg}(\mathsf{XOR}_n \circ f) = O(T\sqrt{n})$.

Computing the parity of n copies of a function f is usually n times as hard as computing f in most models of computation. Such a result is known for all the measures considered in this paper. The argument is now completed by combining the fact that $\widetilde{\deg}(\mathsf{XOR}_n \circ f) = \Omega(n \widetilde{\deg}(f))$ [43] and $\widetilde{\deg}(\mathsf{XOR}_n \circ f) = O(T\sqrt{n})$. Combining these gives us

$T = \Omega(\sqrt{n}\,\widetilde{\deg}(f))$, as desired.

Our results in communication complexity and the extension to arbitrary symmetric functions build on the ideas presented here. The flowchart in Fig. 1 describes the flow of ideas as well as the dependencies between various sections.

2) OR composition in communication complexity: The general strategy outlined above also works in communication complexity for the measures approximate rank and approximate gamma 2 norm, but we need to make additional arguments to make some steps work.

First, as noted above if one player knows a subset S of the shared input, but the other does not, it is not in general possible for them to run a communication protocol on that subset of their shared input. Thus our communication results have some overhead for dealing with this situation. Naively it would seem this overhead is too expensive, since Alice would need to communicate the entire subset S to Bob, which might be more expensive than the rest of the protocol. However, a recursive argument based on self-reducibility of the OR function allows the conversion of the additive $O(n)$ loss into a multiplicative polylogarithmic loss.

The other technically challenging part of porting this argument to communication complexity is in composing approximating polynomials with approximating matrices. This composition does not work as cleanly as in query complexity, and in some cases leads to an additional log factor loss.

3) Approximate degree PrOR-composition: To lower bound the approximate degree of functions of the form $g \circ f$, where g is a symmetric Boolean function, we first show an intermediate lower bound which will play a key role in our symmetric composition theorem. In particular we consider the Promise-OR function, denoted PrOR. The $\mathsf{PrOR}_n : \{0,1\}^n \to \{0,1,*\}$ function is the same as the OR function with the additional promise that the input has Hamming weight either 0 or 1. We first extend our lower bound on the approximate degree of $\mathsf{OR}_n \circ f$ to the partial function $\mathsf{PrOR}_n \circ f$. (For partial functions, we require that an approximating polynomial be close to the function on inputs in the domain, and be bounded in $[0,1]$ on all inputs including those outside the domain.)

The main insight that allows us to extend our lower bounds from OR to PrOR is that Belovs' algorithm actually solves a more general problem than combinatorial group testing, or more precisely, assumes a weaker access model to the input. In particular Belovs' algorithm only requires that the queries that are supposed to return the OR of a subset S, i.e., the value $\bigvee_{i \in S} x_i$, return the correct answer when $\sum_{i \in S} x_i \in \{0,1\}$. The queries may return incorrect answers on those subsets S for which $\sum_{i \in S} x_i > 1$.

While this is the key conceptual step needed for the generalization, working with partial functions presents several technical challenges. One of the main challenges corresponds to the robustness of polynomials, for which we used Sherstov's robust polynomial construction [35] previously.

Recall that our proof strategy is to compose the polynomial induced by Belovs' algorithm with a too-good-to-be-true (approximating) polynomial for $\mathsf{PrOR}_n \circ f$. This requires Belovs' polynomial to be robust, i.e. handle noisy inputs, which it may not be. For OR composition, we applied Sherstov's construction to obtain a robust version of Belovs' polynomial, which tolerates $1/3$ noise in the input bits. However, Sherstov's robust polynomial construction has a downside—it constructs polynomials that are not multilinear and whose value may blow up when an input variable is not close to being Boolean. This is exactly what can happen when we plug in an approximating polynomial for a partial function.

For this reason we use a different strategy for composing polynomials without using Shertov's technique. In particular we prove that the polynomials constructed from quantum algorithms are already mildly robust, i.e., they can handle $1/\operatorname{poly}(q)$ noise in the inputs, where q is the query complexity of the quantum algorithm. Since the polynomials induced by quantum algorithms are multilinear (and hence they are bounded whenever the inputs are in $[0,1]$), this allows us to extend our composition framework to the setting of partial functions (at the expense of losing a logarithmic factor).

We note we are not the first to prove intrinsic robustness of polynomials derived from quantum algorithms. For instance, Buhrman *et al.* [44] show that the polynomials derived from a quantum algorithm computing a *total* function f can tolerate $O(1/C(f))$ noise in the inputs, where $C(f)$ is the certificate complexity of f. However this result is insufficient for our application as we are applying it to a partial function. It is also not hard to show that all multilinear polynomials are $O(1/n)$ robust to noise, where n is the number of input bits. However, this does not suffice for our application either because the number of input bits for CGT is exponentially larger than its quantum query complexity. To the best of our knowledge this particular robustness property of polynomials derived from quantum algorithms was not known before and might be of independent interest.

4) Approximate degree composition for symmetric functions: We now describe how an approximate degree lower bound for $\mathsf{PrOR}_n \circ f$ can be used to lower bound the approximate degree of $g \circ f$, where g is a symmetric function. By a result of Paturi [45], it is known that the approximate degree of a symmetric n-bit function is completely determined by the Hamming weight closest to $n/2$ where the function g changes value. This implies that it suffices to prove the composition theorem for the case when the outer function g is PrTH^k_n which is defined as follows:

$$\mathsf{PrTH}^k_n(x) = \begin{cases} 0 & \text{if } |x| = k \\ 1 & \text{if } |x| = k+1 \\ * & \text{otherwise} \end{cases}.$$

Now the elementary, but crucial, observation is that

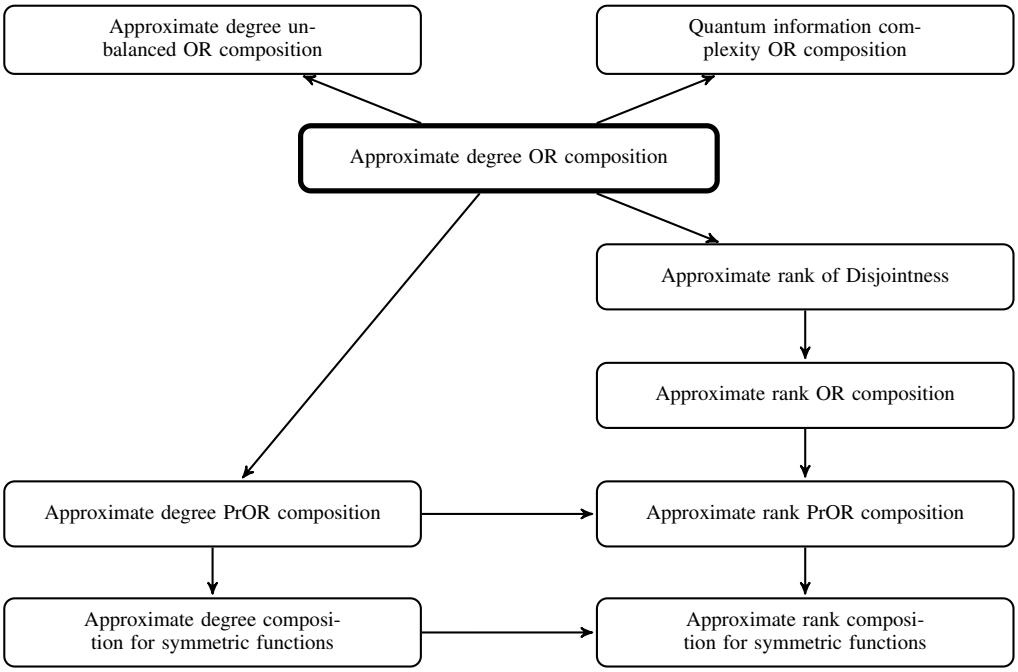


Figure 1. Reading order for the results shown in this paper. An arrow from A to B indicates that A is a prerequisite for reading B.

$\mathsf{PrTH}^k_{2k} \circ \mathsf{PrOR}_{n/2k}$ is a sub-function of PrTH^k_n. Hence we can obtain an approximate degree lower bound for $\mathsf{PrTH}^k_n \circ f$ using our composition theorem for PrOR, and a prior composition theorem of Sherstov that works for PrTH^k_{2k}. (Sherstov's result yields optimal composition theorems whenever the outer function has linear approximate degree [43]). This yields the composition theorem for arbitrary symmetric functions.

IV. Approximate degree

In this section we prove our OR composition theorem for approximate degree. We start with some definitions and known results in Section IV-A. In Section IV-B we prove the OR-composition theorem (Theorem 1), which is the starting point for the more general results proved in this paper. For the extension to arbitrary symmetric functions, and to communication complexity, please see the full version of our paper [39].

A. Preliminaries

In this section we collect some basic definition and known results about partial functions, approximate degree, and quantum query complexity. Partial functions will play a key role in our proofs, even though the main results are about total Boolean functions. Hence it is necessary to formally define partial functions and extend the definitions of approximate degree and quantum query complexity to partial functions.

1) Definitions: A partial Boolean function on m bits is a function that is only defined on a subset of $\{0,1\}^m$. There are two common ways to talk about partial functions. We can either view it as a function from D to $\{0,1\}$, where $D \subseteq \{0,1\}^m$, or as a function $f : \{0,1\}^m \to \{0,1,*\}$, where the function evaluates to $*$ outside D. We will mostly use the second definition and refer to the subset of $x \in \{0,1\}^m$ with $f(x) \neq *$ as the "promise" and denote it $\mathrm{Dom}(f)$. We can now define the composition of two partial functions more formally.

Definition 6: Let $g : \{0,1\}^n \to \{0,1,*\}$ and $f : \{0,1\}^m \to \{0,1,*\}$ be partial Boolean functions. Then we define $g \circ f : \{0,1\}^{nm} : \{0,1,*\}$ to be the partial function $g \circ f(x_1,\ldots,x_n) = g(f(x_1),\ldots,f(x_n))$ on those inputs for which all $x_i \in \mathrm{Dom}(f)$ and $(f(x_1),\ldots,f(x_n)) \in \mathrm{Dom}(g)$. The function evaluates to $*$ on all other inputs.

Most algorithmic models are easily generalized to partial functions. A (classical or quantum) algorithm for a partial function f is only required to be correct on inputs in $\mathrm{Dom}(f)$ and can have arbitrary behavior on inputs outside $\mathrm{Dom}(f)$. Extending the definition of approximate degree to partial functions is more subtle, and we motivate it by using an example of a partial function.

Recall that the OR function on n bits is defined as $\mathsf{OR}_n(x) = 0$ if $|x| = 0$ and $\mathsf{OR}_n(x) = 1$ if $|x| > 0$, where $|x|$ denotes the Hamming weight of x or the number of 1s in x. Let us define a partial function related to OR, which we call PromiseOR, as follows. $\mathsf{PrOR}_n : \{0,1\}^n \to \{0,1,*\}$ is the OR function with the additional promise that the input

has Hamming weight 0 or 1. In other words,

$$\mathsf{PrOR}_n(x) = \begin{cases} 0 & \text{if } |x| = 0 \\ 1 & \text{if } |x| = 1 \\ * & \text{otherwise} \end{cases}. \tag{7}$$

Intuitively PrOR contains the hardest instances of the OR function, and hence lower bounds for the OR function should hold against the PrOR function as well. For example, the quantum query complexity of PrOR is still $\Theta(\sqrt{n})$, and the deterministic and randomized query complexities of PrOR are $\Theta(n)$.

The approximate degree of PrOR is also $\Theta(\sqrt{n})$ as one might expect, as long as we define approximate degree for partial functions appropriately. For a partial function we clearly want the polynomial to approximate the function value on inputs in the promise. But we additionally want the polynomial to be *bounded*. We say a polynomial p on m variables is bounded if for all $x \in \{0,1\}^m$, $p(x) \in [0,1]$.

We use the following standard generalization of approximate degree to partial functions that is sometimes called "bounded approximate degree" in the literature [46].

Definition 7 (Bounded approximate degree): For any partial Boolean function $f : \{0,1\}^m \to \{0,1,*\}$, the bounded approximate degree of f, denoted $\widetilde{\deg}(f)$, is the minimum degree of any real polynomial p over the variables $x_1, \ldots, x_m$, such that

- (p is bounded) for all $x \in \{0,1\}^m$, $p(x) \in [0,1]$, and
- (p approximates f) for all $x \in \mathrm{Dom}(f)$, $|f(x) - p(x)| \leq 1/3$.

With this generalization of approximate degree, it is indeed true that $\widetilde{\deg}(\mathsf{PrOR}) = \Theta(\sqrt{n})$, as expected. Note that if we did not require that the polynomial be bounded on all inputs in the domain, then there would be a degree-1 polynomial that exactly represents the PrOR function, which is the polynomial $\sum_{i=1}^m x_i$.

Finally, we define what it means for a polynomial approximating a Boolean function to be δ-robust to input noise. Informally it means the polynomial continues to approximate the Boolean function even if the input bits are δ-far from being Boolean.

Definition 8 (δ-robustness to input noise): Let $h : \{0,1\}^n \to \{0,1,*\}$ be a partial Boolean function, and let $p : \{0,1\}^n \to \mathbb{R}$ be a polynomial. We say that p approximately computes h with robustness $\delta \in [0,1/2)$ if for any $x \in \mathrm{Dom}(h)$ and any $\Delta \in [-\delta,\delta]^n$, we have $|h(x) - p(x+\Delta)| \leq 1/3$.

2) Known results: We now collect some facts about bounded polynomials and bounded approximate degree that we need to prove our results.

The first result we use is Sherstov's result on making polynomials robust to noise [35, Theorem 1.1]. This result states that any polynomial p can be made $1/3$-robust to input noise by only increasing the degree of the polynomial by a constant factor.

Theorem 9 (Sherstov): Let $q : \{0,1\}^n \to [0,1]$ be a given polynomial. Then there exists a polynomial $q' : \mathbb{R}^n \to \mathbb{R}$ of degree $O(\deg(q) + \log(1/\epsilon))$ such that

$$|q(x) - q'(x+\Delta)| < \epsilon, \tag{8}$$

for all $x \in \{0,1\}^n$ and $\Delta \in [-1/3, 1/3]^n$.

We will also need a result of Sherstov that establishes the hardness of computing the parity of n copies of a function f, or more generally of n different functions $f_1, f_2, \ldots, f_n$. We denote the parity of these n functions $\mathsf{XOR}_n \circ (f_1, f_2, \ldots, f_n)$. Sherstov shows that the approximate degree of the parity of n functions is at least the sum of their approximate degrees [43, Theorem 5.9].

Theorem 10 (Sherstov): For any partial Boolean functions $f_1, f_2, \ldots, f_n$, we have

$$\widetilde{\deg}\Big(\mathsf{XOR}_n \circ (f_1, f_2, \ldots, f_n)\Big) = \Omega\Big(\sum_i \widetilde{\deg}(f_i)\Big). \tag{9}$$

In particular, for any partial Boolean function f, we have $\widetilde{\deg}(\mathsf{XOR}_n \circ f) = \Omega(n\,\widetilde{\deg}(f))$.

Finally, we also need the following result of Sherstov [43, Theorem 6.6] that proves a composition theorem for bounded approximate degree when the outer function has high degree.

Theorem 11 (Sherstov): Let $g : \{0,1\}^n \to \{0,1,*\}$ and $f : \{0,1\}^m \to \{0,1,*\}$ be partial Boolean functions. Then $\widetilde{\deg}(g \circ f) = \Omega\left(\widetilde{\deg}(g)^2\, \widetilde{\deg}(f)/n\right)$.

We now formally state the connection between quantum algorithms and approximating polynomials. Beals et al. [12] showed that the acceptance probability of a quantum query algorithm that makes few queries can be expressed as a low degree polynomial.

Theorem 12 (Beals et al.): Let A be a quantum query quantum algorithm that makes T queries to an oracle string $x \in \{0,1\}^n$ and outputs 1 with probability $A(x)$. Then there exists a real polynomial p of degree $2T$ over the variables $x_1, \ldots, x_n$ such that for all $x \in \{0,1\}^n$, $p(x) = A(x)$.

By choosing A to be a quantum algorithm that computes a partial function f to bounded error, we get the following corollary.

Corollary 13: For any partial Boolean function f, $\mathrm{Q}(f) \geq \frac{1}{2}\widetilde{\deg}(f)$.

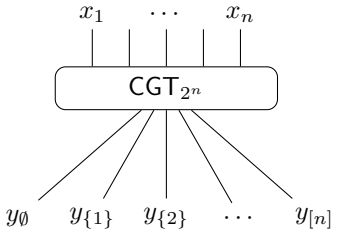
B. OR composition

In this section we prove our first main result, Theorem 1. We start by formally defining the combinatorial group testing problem, whose quantum query complexity was first studied by Ambainis and Montanaro [47].

1) Combinatorial group testing problem: Let CGT_{2^n} be the following problem. There is a hidden n-bit string x, which we have to determine using OR-queries to x. In an OR-query, we query the oracle with a subset $S \subseteq [n]$ and the oracle outputs 1 if there exists an $i \in S$ such that $x_i = 1$. In other words, the oracle's output is the function $\bigvee_{i \in S} x_i$. Formally, combinatorial group testing is a partial function

$$\mathsf{CGT}_{2^n} : \{0,1\}^{2^n} \to \{0,1\}^n \cup \{*\}, \tag{10}$$

where the input is a 2^n-bit string corresponding to the ORs of all possible subsets of x, and the promise is that all bits are indeed the OR of some string $x \in \{0,1\}^n$. When the promise is satisfied the desired output is the hidden string x. In other words, $y \in \{0,1\}^{2^n}$ is in $\mathrm{Dom}(\mathsf{CGT}_{2^n})$ if there exists an $x \in \{0,1\}^n$ such that for all $S \subseteq \{0,1\}^n$, $y_S = \bigvee_{i \in S} x_i$. For such a y, $\mathsf{CGT}_{2^n}(y) = x$. Note that for any $y \in \mathrm{Dom}(\mathsf{CGT}_{2^n})$, the string x is uniquely defined by $x_i = y_{\{i\}}$.



Note that although the problem has an input size of 2^n bits, the problem is easily solved with n queries as we can simply query all the singleton subsets $y_{\{i\}}$ for $i \in [n]$ to learn all the bits of x. Surprisingly, Belovs showed that the quantum query complexity of this problem is quadratically better than this [28, Theorem 3.1].

Theorem 14 (Belovs): The bounded-error quantum query complexity of CGT_{2^n} is $\Theta(\sqrt{n})$.

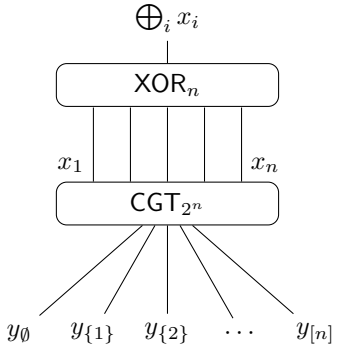
2) Decision problem associated with CGT*:* Since we want to work with polynomials, it will be more convenient to consider a decision problem corresponding to combinatorial group testing. To do so, we define the problem

$$\mathsf{XOR}_n \circ \mathsf{CGT}_{2^n} : \{0,1\}^{2^n} \to \{0,1,*\}, \tag{11}$$

which computes the parity of all the output bits of the CGT function.

In other words, $\mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}(y) = \mathsf{XOR}_n(\mathsf{CGT}_{2^n}(y))$, which is the XOR of all the bits of x, the hidden string in the CGT problem. Of course, any quantum algorithm that solves CGT_{2^n} and outputs x can instead output the parity of all the bits of x.

We can now construct a polynomial that approximates this Boolean function. Using Theorem 12 and Theorem 14, we can get a polynomial of degree $O(\sqrt{n})$ that approximates $\mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}$ on all inputs in the promise and is bounded in $[0,1]$ outside the promise.



For our application we need a more robust version of this polynomial. We need a polynomial that also works when the input variables are close to being Boolean. Combining this polynomial with Theorem 9, we get the following.

Theorem 15: There is a real polynomial p of degree $O(\sqrt{n})$ acting on 2^n variables $\{y_S\}_{S \subseteq [n]}$ such that for any input $y \in \{0,1\}^{2^n}$ with $\mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}(y) \neq *$, and any $\Delta \in [-1/3, 1/3]^{2^n}$,

$$|p(y + \Delta) - \mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}(y)| \leq 1/3, \tag{12}$$

and for all $y \in \{0,1\}^{2^n}$, $p(y) \in [0,1]$.

Proof: We start with Theorem 14 which gives us a quantum algorithm that makes $O(\sqrt{n})$ queries and approximates $\mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}$ to bounded error. Given a quantum algorithm computing a function with probability at least $2/3$, we can always boost the success probability to any constant in $(1/2, 1)$ by repeating the quantum algorithm and taking the majority vote of the outcomes. This only increases the quantum query complexity by a constant factor. Hence we can assume the quantum algorithm of Theorem 14 has error at most $1/6$ and apply Theorem 12 to get a polynomial p' of degree $O(\sqrt{n})$ such that for all $y \in \{0,1\}^{2^n}$ with $\mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}(y) \neq *$,

$$|p'(y) - \mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}(y)| \leq 1/6. \tag{13}$$

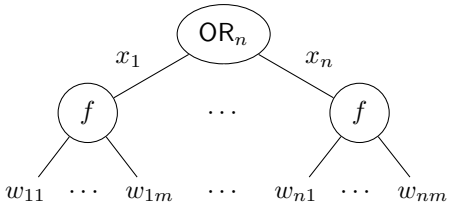
Furthermore, because p' arises from a quantum algorithm, we know that even on inputs outside the promise, i.e., inputs with $\mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}(y) = *$, $p'(y) \in [0,1]$. Since p' is bounded in $[0,1]$, we can apply Theorem 9 to it with $\delta = 1/6$ to obtain a new polynomial p that is robust to input noise. Note that since $|p'(y) - p(y)| \leq 1/6$ on all inputs $y \in \{0,1\}^{2^n}$, including those outside the promise, $p'(y) \in [-1/6, 7/6]$ for all $y \in \{0,1\}^{2^n}$. By rescaling and shifting the polynomial, we can map the interval $[-1/6, 7/6]$ to the interval $[0,1]$. Explicitly, we map $p(y)$ to $\frac{3}{4}(p(y) + \frac{1}{6})$. Since the original polynomial was in $[0, 1/6]$ for 0-inputs, this rescaled and shifted polynomial lies in $[0, 1/4]$, and similarly for 1-inputs it lies in $[3/4, 1]$, satisfying the conditions of the theorem. ∎

Using these results we can now prove the main result of this section.

Theorem 1: For any Boolean function $f : \{0,1\}^m \to \{0,1\}$, we have

$$\widetilde{\deg}(\mathsf{OR}_n \circ f) = \Omega(\sqrt{n}\ \widetilde{\deg}(f)). \tag{2}$$

Proof. Assuming $\widetilde{\deg}(f) \neq 0$ (otherwise the result is trivial), there is an input w^* such that $f(w^*) = 0$. Let w^* be any such input.



Let q be a polynomial of degree $T := \widetilde{\deg}(\mathsf{OR}_n \circ f)$ that approximates $\mathsf{OR}_n \circ f$. Let the input variables of the i^{th} copy of f, for $i \in [n]$, be called $w_{i1}, w_{i2}, \ldots, w_{im}$. Let us also define for all $i \in [n]$, $x_i := f(w_{i1}, w_{i2} \ldots, w_{im})$ to be the output of the i^{th} function f.

Thus q is a polynomial over the variables w_{11} to w_{nm} that approximately computes the Boolean function $\bigvee_{i=1}^n x_i$. From q, we can define for any $S \subseteq [n]$, a new polynomial q_S over the same set of variables $\{w_{ij} : i \in [n], j \in [m]\}$ that approximately computes the Boolean function $\bigvee_{i \in S} x_i$. The polynomial q_S is obtained from q by setting all the inputs to f for which $i \notin S$ equal to the special input w^* for which $f(w^*) = 0$. Thus the polynomial q_S is a polynomial over the same variables as q and has degree at most T and approximates the function $\bigvee_{i \in S} x_i$.

Now from Theorem 15, we have a real polynomial p of degree $O(\sqrt{n})$ acting on 2^n variables $\{y_S\}_{S \subseteq [n]}$ such that for any input $y \in \{0,1\}^{2^n}$ with $\mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}(y) \neq *$, and any $\Delta \in [-1/3, 1/3]^{2^n}$,

$$|p(y + \Delta) - \mathsf{XOR}_n \circ \mathsf{CGT}_{2^n}(y)| \leq 1/3. \tag{14}$$

Now we define a polynomial r in the variables w_{11} to w_{nm} by taking the polynomial p over variables y_S and replacing each occurrence of the variable y_S with the polynomial q_S.

Then because of equation (14) and the fact that the polynomial q_S approximates $\bigvee_{i \in S} x_i$, the polynomial r approximates the parity of the bits x_i (recall $x_i = f(w_{i1}, w_{i2} \ldots, w_{im})$). Also note that r is of degree $O(\sqrt{n}T)$. Thus we have

$$\widetilde{\deg}(\mathsf{XOR}_n \circ f) = O(\sqrt{n}T) = O(\sqrt{n}\ \widetilde{\deg}(\mathsf{OR}_n \circ f)). \tag{15}$$

Since $\widetilde{\deg}(\mathsf{XOR}_n \circ f)) = \Omega(n\ \widetilde{\deg}(f))$ (Theorem 10), we get $\widetilde{\deg}(\mathsf{OR}_n \circ f) = \Omega(\sqrt{n}\ \widetilde{\deg}(f))$.

Note that essentially the same proof yields a weak lower bound for the OR of n different functions $f_1, f_2, \ldots, f_n$. The proof would follow similarly, except instead of (15), we would arrive at

$$\widetilde{\deg}(\mathsf{XOR}_n \circ (f_1, f_2, \ldots, f_n)) = \tag{16}$$

$$O(\sqrt{n}\ \widetilde{\deg}(\mathsf{OR}_n \circ (f_1, f_2, \ldots, f_n))). \tag{17}$$

Now from Theorem 10, we have that $\widetilde{\deg}(\mathsf{XOR}_n \circ (f_1, f_2, \ldots, f_n)) = \Omega(n \min_i \widetilde{\deg}(f_i))$, and hence

$$\widetilde{\deg}(\mathsf{OR}_n \circ (f_1, f_2, \ldots, f_n)) = \Omega(\sqrt{n} \min_i \widetilde{\deg}(f_i)). \tag{18}$$

We use this weak result in the full version of our paper [39] to establish an optimal bound on the approximate degree of the OR of n different functions.

V. Open problems

We end with a discussion of main open problems left open by our work. The foremost open problem is whether the following conjecture is true.

Conjecture 1: For all Boolean functions $g : \{0,1\}^n \to \{0,1\}$ and $f : \{0,1\}^m \to \{0,1\}$, we have $\widetilde{\deg}(g \circ f) = \Omega(\widetilde{\deg}(g)\ \widetilde{\deg}(f))$.

Our result resolves this (up to log factors) when g is symmetric and f is arbitrary. A related question is whether any of our results can be reproved using the dual polynomials framework that has been used to show recent lower bounds for approximate degree [18]–[20]. In particular, is there a way to convert a dual witness for $\widetilde{\deg}(f)$ into a dual witness for $\widetilde{\deg}(\mathsf{OR} \circ f)$?

A more open ended question is whether this technique can be generalized to functions other than OR by developing new quantum algorithms. Belovs' algorithm used OR-queries to a hidden string x to learn all of x. What other quantum algorithms of this form exist? Are there nontrivial quantum algorithms that use g-queries to learn x for some function $g \notin \{\mathsf{OR}, \mathsf{XOR}\}$? Are there nontrivial quantum algorithms that use g-queries to compute some other function $h(x)$ of the input? This motivates the study of a whole class of quantum algorithms, which to the best of our knowledge has not been systematically studied other than in the work of Belovs [28].

Acknowledgment

We would like to thank Mark Bun and Justin Thaler for helpful discussions and feedback on an early draft of this work. We would also like to thank Harry Buhrman for bringing reference [34] to our attention. R.K. would like to thank Jeongwan Haah for helpful discussions regarding the proof of a theorem which appears in the full version of our paper [39]. S.B. would like to thank Xuangui Huang for helpful discussions.

Some of this work was performed while the first two authors were students at the Massachusetts Institute of Technology and the last author was a postdoctoral associate

at the Massachusetts Institute of Technology. This work was partially supported by ARO grant W911NF-12-1-0541, NSF grant CCF-1410022, NSF grant CCF-1629809, and a Vannevar Bush faculty fellowship.

REFERENCES

[1] J.-P. Kahane, "Jacques Hadamard," *The Mathematical Intelligencer*, vol. 13, no. 1, pp. 23–29, Dec 1991.

[2] I. Kerenidis and R. de Wolf, "Exponential lower bound for 2-query locally decodable codes via a quantum argument," in *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, 2003, pp. 106–115.

[3] R. Beigel, N. Reingold, and D. Spielman, "PP is closed under intersection," *Journal of Computer and System Sciences*, vol. 50, no. 2, pp. 191–202, 1995.

[4] S. Aaronson, "Quantum computing, postselection, and probabilistic polynomial-time," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461:2063, 2005, pp. 3473–3482.

[5] A. Drucker and R. d. Wolf, *Quantum Proofs for Classical Theorems*, ser. Graduate Surveys. Theory of Computing Library, 2011, no. 2.

[6] A. Tal, "Properties and applications of Boolean function composition," in *Innovations in Theoretical Computer Science (ITCS 2013)*, 2013, pp. 441–454, TR12-163.

[7] A. Montanaro, "A composition theorem for decision tree complexity," *Chicago Journal of Theoretical Computer Science*, vol. 2014, no. 6, Jul. 2014.

[8] B. W. Reichardt, "Reflections for quantum query algorithms," in *Proceedings of the twenty-second annual ACM-SIAM symposium on Discrete Algorithms (SODA 2011)*. SIAM, 2011, pp. 560–569.

[9] T. Lee, R. Mittal, B. W. Reichardt, R. Špalek, and M. Szegedy, "Quantum query complexity of state conversion," in *Foundations of Computer Science (FOCS 2011)*, 2011, pp. 344–353.

[10] M. Göös, T. S. Jayram, T. Pitassi, and T. Watson, "Randomized Communication vs. Partition Number," in *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), vol. 80, 2017, pp. 52:1–52:15.

[11] N. Nisan and M. Szegedy, "On the degree of Boolean functions as real polynomials," *Computational complexity*, vol. 4, no. 4, pp. 301–313, 1994.

[12] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, "Quantum lower bounds by polynomials," *Journal of the ACM*, vol. 48, no. 4, pp. 778–797, 2001.

[13] H. Buhrman and R. de Wolf, "Communication complexity lower bounds by polynomials," in *Proceedings 16th Annual IEEE Conference on Computational Complexity*, 2001, pp. 120–130.

[14] T. Lee and A. Shraibman, "An approximation algorithm for approximation rank," in *24th Annual IEEE Conference on Computational Complexity*, 2009, pp. 351–357.

[15] Y. Shi, "Approximating linear restrictions of Boolean functions," 2002. [Online]. Available: https://web.eecs.umich.edu/ shiyy/mypapers/linear02-j.ps

[16] A. Ambainis, "Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range." *Theory of Computing*, vol. 1, no. 1, pp. 37–46, 2005.

[17] A. A. Sherstov, "The intersection of two halfspaces has high threshold degree," *SIAM Journal on Computing*, vol. 42, no. 6, pp. 2329–2374, 2013.

[18] ——, "Approximating the AND-OR tree," *Theory of Computing*, vol. 9, no. 20, pp. 653–663, 2013.

[19] M. Bun and J. Thaler, "Dual lower bounds for approximate degree and Markov-Bernstein inequalities," in *Automata, Languages, and Programming: 40th International Colloquium, ICALP 2013*, 2013, pp. 303–314.

[20] ——, "Hardness amplification and the approximate degree of constant-depth circuits," in *Automata, Languages, and Programming: 42nd International Colloquium, ICALP 2015*, 2015, pp. 268–280.

[21] A. A. Razborov, "Quantum communication complexity of symmetric predicates," *Izvestiya: Mathematics*, vol. 67, no. 1, p. 145, 2003.

[22] M. Braverman, A. Garg, Y. K. Ko, J. Mao, and D. Touchette, "Near-optimal bounds on bounded-round quantum communication complexity of disjointness," in *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS 2015)*, 2015, pp. 773–791.

[23] P. Høyer, M. Mosca, and R. de Wolf, "Quantum search on bounded-error inputs," in *Automata, Languages and Programming: 30th International Colloquium, ICALP 2003*, ser. Lecture Notes in Computer Science, vol. 2719, 2003, pp. 291–299.

[24] A. C. Yao, "Theory and application of trapdoor functions," in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, ser. SFCS '82, 1982, pp. 80–91.

[25] R. O'Donnell, "Hardness amplification within NP," *Journal of Computer and System Sciences*, vol. 69, no. 1, pp. 68 – 94, 2004, special Issue on Computational Complexity 2002.

[26] D. Gavinsky, T. Lee, and M. Santha, "On the randomised query complexity of composition," *arXiv preprint arXiv:1801.02226*, 2018.

[27] S. Sanyal, "A composition theorem via conflict complexity," *arXiv preprint arXiv:1801.03285*, 2018.

[28] A. Belovs, "Quantum algorithms for learning symmetric juntas via the adversary bound," *Computational Complexity*, vol. 24, no. 2, pp. 255–293, 2015.

[29] S. Aaronson, "P=?NP," in *Open Problems in Mathematics*. Springer, 2016, pp. 1–122.

[30] R. Williams, "Nonuniform ACC circuit lower bounds," *Journal of the ACM*, vol. 61, no. 1, pp. 2:1–2:32, 2014.

[31] W. M. Hoza, "Quantum communication-query tradeoffs," *arXiv preprint arXiv:1703.07768*, 2017.

[32] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, "Quantum entanglement and the communication complexity of the inner product function," *Theoretical Computer Science*, vol. 486, pp. 11–19, 2013.

[33] E. Bernstein and U. Vazirani, "Quantum complexity theory," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1411–1473, 1997.

[34] H. Buhrman and R. de Wolf, "Lower bounds for quantum search and derandomization," *arXiv preprint arXiv:quant-ph/9811046*, 1998.

[35] A. A. Sherstov, "Making polynomials robust to noise," *Theory of Computing*, vol. 9, no. 18, pp. 593–615, 2013.

[36] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '96, 1996, pp. 212–219.

[37] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation," in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing (STOC 1998)*, 1998, pp. 63–68.

[38] S. Aaronson and A. Ambainis, "Quantum search of spatial regions," in *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2003)*, 2003, pp. 200–209.

[39] S. Ben-David, A. Bouland, A. Garg, and R. Kothari, "Classical lower bounds from quantum upper bounds," *arXiv:1807.06256*, 2018.

[40] D. Touchette, "Quantum information complexity," in *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*, ser. STOC '15, 2015, pp. 317–326.

[41] D. Du, F. K. Hwang, and F. Hwang, *Combinatorial group testing and its applications*. World Scientific, 2000, vol. 12.

[42] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997.

[43] A. A. Sherstov, "Strong direct product theorems for quantum communication and query complexity," *SIAM Journal on Computing*, vol. 41, no. 5, pp. 1122–1165, 2012.

[44] H. Buhrman, I. Newman, H. Rohrig, and R. de Wolf, "Robust polynomials and quantum algorithms," *Theory of Computing Systems*, vol. 40, no. 4, pp. 379–395, 2007.

[45] R. Paturi, "On the degree of polynomials that approximate symmetric Boolean functions (preliminary version)," in *Proceedings of the Twenty-fourth Annual ACM Symposium on Theory of Computing*, ser. STOC '92, 1992, pp. 468–474.

[46] M. Bun, R. Kothari, and J. Thaler, "The polynomial method strikes back: Tight quantum query bounds via dual polynomials," in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC 2018. ACM, 2018, pp. 297–310.

[47] A. Ambainis and A. Montanaro, "Quantum algorithms for search with wildcards and combinatorial group testing," *Quantum Information & Computation*, vol. 14, no. 5&6, pp. 439–453, Apr. 2014. [Online]. Available: http://dl.acm.org/citation.cfm?id=2638661.2638665