comput. complex. 23 (2014), 323 – 354
© Springer Basel 2014
1016-3328/14/020323-32
published online May 13, 2014
DOI 10.1007/s00037-014-0084-1

computational complexity

ON THE POWER OF NON-ADAPTIVE LEARNING GRAPHS

Aleksandrs Belovs and Ansis Rosmanis

Abstract. We introduce a notion of the quantum query complexity of a certificate structure. This is a formalization of a well-known observation that many quantum query algorithms only require the knowledge of the position of possible certificates in the input string, not the precise values therein.

Next, we derive a dual formulation of the complexity of a non-adaptive learning graph and use it to show that non-adaptive learning graphs are tight for all certificate structures. By this, we mean that there exists a function possessing the certificate structure such that a learning graph gives an optimal quantum query algorithm for it.

For a special case of certificate structures generated by certificates of bounded size, we construct a relatively general class of functions having this property. The construction is based on orthogonal arrays and generalizes the quantum query lower bound for the k-sum problem derived recently by Belovs and Špalek (Proceeding of 4th ACM ITCS, 323–328, 2012).

Finally, we use these results to show that the learning graph for the triangle problem by Lee et al. (Proceeding of 24th ACM-SIAM SODA, 1486–1502, 2013) is almost optimal in the above settings. This also gives a quantum query lower bound for the triangle sum problem.

Keywords. Quantum computing, query algorithms, adversary method, k-sum problem, triangle problem, semidefinite optimization.

Subject classification. 68Q12, 81P68.

Birkhäuser

1. Introduction

Determining the minimum amount of computational resources required to solve a computational problem is one of the main problems in theoretical computer science. At the current stage of knowledge, however, this task seems far out of reach for many problems. In this case, it is possible to analyze the complexity of the problem under some simplifying assumptions.

One such assumption is exhibited by the query model. In this model, it is assumed that all computational resources except accessing the input string are free of charge. (For a detailed description of the model, including our case of interest—quantum query complexity, refer to Buhrman & de Wolf 2002.) Under this assumption, it is possible to prove some tight bounds. In particular, a relatively simple semidefinite program (SDP) was constructed, yielding a tight estimate for the quantum query complexity of any function. This is the adversary bound which we describe in Section 4.1.

Unfortunately, for many functions, even this SDP is too hard to solve. In this paper, we investigate a possibility of constructing an even simpler optimization problem under further simplifying assumptions. Our assumptions are motivated by the class of algorithms based on quantum walks. A popular framework for the development of such algorithms (Magniez *et al.* 2011) includes a black-box *checking* subroutine that, given the information gathered during the walk, signals if this information is enough to accept the input string. In many cases, the precise content of the gathered information is not relevant for the implementation of the quantum walk, what matters are the possible locations of these pieces of information. We formalize this by the following definition.

In the definition, we use the following notation. If m and n are positive integers, we use $[n]$ to denote the set $\{1, 2, \ldots, n\}$ and $[m, n]$ to denote the set $\{m, m+1, \ldots, n\}$. Also, for a sequence $x = (x_i) \in [q]^n$ and $S \subseteq [n]$, let $x_S \in [q]^S$ denote the projection of x on S, i.e., the sequence $(x_{s_1}, \ldots, x_{s_\ell})$ indexed by the elements $s_1, \ldots, s_\ell$ of S.

Definition 1.1 (Certificate structure). *A certificate structure $\mathcal{C}$ on n variables is a collection of non-empty subsets of $2^{[n]}$ with each* *subset closed under taking supersets. We say a function $f\colon \mathcal{D} \to \{0,1\}$ with $\mathcal{D} \subseteq [q]^n$* has *certificate structure $\mathcal{C}$ if, for every $x \in f^{-1}(1)$, one can find $M \in \mathcal{C}$ such that*

$$\forall S \in M\ \forall z \in \mathcal{D}\colon z_S = x_S \Longrightarrow f(z) = 1.$$

For example, all functions on n variables satisfy the trivial certificate structure $\{\{[n]\}\}$.

We are interested in quantum algorithms that only depend on the certificate structure of a function. More formally, define the *quantum query complexity of a certificate structure* as the maximum quantum query complexity over all functions possessing this certificate structure.

The most celebrated examples of such algorithms are Grover's search algorithm (Grover 1996) and Ambainis's algorithm for element distinctness and k-distinctness (Ambainis 2007). As first noticed by Childs & Eisenberg (2005), Ambainis's algorithm can be applied to any function with 1-certificate complexity k. In our terms, it works for any function having the following certificate structure:

Definition 1.2. *The k*-subset certificate structure *$\mathcal{C}$ on n elements with $k = O(1)$ is defined as follows. It has $\binom{n}{k}$ elements, and, for each subset $A \subseteq [n]$ of size k, there exists a unique $M \in \mathcal{C}$ such that $S \in M$ if and only if $A \subseteq S \subseteq [n]$.*

In the same paper, Childs and Eisenberg also conjectured that Ambainis's algorithm is optimal for the k-sum problem. Our Theorem 1.6 below can be seen as a strong generalization of this conjecture.

A recently developed computation model of a (non-adaptive) learning graph (Belovs 2012a) relies on the certificate structure of the function by definition. This suggests to define the *learning graph complexity of a certificate structure* as the minimum complexity of a non-adaptive learning graph computing a function (hence, any function) with this certificate structure. Since a learning graph can be transformed into a quantum query algorithm with the same complexity, the learning graph complexity of a certificate structure is an upper bound on its quantum query complexity. In this paper, we prove that these two complexities are actually equal up to a constant factor.

THEOREM 1.3. *For any certificate structure, its quantum query and learning graph complexities differ by at most a constant multiplicative factor.*

This means that any quantum query algorithm that performs better than the best learning graph has to take the values of the variables into account on the earlier stages of the algorithm. Although Theorem 1.3 is a very general result, it is unsatisfactory in the sense that the function having the required quantum query complexity is rather artificial, and the size of the alphabet is astronomical. However, for a special case of certificates structures we are about to define, it is possible to construct a relatively natural problem with a modestly sized alphabet having high quantum query complexity.

DEFINITION 1.4 (Boundedly generated certificate structure). *A certificate structure $\mathcal{C}$ is* boundedly generated *if, for any $M \in \mathcal{C}$, one can find a subset $A_M \subseteq [n]$ such that $|A_M| = O(1)$, and $S \in M$ if and only if $S \supseteq A_M$.*

DEFINITION 1.5 (Orthogonal array). *Assume T is a subset of $[q]^k$. We say that T is an* orthogonal array *over alphabet $[q]$ if, for every index $i \in [k]$ and for every sequence $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$ of elements in $[q]$, there exist exactly $|T|/q^{k-1}$ choices of $x_i \in [q]$ such that $(x_1, \ldots, x_k) \in T$. We call $|T|$ the* size *of the array, and k its* length.

Compared to a standard definition of orthogonal arrays (cf. Hedayat *et al.* 1999), we always require that the so-called strength of the array equals $k - 1$.

THEOREM 1.6. *Assume a certificate structure $\mathcal{C}$ is boundedly generated, and let A_M be like in Definition 1.4. Assume the alphabet is $[q]$ for some $q \geq 2|\mathcal{C}|$, and each A_M is equipped with an orthogonal array T_M over alphabet $[q]$ of length $|A_M|$ and size $q^{|A_M|-1}$.*

Consider a function $f\colon [q]^n \to \{0,1\}$ *defined by* $f(x) = 1$ *iff there exists* $M \in \mathcal{C}$ *such that* $x_{A_M} \in T_M$. *Then, the quantum query complexity of* f *is at least a constant times the learning graph complexity of* $\mathcal{C}$.

For example, for a boundedly generated certificate structure $\mathcal{C}$, one can define a corresponding *sum* problem: Given $x \in [q]^n$, detect whether there exists $M \in \mathcal{C}$ such that $\sum_{j\in A_M} x_j \equiv 0 \pmod q$. If $q \geq 2|\mathcal{C}|$, Theorem 1.6 implies that the quantum query complexity of this problem is at least a constant times the learning graph complexity of $\mathcal{C}$.

Theorem 1.6 is a generalization of the lower bound for the k-sum problem from Belovs & Špalek (2012) and provides additional intuition on the construction, by linking it to learning graphs. Much of the discussion in Belovs & Špalek (2012) applies here as well.

Let us give some more examples. Another (besides Ambainis's algorithm) well-known quantum walk-based algorithm (Magniez *et al.* 2007) (implicitly) solves any function with the following certificate structure:

Definition 1.7. *The* triangle certificate structure $\mathcal{C}$ *on* n *vertices is a certificate structure on* $\binom{n}{2}$ *variables defined as follows. Assume that the variables are labeled as* x_{ij} *where* $1 \leq i < j \leq n$. *The certificate structure has* $\binom{n}{3}$ *elements, and, for every triple* $1 \leq a < b < c \leq n$, *there exists unique* $M \in \mathcal{C}$ *such that* $S \in M$ *if and only if* $S \supseteq \{ab, bc, ac\}$. *(Note that for this certificate structure, the letter* n *that customary denotes the number of input variables, is used to denote the number of vertices. This is a standard notation, and we hope it will not cause much confusion.)*

Originally, the algorithm in Magniez *et al.* (2007) dealt with the *triangle problem*: All x_{ij} are Boolean, and the condition on $f(x) = 1$ is that $x_{ab} = x_{ac} = x_{bc} = 1$ for some M. The quantum walk algorithm for this certificate structure was lately superseded by an algorithm based on learning graphs (Lee *et al.* 2013). We will show in Section 3 that this learning graph is essentially optimal.

Both the k-subset and the triangle certificate structures are boundedly generated. We also consider some certificate structures that are not. Recall the *collision problem* (Brassard *et al.* 1998).

Given an input string $x \in [q]^{2n}$, the task is to distinguish two cases. In the negative case, all input variables are distinct. In the positive case, there exists a decomposition of the input variables $[2n] = \{a_1, b_1\} \sqcup \{a_2, b_2\} \sqcup \cdots \sqcup \{a_n, b_n\}$ into n pairs such that $x_{a_i} = x_{b_i}$ for all $i \in [n]$, but $x_{a_i} \neq x_{a_j}$ for all $i \neq j$. The *set equality problem* is defined similarly, with an additional promise that, in the positive case, $a_i \in [n]$ and $b_i \in [n+1, 2n]$ for all i. Finally, the *hidden shift problem* is defined like the set equality problem with an additional promise that, in the positive case, there exists $d \in [n]$ such that $b_i = n + 1 + ((a_i + d) \bmod n)$ for all $i \in [n]$. Inspired by these problems, we define the following certificate structures.

DEFINITION 1.8. *Each of the following certificate structures is defined on $2n$ input variables. In the* collision certificate structure, *there is unique M for each decomposition $[2n] = \{a_1, b_1\} \sqcup \{a_2, b_2\} \sqcup \cdots \sqcup \{a_n, b_n\}$, and $S \in M$ if and only if $S \supseteq \{a_i, b_i\}$ for some $i \in [n]$. The* set equality certificate structure *contains only those M from the collision certificate structure that correspond to decompositions with $a_i \in [n]$ and $b_i \in [n+1, 2n]$ for all i. Finally, the* hidden shift certificate structure *contains only those M from the set equality certificate structure that correspond to decompositions such that $d \in [n]$ exists with the property $b_i = n + 1 + ((a_i + d) \bmod n)$ for all $i \in [n]$.*

All certificates structures from Definition 1.8 are not boundedly generated. The algorithm for the collision problem from Brassard *et al.* (1998) actually solves any function possessing the collision certificate structure in $O(n^{1/3})$ quantum queries, and it is tight (Aaronson & Shi 2004). Clearly, the same algorithm is applicable for the set equality and hidden shift certificate structures. The situation with the hidden shift problem is more interesting. This problem reduces to the hidden subgroup problem in the dihedral group (Kuperberg 2005), and the latter has logarithmic query complexity (Ettinger *et al.* 2004). Unlike other algorithms in this section, the latter one is not, in general, applicable to any function with the hidden shift certificate structure.

Let us briefly describe organization of the paper. In Section 2, we define the complexity of a learning graph and derive its dual formulation of the complexity of a non-adaptive learning graph. In Section 3, we apply this dual formulation to give lower bounds on the learning graph complexity of the certificate structures from the introduction. We demonstrate that transition to the learning graph complexity indeed simplifies the problem by obtaining an almost optimal $\widetilde{\Omega}(n^{9/7})$ lower bound for the triangle certificate structure, whereas nothing better than trivial $\Omega(n)$ is known for the original triangle problem. Finally, in Section 4, we prove both Theorems 1.3 and 1.6.

2. Learning graph complexity

In this section, we recall the definition of a non-adaptive learning graph from Belovs (2012a) and derive its dual formulation. Non-adaptive learning graphs were used to construct best known quantum query algorithms for triangle and other subgraph detection (Lee *et al.* 2011a, 2013; Zhu 2012) and associativity testing (Lee *et al.* 2013). Although more general versions of learning graphs were used for k-distinctness (Belovs 2012b; Belovs & Lee 2011) and graph collision (Gavinsky & Ito 2012), the non-adaptive version is much easier to apply. This makes it important to understand its limitations.

Let $\mathcal{E}$ by the set of pairs (S, S') of subsets of $[n]$ such that $S' = S \cup \{j\}$ for some $j \notin S$. This set is known as the *set of arcs* of a learning graph on n variables. For $e = (S, S') \in \mathcal{E}$, let $\mathrm{s}(e) = S$ and $\mathrm{t}(e) = S'$.

Definition 2.1. *The learning graph complexity of a certificate structure $\mathcal{C}$ on n variables is equal to the optimal value of the following two optimization problems*

$$\text{(2.2a)} \qquad \text{minimize} \qquad \sqrt{\sum\nolimits_{e\in\mathcal{E}} w_e}$$

$$\text{(2.2b)} \qquad \text{subject to} \qquad \sum\nolimits_{e\in\mathcal{E}} \frac{p_e(M)^2}{w_e} \le 1 \qquad \text{for all } M \in \mathcal{C};$$

$$\text{(2.2c)} \qquad \sum_{e\in\mathcal{E}\colon \mathrm{t}(e)=S} p_e(M) = \sum_{e\in\mathcal{E}\colon \mathrm{s}(e)=S} p_e(M)$$

$$\text{for all } M\in\mathcal{C} \text{ and } S\in 2^{[n]}\setminus(M\cup\{\emptyset\});$$

$$\text{(2.2d)} \qquad \sum\nolimits_{e\in\mathcal{E}\colon \mathrm{s}(e)=\emptyset} p_e(M) = 1 \qquad \text{for all } M\in\mathcal{C};$$

$$\text{(2.2e)} \qquad p_e(M)\in\mathbb{R}, \quad w_e\ge 0 \qquad \text{for all } e\in\mathcal{E} \text{ and } M\in\mathcal{C}.$$

(here, $0/0$ *in (2.2b) is defined to be* 0*), and*

$$\text{(2.3a)} \qquad \text{maximize} \qquad \sqrt{\sum\nolimits_{M\in\mathcal{C}} \alpha_\emptyset(M)^2}$$

$$\text{(2.3b)} \qquad \text{subject to} \qquad \sum\nolimits_{M\in\mathcal{C}} \bigl(\alpha_{\mathrm{s}(e)}(M)-\alpha_{\mathrm{t}(e)}(M)\bigr)^2 \le 1$$

$$\text{for all } e\in\mathcal{E};$$

$$\text{(2.3c)} \qquad \alpha_S(M)=0 \qquad \text{whenever } S\in M;$$

$$\text{(2.3d)} \qquad \alpha_S(M)\in\mathbb{R} \qquad \text{for all } S\subseteq[n] \text{ and } M\in\mathcal{C}.$$

Equation (2.2) is a trivial restatement of the definition of a non-adaptive learning graph from Belovs (2012a). The second expression (2.3) is new and requires a proof that we will give shortly.

The relation of this construction to quantum algorithms is as follows:

Theorem 2.4 (Belovs 2012a; Belovs & Lee 2011). *The quantum query complexity of a certificate structure is at most a constant times its learning graph complexity.*

In Section 4, we prove the reverse statement for all certificate structures.

Proof (of the equivalence of (2.2) and (2.3)). The equivalence is obtained by duality. We use basic convex duality (Boyd & Vandenberghe 2004, Chapter 5). First of all, we consider both programs with their objective values (2.2a) and (2.3a) squared. With this change, (2.2) becomes a convex program (in fact, an SDP; for the convexity of (2.2b), see Section 3.1.5 of Boyd & Vandenberghe (2004)). The program is strictly feasible. Indeed, it is easy to see that (2.2c) and (2.2d) are feasible. To assure strict feasibility in (2.2b), it is enough to take w_e large enough. Hence, by Slater's condition, the optimal values of (2.2) and its dual are equal. Let us calculate the dual. The Lagrangian of (2.2) is as follows

$$\begin{aligned}\sum_{e\in\mathcal{E}} w_e + \sum_{M\in\mathcal{C}} \mu_M \Bigl(\sum_{e\in\mathcal{E}} \frac{p_e(M)^2}{w_e} - 1\Bigr) \\ + \sum_{\substack{M\in\mathcal{C},\, S\subseteq[n]\\ S\neq\emptyset,\, S\notin M}} \nu_{M,S}\Bigl(\sum_{\substack{e\in\mathcal{E}\\ \mathrm{t}(e)=S}} p_e(M) - \sum_{\substack{e\in\mathcal{E}\\ \mathrm{s}(e)=S}} p_e(M)\Bigr) \\ + \sum_{M\in\mathcal{C}} \nu_{M,\emptyset}\Bigl(1 - \sum_{\substack{e\in\mathcal{E}\\ \mathrm{s}(e)=\emptyset}} p_e(M)\Bigr). \qquad (2.5)\end{aligned}$$

Here, $\mu_M \geq 0$, and $\nu_{M,S}$ are arbitrary. Let us first minimize over $p_e(M)$. Each $p_e(M)$ appears three times in (2.5) with the following coefficients:

$$p_e(M)^2 \frac{\mu_M}{w_e} + p_e(M)\bigl(\nu_{M,\mathrm{t}(e)} - \nu_{M,\mathrm{s}(e)}\bigr),$$

where we assume $\nu_{M,S} = 0$ for all $S \in M$. The minimum of this expression clearly is

$$-\frac{w_e}{4\mu_M}\bigl(\nu_{M,\mathrm{t}(e)} - \nu_{M,\mathrm{s}(e)}\bigr)^2.$$

Plugging this into (2.5) yields

$$\sum_{M\in\mathcal{C}} (\nu_{M,\emptyset} - \mu_M) + \sum_{e\in\mathcal{E}} w_e \Bigl(1 - \sum_{M\in\mathcal{C}} \frac{\bigl(\nu_{M,\mathrm{t}(e)} - \nu_{M,\mathrm{s}(e)}\bigr)^2}{4\mu_M}\Bigr). \qquad (2.6)$$

Define $\alpha_S(M)$ as $\nu_{M,S}/(2\sqrt{\mu_M})$. Minimizing (2.6) over w_e, the second term disappears if condition (2.3b) is satisfied. The first term is

$$\sum_{M\in\mathcal{C}} (2\sqrt{\mu_M}\alpha_\emptyset(M) - \mu_M).$$

We can also maximize over μ_M that gives the square of (2.3a). □

3. Examples of application

In this section, we construct feasible solutions to the dual formulation of the learning graph complexity (2.3) for the certificate structures from Section 1. Their objective values match the objective values of feasible solutions to the corresponding primal formulations (2.2) that were obtained previously.

Proposition 3.1. *The learning graph complexity (and, hence, the quantum query complexity) of the k-subset certificate structure is $\Omega(n^{k/(k+1)})$.*

Proof. Let $\mathcal{C}$ be the k-subset certificate structure, and $\alpha_S(M)$ be defined by

$$\binom{n}{k}^{-1/2} \max\left\{n^{k/(k+1)} - |S|,\ 0\right\}$$

if $S \notin M$, and as 0 otherwise.

Let us prove that (2.3b) holds up to a constant factor. Take any $S \subset [n]$ and let j be any element not in S. If $|S| \geq n^{k/(k+1)}$, then $\alpha_S(M) = \alpha_{S\cup\{j\}}(M) = 0$, and we are done. Thus, we further assume $|S| < n^{k/(k+1)}$. There are $\binom{n}{k}$ choices of M. If $S \cup \{j\} \notin M$, then the value of $\alpha_S(M)$ changes by $\binom{n}{k}^{-1/2}$ as the size of $|S|$ increases by 1. Also, there are at most $\binom{|S|}{k-1} \leq n^{k(k-1)/(k+1)}$ choices of $M \in \mathcal{C}$ such that $S \notin M$ and $S \cup \{j\} \in M$. For each of them, the value of $\alpha_S(M)$ changes by at most $\binom{n}{k}^{-1/2} n^{k/(k+1)}$. Thus,

$$\sum_{M\in\mathcal{C}} (\alpha_S(M) - \alpha_{S\cup\{j\}}(M))^2 \\ \leq \binom{n}{k}^{-1} \left[\binom{n}{k} \cdot 1 + n^{k(k-1)/(k+1)} n^{2k/(k+1)}\right] = O(1).$$

On the other hand, for the objective value (2.3a), we have

$$\sqrt{\sum_{M\in\mathcal{C}} \alpha_\emptyset(M)^2} = n^{k/(k+1)}.$$

By scaling all $\alpha_S(M)$ down by an appropriate constant factor, we obtain a feasible solution to (2.3) with the objective value $\Omega(n^{k/(k+1)})$. □

Belovs & Lee (2011) and Zhu (2012) show that the corresponding upper bound is $O(n^{k/(k+1)})$, thus the result of Proposition 3.1 is tight. Moreover, Theorem 1.6 implies that the complexity of the k-sum problem is $\Theta(n^{k/(k+1)})$, a result previously proven in Belovs & Špalek (2012).

Proposition 3.2. *The learning graph complexity of the hidden shift (and, hence, the set equality and the collision) certificate structure is* $\Omega(n^{1/3})$.

Proof. The proof is similar to the proof of Proposition 3.1. Let $\mathcal{C}$ be the hidden shift certificate structure. Define $\alpha_M(S)$ as $n^{-1/2}\max\{n^{1/3} - |S|, 0\}$ if $S \notin M$, and as 0 otherwise. Take any $S \subset [n]$, $j \notin S$, and let us prove (2.3b). Again, if $|S| \geq n^{1/3}$, we are done. Otherwise, there are n choices of M in total, and at most $n^{1/3}$ of them are such that $S \notin M$ and $S \cup \{j\} \in M$. Thus,

$$\sum_{M\in\mathcal{C}} (\alpha_S(M) - \alpha_{S\cup\{j\}}(M))^2 \leq \frac{1}{n}\left[n \cdot 1 + n^{1/3}n^{2/3}\right] = O(1).$$

The objective value (2.3a) is $n^{1/3}$. For the set equality and collision certificate structures, just assign $\alpha_S(M) = 0$ for all M that are not in the hidden shift certificate structure. □

The result of this proposition is also tight. The corresponding upper bound can be derived by similar methods as used for the k-sum problem in Belovs & Lee (2011) and Zhu (2012). We omit the precise construction.

Proposition 3.3. *The learning graph (and the quantum query) complexity of the triangle certificate structure is* $\Omega(n^{9/7}/\sqrt{\log n})$.

The best known upper bound is $O(n^{9/7})$ as proven in (Lee *et al.* 2013). The proof of the lower bound is rather bulky and essentially proceeds by showing, in a formal way, that all possible strategies of constructing a better upper bound fail.

Proof (Proof of Proposition 3.3). Let $E = \{uv \mid 1 \le u < v \le n\}$ be the set of input variables (potential edges of the graph). Let $\mathcal{C}$ be the triangle certificate structure. We will construct a feasible solution to (2.3) (with $[n]$ replaced by E) in the form

$$\alpha_S(M) = \max\Bigl\{n^{-3/14} - \sum_{i=0}^{k} g_i(S,M),\ 0\Bigr\} \tag{3.4}$$

if $S \notin M$, and $\alpha_S(M) = 0$ otherwise. Here, $g_i(S,M)$ is a function satisfying $0 \le g_i(S,M) \le n^{-3/14}$ and $g_i(\emptyset, M) = 0$. The value of (2.3a) is $\sqrt{\binom{n}{3}}\ n^{-3/14} = \Omega(n^{9/7})$. The hard part is to show that (2.3b) holds up to logarithmic factors.

We define

$$g_0(S,M) = \min\{n^{-3/2}|S|, n^{-3/14}\}.$$

This forces $\alpha_S(M) = 0$ if $|S| \ge n^{9/7}$. Hence, we may further assume $|S| \le n^{9/7}$.

For $S \subset E$ and $j \in E \setminus S$, let $F(S,j)$ denote the set of $M \in \mathcal{C}$ such that $S \notin M$, but $S \cup \{j\} \in M$. We have

$$\sum_{M\in\mathcal{C}} (\alpha_S(M) - \alpha_{S\cup\{j\}}(M))^2 \tag{3.5}$$

$$\le \sum_{M\in F(S,j)} \Bigl(\max\Bigl\{n^{-3/14} - \sum_{i=0}^{k} g_i(S,M),\ 0\Bigr\}\Bigr)^2 \tag{3.6}$$

$$+ \sum_{M\in\mathcal{C}\setminus F(S,j)} \Bigl(\sum_{i=0}^{k} (g_i(S,M) - g_i(S\cup\{j\},M))\Bigr)^2. \tag{3.7}$$

We estimate two terms of (3.5) separately. In order to estimate the first one, we decompose $F(S,j)$ into a disjoint union $F_1(S,j) \sqcup \cdots \sqcup F_k(S,j)$ of $k = O(\log n)$ subsets so that $g_i(S,M)$ is large for all $M \in F_i(S,j)$, or, more precisely,

$$\sum_{M\in F_i(S,j)} \bigl(n^{-3/14} - g_i(S,M)\bigr)^2 = O(1). \tag{3.8}$$

Hence, the first term of (3.5) is $O(\log n)$. For the second term, we show that for all, except $O(1)$, values of $i \in [0,k]$, we have

$g_i(S, M) = g_i(S \cup \{j\}, M)$ for all $M \in \mathcal{C} \setminus F(S, j)$, and, for the remaining values of i,

$$\sum_{M \in \mathcal{C} \setminus F(S,j)} \bigl(g_i(S, M) - g_i(S \cup \{j\}, M)\bigr)^2 = O(1). \tag{3.9}$$

(In particular, it is not hard to see that g_0 satisfies (3.9).) Hence, the second term of (3.5) is $O(1)$. By scaling all $\alpha_S(M)$ down by a factor of $O(\sqrt{\log n})$, we obtain a feasible solution to (2.3) with the objective value $\Omega(n^{9/7}/\sqrt{\log n})$.

Let us now define $F_i(S, j)$. For each $M \in \mathcal{C}$ fix three vertices $a = a(M), b = b(M), c = c(M)$ forming the triangle, i.e., such that $S \in M$ if and only if $ab, ac, bc \in S$. An input index $j \in E$ satisfies $S \notin M$ and $S \cup \{j\} \in M$ only if $j \in \{ab, ac, bc\}$. We specify to which of $F_i(S, j)$ an element $M \in F(S, j)$ belongs by the following criteria:

- to which of the three possible edges, ab, ac or bc, the new edge j is equal, and
- the range to which the degree in S of the third vertex of the triangle belongs: $[0, n^{3/7}]$, $[n^{3/7}, 2n^{3/7}]$, $[2n^{3/7}, 4n^{3/7}]$, $\ldots$, $[2^i n^{3/7}, 2^{i+1} n^{3/7}]$, $\ldots$

Hence, $k \approx 12/7 \log_2 n$. (We need the labeling of vertices here because we want to prepare in advance for all possible sequences of loading the edges of the triangle.) For notational convenience, let $j = bc$. Then, the second property is determined by $\deg a = \deg_S a$, the degree of a in the graph with edge set S.

It remains to define the functions $g_i(S, M)$. In the following, let $\mu(x)$ be the median of 0, x, and 1, i.e., $\mu(x) = \max\{0, \min\{x, 1\}\}$. The first interval of $\deg a$ will be considered separately from the rest.

First interval. Let us define

$$g_i(S, M) = \begin{cases} n^{-3/14}\, \mu(2 - n^{-3/7} \deg a), & ab, ac \in S; \\ 0, & \text{otherwise.} \end{cases} \tag{3.10}$$

Clearly, g_i satisfies (3.8) for the case when $\deg a \leq n^{3/7}$. Let us prove (3.9). There are two possibilities how $g_i(S, M)$ can be influenced when the element j is added to S:

- It may happen if $|\{ab, ac\} \cap S| = 1$ and $j \in \{ab, ac\}$, i.e., the transition from the second case of (3.10) to the first one happens. Moreover, $g_1(S, M)$ changes only if $\deg a \leq 2n^{3/7}$. Then j identifies two vertices of the triangle, and the third one is among the neighbors of an end point of j having degree at most $2n^{3/7}$. Thus, the total number of M satisfying this scenario is at most $4n^{3/7}$. The contribution to (3.9) is at most $O(n^{3/7})(n^{-3/14})^2 = O(1)$.
- Another possibility is that $ab, ac \in S$ and $\deg a$ changes. In this case, a is determined as an end point of j, and b and c are among its at most $2n^{3/7}$ neighbors. The number of M influenced is $O(n^{6/7})$, and the contribution is $O(n^{6/7})(n^{-9/14})^2 = o(1)$.

Other intervals Now we consider an interval $d < \deg a \leq 2d$ with $d \geq n^{3/7}$. Define a piece-wise linear function τ as follows

$$\tau(x) = \begin{cases} 0, & x < d/2; \\ (2x-d)/d, & d/2 \leq x < d; \\ 1, & d \leq x < 2d; \\ (5d-2x)/d, & 2d \leq x \leq 5d/2; \\ 0, & x \geq 5d/2. \end{cases}$$

It can be interpreted as a continuous version of the indicator function that a vertex has the right degree. Define

$$\nu(S, M) = \sum_{v \in N(b) \cap N(c)} \tau(\deg v),$$

where the sum is over the common neighbors of b and c. Let

$$g_i(S, M) = n^{-3/14}\,\mu\Big(\min\Big\{\frac{2\deg a}{d},\ \frac{\nu(S, M)}{n^{3/7}}\Big\} - 1\Big).$$

Let us check that this function satisfies (3.8). We know that $\deg a \geq d$, hence, either $n^{-3/14} - g_i(S, M) = 0$ or $\nu(S, M) \leq 2n^{3/7}$, in which case, there are $O(n^{3/7})$ choices of a satisfying the constraint $d \leq \deg a \leq 2d$. Hence, the left hand side of (3.8) is $O(n^{3/7})(n^{-3/14})^2 = O(1)$.

Let us prove (3.9). There are three possibilities how $g_i(S, M)$ may be influenced when j is added:

- It may happen that j is incident to a common neighbor of b and c, and $\nu(S, M)$ changes. This means that b and c are among the neighbors of an end point of j of degree at most $5d/2$. As a can be arbitrary, this affects $O(nd^2)$ different M. The contribution to (3.9) is $O(nd^2)(n^{-9/14}/d)^2 = o(1)$.
- The set $N(b) \cap N(c)$ may increase. This causes a change in $g_i(S, M)$ only under the following circumstances. The new edge j is incident to b or c. The second vertex in $\{b, c\}$ is among $\Theta(d)$ neighbors of the second end point of j. Finally, $\deg a \geq d/2$ that together with $|S| \leq n^{9/7}$ implies that there are $O(n^{9/7}/d)$ choices for a. Altogether, the number of M affected by this is $O(n^{9/7})$, and the change in $g_i(S, M)$ does not exceed $n^{-9/14}$. The contribution is $O(1)$.
- The degree of a may change. Let us calculate the number P of possible pairs b and c affected by this. Let A denote the set of vertices having degrees between $d/2$ and $5d/2$ in S. There is a change in $g_i(S, M)$ only if b and c are connected to at least $n^{3/7}$ vertices in A, so we will count only those M that satisfy this condition. Since $|S| \leq n^{9/7}$, we have $|A| = O(n^{9/7}/d)$.

  Let us calculate the number of paths of length 2 in S having the middle vertex in A. On the one hand, this number is at least $Pn^{3/7}$. On the other hand, it is at most $O(d^2|A|) = O(dn^{9/7})$. Thus, $P = O(dn^{6/7})$. Since a is determined as an end point of j, the contribution is $O(dn^{6/7})(n^{-3/14}/d)^2 = O(1)$, as $d \geq n^{3/7}$.

If $g_i(S, M) \neq g_i(S \cup \{j\}, M)$, then the value of d, up to a small ambiguity, may be determined from the degree of one of the end points of j; hence, there are $O(1)$ choices of i satisfying $g_i(S, M) \neq g_i(S \cup \{j\}, M)$ for some M. □

Automatically, we obtain that the quantum query complexity of the *triangle sum* problem is $\widetilde{\Omega}(n^{9/7})$. Thus, any quantum query algorithm, willing to improve the $O(n^{9/7})$ bound for the triangle detection problem, will have to take differences between the triangle detection and triangle sum problems into consideration.

4. Lower bound

In this section, we prove Theorems 1.3 and 1.6. The results are strongly connected: In the second one, we prove a stronger statement from stronger premises. As a consequence, the proofs also have many common elements.

This section is organized as follows. In Section 4.1, we recall the adversary method that we use to prove the lower bound. In the proofs, we will define a number of matrices and argue about their spectral properties. For convenience, we describe the main parameters of the matrices, such as the labeling of their rows and columns, as well as their mutual relationships in one place, Section 4.2. In Section 4.3, we state the intermediate results important to both Theorems 1.3 and 1.6. In Section 4.4, we finish the proof of Theorem 1.6. In Section 4.5, we recall the definition and main properties of the Fourier basis and define the important notion of the Fourier bias. Finally, in Section 4.6, we prove Theorem 1.3.

4.1. Adversary bound. The adversary method is one of the main techniques for proving lower bounds on quantum query complexity. At first, it was developed by Ambainis (2002) in what later became known as the nonnegative-weight variant of the bound. This version of the bound is widely used because of its intuitive combinatorial formulation. Unfortunately, it has several limitations. In particular, the so-called certificate complexity barrier (Špalek & Szegedy 2006; Zhang 2005) implies that the nonnegative version of the adversary bound fails to prove a better lower bound than $O(\sqrt{n})$ for any function possessing a boundedly generated certificate structure. This renders this version of the bound totally useless for our purposes.

Luckily, a stronger variant of the adversary bound was obtained by Høyer *et al.* (2007). It is the general or negative-weight version of the bound. After that, the adversary bound was proven to be optimal (Lee *et al.* 2011b; Reichardt 2011). Although being more powerful, this version of the bound is much less intuitive, which explains why it has almost never been used previously. Below, we use a variation in the negative-weight adversary bound from Belovs & Špalek (2012).

Definition 4.1. *Let f be a function $f\colon \mathcal{D} \to \{0,1\}$ with domain $\mathcal{D} \subseteq [q]^n$. Let $\widetilde{\mathcal{D}}$ be a set of pairs (x,a) with the property that the first element of each pair belongs to $\mathcal{D}$. (The second element may be arbitrary: Its only purpose is to distinguish pairs with the same first element.) Let also $\widetilde{\mathcal{D}}_i = \{(x,a) \in \widetilde{\mathcal{D}} \mid f(x) = i\}$ for $i \in \{0,1\}$. An* adversary matrix *for the function f is a nonzero real $\widetilde{\mathcal{D}}_1 \times \widetilde{\mathcal{D}}_0$ matrix Γ. And, for $j \in [n]$, let Δ_j denote the $\widetilde{\mathcal{D}}_1 \times \widetilde{\mathcal{D}}_0$ matrix defined by*

$$\Delta_j[\![(x,a),(y,b)]\!] = \begin{cases} 0, & x_j = y_j; \\ 1, & \textit{otherwise.} \end{cases}$$

Theorem 4.2 (Adversary bound, Belovs & Špalek 2012; Høyer *et al.* 2007). *In the notation of Definition 4.1, the quantum query complexity of f is $\Omega(\mathrm{Adv}(f))$, where*

$$\mathrm{Adv}(f) = \sup_{\Gamma} \frac{\|\Gamma\|}{\max_{j\in n} \|\Gamma \circ \Delta_j\|} \tag{4.3}$$

with the maximization over all adversary matrices for f, $\|\cdot\|$ is the spectral norm, and $\circ$ is the entrywise matrix product.

The following result is very useful when proving lower bounds using the adversary method.

Lemma 4.4 (Lee *et al.* 2011b). *Let Δ_j be as in Definition 4.1. Then, for any matrix A of the same size,*

$$\|A \circ \Delta_j\| \le 2\,\|A\|\,.$$

We will use it to replace $\Gamma \circ \Delta_j$ in the denominator of (4.3) with a matrix Γ' such that $\Gamma \circ \Delta_j = \Gamma' \circ \Delta_j$. By Lemma 4.4, this gives the same result up to a factor of 2. We will denote this relation between matrices by $\Gamma \xmapsto{\Delta_j} \Gamma'$.

4.2. Outline. Let us now outline how Theorems 1.3 and 1.6 are proven. Let $\mathcal{C}$ denote the certificate structure. Let $\alpha_S(M)$ satisfy (2.3) and be such that (2.3a) equals the learning graph complexity of $\mathcal{C}$. We define an explicit function $f\colon \mathcal{D} \to \{0,1\}$ with $\mathcal{D} \subseteq [q]^n$ having the objective value (2.3a) of program (2.3) as a lower bound on its quantum query complexity. The latter is proven using the adversary bound, Theorem 4.2.

Function. Let M be an element of the certificate structure $\mathcal{C}$. Let $A_M^{(1)}, \dots, A_M^{(\ell(M))}$ be all the inclusion-wise minimal elements of M. (In a boundedly generated certificate structure, M has only one inclusion-wise minimal element A_M.) For each $A_M^{(i)}$, we choose an orthogonal array $T_M^{(i)}$ of length $|A_M^{(i)}|$ over the alphabet $[q]$ and define

$$X_M = \left\{ x \in [q]^n \mid x_{A_M^{(i)}} \in T_M^{(i)} \text{ for all } i \in [\ell(M)] \right\}. \tag{4.5}$$

The orthogonal arrays are chosen so that X_M is non-empty and satisfies the following *orthogonality property*:

$$\forall S \in 2^{[n]} \setminus M \ \ \forall z \in [q]^S \ : \ \bigl|\{x \in X_M \mid x_S = z\}\bigr| = |X_M|/q^{|S|}. \tag{4.6}$$

For boundedly generated certificate structures, this property is satisfied automatically.

The set of positive inputs is defined by $f^{-1}(1) = \bigcup_{M\in\mathcal{C}} X_M$. The set of negative inputs $Y = f^{-1}(0)$ is defined by

$$Y = \left\{ x \in [q]^n \mid x_{A_M^{(i)}} \notin T_M^{(i)} \text{ for all } M \in \mathcal{C} \text{ and } i \in [\ell(M)] \right\}. \tag{4.7}$$

It is easy to see that f has $\mathcal{C}$ as its certificate structure. The parameters will be chosen so that $|f^{-1}(0)| = \Omega(q^n)$.

Matrices. We define a number of matrices whose mutual relations are shown in Figure 4.1. At first, we construct a matrix $\widetilde{\Gamma}$ satisfying the following properties. Firstly, it has rows labeled by the elements of $[q]^n \times \mathcal{C}$ and columns labeled by the elements of

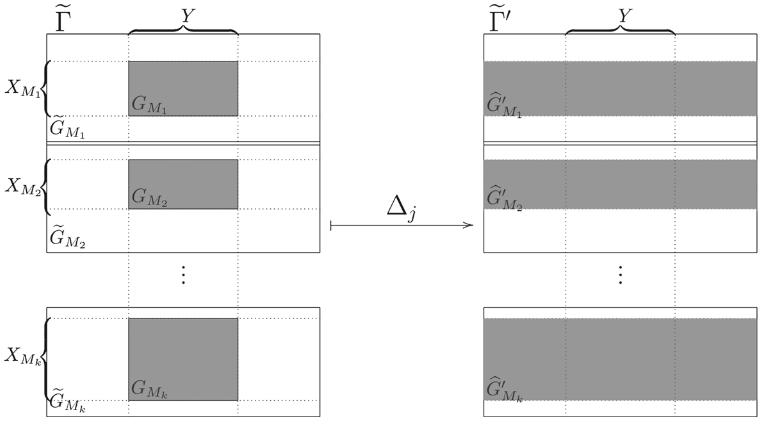

Figure 4.1: The relationships between matrices used in Section 4. The parts marked in gray form the matrix Γ on the left and $\widehat{\Gamma}'$ on the right. Note that they are *not* submatrices of $\widetilde{\Gamma}$ and $\widetilde{\Gamma}'$, respectively: They have additional multiplicative factor as specified in (4.9) and (4.10).

$[q]^n$. Thus, if we denote $\mathcal{C} = \{M_1, \ldots, M_k\}$, the matrix $\widetilde{\Gamma}$ has the following form

$$\widetilde{\Gamma} = \begin{pmatrix} \widetilde{G}_{M_1} \\ \widetilde{G}_{M_2} \\ \vdots \\ \widetilde{G}_{M_k} \end{pmatrix}, \tag{4.8}$$

where each $\widetilde{G}_{M_i}$ is an $[q]^n \times [q]^n$-matrix. Next, $\|\widetilde{\Gamma}\|$ is at least the objective value (2.3a). And finally, for each $j \in [n]$, there exists $\widetilde{\Gamma}'$ such that $\widetilde{\Gamma} \xmapsto{\Delta_j} \widetilde{\Gamma}'$ and $\|\widetilde{\Gamma}'\| \leq 1$. The matrix $\widetilde{\Gamma}'$ has a decomposition into blocks $\widetilde{G}'_M$ similar to (4.8).

Thus, $\widetilde{\Gamma}$ has a good value of (4.3). But, we cannot use it, because it is not an adversary matrix: It uses all possible inputs as labels of both rows and columns. However, due to the specific way $\widetilde{\Gamma}$ is constructed, we will be able to transform $\widetilde{\Gamma}$ into a true adversary matrix Γ such that the value of (4.3) is still good.

Let us define $X = \{(x, M) \in [q]^n \times \mathcal{C} \mid x \in X_M\}$. Also, as mentioned previously, $Y = f^{-1}(0)$. The matrix Γ is an $X \times Y$

matrix defined by

$$\Gamma[\![(x,M),y]\!] = \sqrt{\frac{q^n}{|X_M|}}\,\widetilde{\Gamma}[\![(x,M),y]\!]. \tag{4.9}$$

Thus, Γ consists of blocks G_M, like in (4.8), where

$$G_M = \sqrt{q^n/|X_M|}\,\widetilde{G}_M[\![X_M, Y]\!].$$

(The latter notation stands for the submatrix formed by the specified rows and columns). We also show that $\|\Gamma\|$ is not much smaller than $\|\widetilde{\Gamma}\|$.

The matrix Γ' is obtained similarly from $\widetilde{\Gamma}'$. It is clear that $\widetilde{\Gamma} \xmapsto{\Delta_j} \widetilde{\Gamma}'$ implies $\Gamma \xmapsto{\Delta_j} \Gamma'$. We show that the norm of Γ' is small by showing that $\|\widehat{\Gamma}'\| = O(\|\widetilde{\Gamma}'\|)$ where $\widehat{\Gamma}'$ is an $X \times [q]^n$-matrix with

$$\widehat{\Gamma}'[\![(x,M),y]\!] = \sqrt{\frac{q^n}{|X_M|}}\,\widetilde{\Gamma}'[\![(x,M),y]\!].$$

As Γ' is a submatrix of $\widehat{\Gamma}'$ and $\|\widetilde{\Gamma}'\| \le 1$, we obtain that $\|\Gamma'\| = O(1)$ as required. We denote the blocks of $\widehat{\Gamma}'$ by $\widehat{G}'_M$. That is,

$$\widehat{G}'_M = \sqrt{\frac{q^n}{|X_M|}}\,\widetilde{G}'_M[\![X_M, [q]^n]\!]. \tag{4.10}$$

4.3. Common Parts of the Proofs. Let $e_0, \dots, e_{q-1}$ be an orthonormal basis of $\mathbb{C}^q$ such that $e_0 = 1/\sqrt{q}(1, \dots, 1)$. Denote $E_0 = e_0 e_0^*$ and $E_1 = \sum_{i>0} e_i e_i^*$. These are $q \times q$ matrices. All entries of E_0 are equal to $1/q$, and the entries of E_1 are given by

$$E_1[\![x,y]\!] = \begin{cases} 1 - 1/q, & x = y; \\ -1/q, & x \neq y. \end{cases} \tag{4.11}$$

For a subset $S \subseteq [n]$, let E_S denote $\bigotimes_{j\in[n]} E_{s_j}$ where $s_j = 1$ if $j \in S$, and $s_j = 0$ otherwise. These matrices are orthogonal projectors:

$$E_S E_{S'} = \begin{cases} E_S, & S = S' \\ 0, & \text{otherwise.} \end{cases} \tag{4.12}$$

We define the matrices $\widetilde{G}_M$ from (4.8) by

$$\widetilde{G}_M = \sum_{S\subseteq[n]} \alpha_S(M)E_S, \tag{4.13}$$

where $\alpha_S(M)$ give an optimal solution to (2.3).

Lemma 4.14. *If $\widetilde{\Gamma}$ and Γ are defined as in Section 4.2, all X_M satisfy the orthogonality property (4.6) and $|Y| = \Omega(q^n)$, then*

$$\|\Gamma\| = \Omega\Bigl(\sqrt{\sum_{M\in\mathcal{C}} \alpha_\emptyset(M)^2}\Bigr). \tag{4.15}$$

Proof. Recall that $G_M = \sqrt{q^n/|X_M|}\widetilde{G}_M[\![X_M, Y]\!]$, hence, from (4.13), we get that

$$\begin{aligned} G_M = {} & \sqrt{\frac{q^n}{|X_M|}}\,\alpha_\emptyset(M)E_0^{\otimes n}[\![X_M, Y]\!] \\ & + \sqrt{\frac{q^n}{|X_M|}}\sum_{S\neq\emptyset} \alpha_S(M)E_S[\![X_M, Y]\!]. \end{aligned}$$

Let us calculate the sum $\mathrm{s}(G_M)$ of the entries of G_M. In the first term, each entry of $E_0^{\otimes n}$ equals q^{-n}. There are $|X_M|$ rows and $|Y|$ columns in the matrix; hence, the sum of the entries of the first term is $\sqrt{|X_M|/q^n}\ |Y|\alpha_\emptyset(M)$.

In the second term, $\mathrm{s}\bigl(\alpha_S(M)E_S[\![X_M, Y]\!]\bigr) = 0$ for all $S \neq \emptyset$. Indeed, if $S \in M$, then $\alpha_S(M) = 0$ by (2.3c). Otherwise,

$$\begin{aligned} \mathrm{s}(E_S[\![X_M, Y]\!]) &= \sum_{y\in Y}\sum_{x\in X_M} E_S[\![x, y]\!] = q^{|S|-n}\sum_{y\in Y}\sum_{x\in X_M} E_1^{\otimes|S|}[\![x_S, y_S]\!] \\ &= \frac{|X_M|}{q^n}\sum_{y\in Y}\sum_{z\in[q]^S} E_1^{\otimes|S|}[\![z, y_S]\!] = 0. \end{aligned}$$

(In the third step, the orthogonality condition (4.6) is used. In the last step, we use that the sum of the entries of every column of $E_1^{\otimes k}$ is zero if $k > 0$.) Summing up,

$$\mathrm{s}(G_M) = \sqrt{\frac{|X_M|}{q^n}}\ |Y|\alpha_\emptyset(M).$$

We are now ready to estimate $\|\Gamma\|$. Define two unit vectors $u \in \mathbb{R}^X$ and $v \in \mathbb{R}^Y$ by

$$u[\![(x,M)]\!] = \frac{\alpha_\emptyset(M)}{\sqrt{|X_M| \sum_{M\in\mathcal{C}} \alpha_\emptyset(M)^2}} \qquad \text{and} \qquad v[\![y]\!] = \frac{1}{\sqrt{|Y|}}$$

for all $(x, M) \in X$ and $y \in Y$. Then,

$$\begin{aligned}\|\Gamma\| \geq u^*\Gamma v &= \frac{\sum_{M\in\mathcal{C}} \alpha_\emptyset(M)\mathrm{s}(G_M)}{\sqrt{|X_M|\,|Y| \sum_{M\in\mathcal{C}} \alpha_\emptyset(M)^2}} \\ &= \sqrt{\frac{|Y|}{q^n} \sum_{M\in\mathcal{C}} \alpha_\emptyset(M)^2} = \Omega\Big(\sqrt{\sum_{M\in\mathcal{C}} \alpha_\emptyset(M)^2}\Big).\end{aligned}$$

□

In the remaining part of this section, we define the transformation $\widetilde{\Gamma} \xmapsto{\Delta_j} \widetilde{\Gamma}'$ and state some of the properties of $\widetilde{\Gamma}'$ that will be used in the subsequent sections. Using (4.11), we can define the action of Δ on E_0 and E_1 by

$$E_0 \xmapsto{\Delta} E_0 \qquad \text{and} \qquad E_1 \xmapsto{\Delta} -E_0.$$

We define $\widetilde{\Gamma}'$ by applying this transformation to E_0 and E_1 in the jth position in the tensor product of (4.13). The result is again a matrix of the form (4.8), but with each $\widetilde{G}_M$ replaced by

$$\widetilde{G}'_M = \sum_{S\subseteq[n]} \beta_S(M) E_S, \tag{4.16}$$

where $\beta_S(M) = \alpha_S(M) - \alpha_{S\cup\{j\}}(M)$. In particular, $\beta_S(M) = 0$ if $j \in S$ or $S \in M$. Thus,

$$(\widetilde{\Gamma}')^*\widetilde{\Gamma}' = \sum_{M\in\mathcal{C}} (\widetilde{G}'_M)^*\widetilde{G}'_M = \sum_{S\in 2^{[n]}} \Big(\sum_{M\in\mathcal{C}} \beta_S(M)^2\Big) E_S. \tag{4.17}$$

In particular, we obtain from (2.3b) that $\|\widetilde{\Gamma}'\| \leq 1$.

4.4. Boundedly generated certificate structures. In this section, we finish the proof of Theorem 1.6. In the settings of the theorem, the orthogonal arrays $T_M^{(i)}$ in (4.5) are already specified. Since each $M \in \mathcal{C}$ has only one inclusion-wise minimal element A_M, we drop all upper indices (i) in this section.

From the statement of the theorem, we have $|X_M| = q^{n-1}$, and, in particular, they are non-empty. Also, X_M satisfies the orthogonality property (4.6), and, by (4.7), we have

$$(4.18)\quad |Y| = \Big|[q]^n \setminus \bigcup_{M \in \mathcal{C}} X_M\Big| \geq q^n - \sum_{M \in \mathcal{C}} |X_M| = q^n - |\mathcal{C}| q^{n-1} \geq \frac{q^n}{2}.$$

Thus, the conditions of Lemma 4.14 are satisfied, and (4.15) holds.

Recall from Section 4.2 that in order to estimate $\|\Gamma'\|$, we consider the matrix $\widehat{\Gamma}'$. The matrix Γ' is a submatrix of $\widehat{\Gamma}'$; hence, it suffices to estimate $\|\widehat{\Gamma}'\|$. Let $k = \max_{M \in \mathcal{C}} |A_M|$. By Definition 1.4, $k = O(1)$.

Fix some order of elements in each $A_M = \{a_{M,1}, \dots, a_{M,|A_M|}\}$, and let $L_{M,i}$, where $M \in \mathcal{C}$ and $i \in [k]$, be subsets of $2^{[n]}$ satisfying the following properties:

- for each M, the set $2^{[n]} \setminus M$ is the disjoint union $L_{M,1} \sqcup \cdots \sqcup L_{M,k}$;
- for each M and each $i \leq |A_M|$, all elements of $L_{M,i}$ omit $a_{M,i}$;
- for each M and each i such that $|A_M| < i \leq k$, the set $L_{M,i}$ is empty.

Recall that, if $S \subseteq [n]$ and (s_j) is the corresponding characteristic vector, $E_S = \bigotimes_{j \in [n]} E_{s_j}$. The main idea behind defining $L_{M,i}$s is as follows.

CLAIM 4.19. *If $S, S' \in L_{M,i}$, then*

$$(E_S[\![X_M, [q]^n]\!])^*(E_{S'}[\![X_M, [q]^n]\!]) = \begin{cases} E_S/q, & S = S'; \\ 0, & \text{otherwise.} \end{cases}$$

PROOF. If we strike out the $a_{M,i}$th element in all elements of X_M, we obtain $[q]^{n-1}$ by the definition of an orthogonal array. All elements of $L_{M,i}$ omit $a_{M,i}$; hence, E_S has E_0 in the $a_{M,i}$th position for all $S \in L_{M,i}$. Thus, the $a_{M,i}$th entries of x and y have no impact on the value of $E_S[\![x, y]\!]$.

Let (s_j) and (s'_j) be the characteristic vectors of S and S'. Then,

$$E_S[\![X_M, [q]^n]\!] = \Big(\bigotimes_{j \in [n] \setminus \{a_{M,i}\}} E_{s_j} \Big) \otimes \frac{e_0^*}{\sqrt{q}}.$$

(Here e_0^* is on the $a_{M,i}$th element of $[q]^n$.) Similarly for S', and the claim follows from (4.12). □

For each M, decompose $\widetilde{G}'_M$ from (4.16) into $\sum_{i\in[k]} \widetilde{G}'_{M,i}$, where

$$\widetilde{G}'_{M,i} = \sum_{S \in L_{M,i}} \beta_S(M) E_S.$$

Define similarly to Section 4.2,

$$\widehat{G}'_{M,i} = \sqrt{\frac{q^n}{|X_M|}}\, \widetilde{G}'_{M,i}[\![X_M, [q]^n]\!] = \sqrt{q} \sum_{S \in L_{M,i}} \beta_S(M) E_S[\![X_M, [q]^n]\!],$$

and let $\widehat{\Gamma}'_i$ be the matrix consisting of $\widehat{G}'_{M,i}$, for all $M \in \mathcal{C}$, stacked one on another like in (4.8). Then, $\widehat{\Gamma}' = \sum_{i\in[k]} \widehat{\Gamma}'_i$. We have

$$(\widehat{\Gamma}'_i)^* \widehat{\Gamma}'_i = \sum_{M \in \mathcal{C}} (\widehat{G}'_{M,i})^* \widehat{G}'_{M,i} = \sum_{M \in \mathcal{C}} \sum_{S \in L_{M,i}} \beta_S(M)^2 E_S,$$

by Claim 4.19. Similarly to (4.17), we get $\|\widehat{\Gamma}'_i\| \le 1$. By the triangle inequality, $\|\widehat{\Gamma}'\| \le k$, hence, $\|\Gamma'\| \le k = O(1)$. Combining this with (4.15) and using Theorem 4.2, we obtain the necessary lower bound. This finishes the proof of Theorem 1.6.

4.5. Fourier Basis. In Section 4.3, we defined e_i as an arbitrary orthonormal basis satisfying the requirement that e_0 has all its entries equal to $1/\sqrt{q}$. In the next section, we will specify a concrete choice for e_i. Its construction is based on the Fourier basis we briefly review in this section.

Let p be a positive integer, and $\mathbb{Z}_p$ be the cyclic group of order p, formed by the integers modulo p. Consider the complex vector space $\mathbb{C}^{\mathbb{Z}_p}$. The vectors $(\chi_a)_{a\in\mathbb{Z}_p}$, defined by $\chi_a[\![b]\!] = \mathsf{e}^{2\pi \mathsf{i} ab/p}/\sqrt{p}$, form its orthonormal basis. Note that the value of $\chi_a[\![b]\!]$ is well defined because $\mathsf{e}^{2\pi\mathsf{i}} = 1$.

If $U \subseteq \mathbb{Z}_p$, then the *Fourier bias* (Tao & Vu 2006) of U is defined by

$$\|U\|_{\mathrm{u}} = \frac{1}{p}\left|\max_{a\in\mathbb{Z}_p\setminus\{0\}} \sum_{u\in U} \mathsf{e}^{2\pi\mathsf{i}au/p}\right|. \tag{4.20}$$

It is a real number between 0 and $|U|/p$. In the next section, we will need the following result stating the existence of sets with small Fourier bias and arbitrary density.

Theorem 4.21. *For any real $0 < \delta < 1$, it is possible to construct $U \subseteq \mathbb{Z}_q$ such that $|U| \sim \delta q$, $\|U\|_{\mathrm{u}} = O(\mathrm{polylog}(q)/\sqrt{q})$ and q is arbitrary large. In particular, $\|U\|_{\mathrm{u}} = o(1)$.*

For instance, one may prove that a random subset satisfies these properties with high probability (Tao & Vu 2006, Lemma 4.16). There also exist explicit constructions (Gillespie 2010).

4.6. General Certificate Structures. In this section, we finish the proof of Theorem 1.3. There are two main reasons why it is not possible to prove a general result like Theorem 1.6 for arbitrary certificate structures.

A first counterexample is given by Proposition 3.2 stating that the learning graph complexity of the hidden shift certificate structure is $\Omega(n^{1/3})$ and the statement at the end of Section 1 that the quantum query complexity of the hidden shift problem is $O(\log n)$. The proof in Section 4.4 cannot be applied here, because k in the decomposition of $\widetilde{G}'_M$ into $\sum_{i\in[k]} \widetilde{G}'_{M,i}$ would not be bounded by a constant. We solve this by considering much "thicker" orthogonal arrays $T_M^{(i)}$.

Next, the orthogonality property (4.6) is not satisfied automatically for general certificate structures. For instance, assume $A_M^{(1)} = \{1,2\}$, $A_M^{(2)} = \{2,3\}$, and the orthogonal arrays are given by the conditions $x_1 = x_2$ and $x_2 = x_3$, respectively. Then, for any input x satisfying both conditions, we have $x_1 = x_3$, and the orthogonality condition fails for $S = \{1, 3\}$.

The problem in the last example is that the orthogonal arrays are not independent because $A_M^{(1)}$ and $A_M^{(2)}$ intersect. We cannot avoid that $A_M^{(i)}$s intersect, but we still can have $T_M^{(i)}$s independent by defining them on independent parts of the input alphabet.

More formally, let $\ell = \max_{M\in\mathcal{C}} \ell(M)$, where $\ell(M)$ is defined in Section 4.2 as the number of inclusion-wise minimal elements of M. We define the input alphabet as $Z = \mathbb{Z}_p^\ell$ for some p to be defined later. Hence, the size of the alphabet is $q = p^\ell$.

Let $Q_M^{(i)}$ be an orthogonal array of length $|A_M^{(i)}|$ over the alphabet $\mathbb{Z}_p$. We will specify a concrete choice in a moment. From $Q_M^{(i)}$, we define $T_M^{(i)}$ in (4.5) by requiring that the ith components of the elements in the sequence satisfy $Q_M^{(i)}$. The sets X_M are defined as in (4.5). We additionally define

$$X_M^{(i)} = \{x \in \mathbb{Z}_p^n \mid x_{A_M^{(i)}} \in Q_M^{(i)}\},$$

for $i \le \ell(M)$, and $X_M^{(i)} = \mathbb{Z}_p^n$ otherwise. Note that $X_M = \prod_{i=1}^{\ell} X_M^{(i)}$ in the sense that, for each sequence $x^{(i)} \in X_M^{(i)}$ with $i = 1, \ldots, \ell$, there is a corresponding element $x \in X_M$ with $x_j = (x_j^{(1)}, \ldots, x_j^{(\ell)})$.

Now we make our choice for $Q_M^{(i)}$. Let $U \subseteq \mathbb{Z}_p$ be a set with small Fourier bias and some $\delta = |U|/p$ that exists due to Theorem 4.21. We define $Q_M^{(i)}$ as consisting of all $x \in \mathbb{Z}_p^{A_M^{(i)}}$ such that the sum of the elements of x belongs to U. With this definition,

$$|X_M^{(i)}| = \delta p^n. \tag{4.22}$$

Hence, there are exactly δq^n elements $x \in Z^n$ such that $x_{A_M^{(i)}} \in T_M^{(i)}$. If we let $\delta = 1/(2\ell|\mathcal{C}|)$, a calculation similar to (4.18) shows that $|Y| \ge q^n/2$. Also, by considering each $i \in [\ell]$ independently, it is easy to see that all X_M satisfy the orthogonality condition. Thus, Lemma 4.14 applies, and (4.15) holds.

Now it remains to estimate $\|\Gamma'\|$, and it is done by considering matrix $\widehat{\Gamma}'$ as described in Section 4.2 and performed once in Section 4.4. If $\widetilde{\Gamma}' = 0$, then also $\Gamma' = 0$, and we are done. Thus, we further assume $\widetilde{\Gamma}' \neq 0$. Recall that $(\chi_a)_{a\in\mathbb{Z}_p}$ denotes the Fourier basis of $\mathbb{Z}_p$. The basis e is defined as the Fourier basis of $\mathbb{C}^Z$. It consists of the elements of the form $e_a = \bigotimes_{i=1}^{\ell} \chi_{a^{(i)}}$ where $a = (a^{(i)}) \in Z$. Note that e_0 has the required value, where 0 is interpreted as the neutral element of Z.

If $v = (v_j) = (v_j^{(i)}) \in Z^n$, we define $e_v = \bigotimes_{j=1}^{n} e_{v_j}$, and $v^{(i)} \in \mathbb{Z}_p^n$ as $(v_1^{(i)}, \ldots, v_n^{(i)})$. Also, for $w = (w_j) \in \mathbb{Z}_p^n$, we define $\chi_w = \bigotimes_{j=1}^{n} \chi_{w_j}$.

Fix an arbitrary $M \in \mathcal{C}$. Let $\widetilde{B}_M = (\widetilde{G}'_M)^*\widetilde{G}'_M$ and $\widehat{B}_M = (\widehat{G}'_M)^*\widehat{G}'_M$. We aim to show that

$$\|\widetilde{B}_M - \widehat{B}_M\| \to 0 \quad \text{as} \quad p \to \infty, \tag{4.23}$$

because this implies

$$\|(\widetilde{\Gamma}')^*\widetilde{\Gamma}' - (\widehat{\Gamma}')^*\widehat{\Gamma}'\| = \Big\|\sum_{M\in\mathcal{C}} (\widetilde{B}_M - \widehat{B}_M)\Big\| \le \sum_{M\in\mathcal{C}} \|\widetilde{B}_M - \widehat{B}_M\| \to 0$$

as $p \to \infty$. As $\|\widetilde{\Gamma}'\| > 0$, this implies that $\|\Gamma'\| \le 2\|\widetilde{\Gamma}'\|$ for p large enough, and together with (4.15) and Theorem 4.2, this implies Theorem 1.3.

From (4.16), we conclude that the eigenbasis of $\widetilde{B}_M$ consists of the vectors e_v, with $v \in Z^n$, defined above. In order to understand $\widehat{B}_M$ better, we have to understand how $e_v[\![X_M]\!]$ behave. We have

$$(e_v[\![X_M]\!])^*(e_{v'}[\![X_M]\!]) = \prod_{i=1}^{\ell} (\chi_{v^{(i)}}[\![X_M^{(i)}]\!])^*(\chi_{v'^{(i)}}[\![X_M^{(i)}]\!]). \tag{4.24}$$

Hence, it suffices to understand the behavior of $\chi_w[\![X_M^{(i)}]\!]$. For $w \in \mathbb{Z}_p^n$, $A \subseteq [n]$ and $c \in \mathbb{Z}_p$, we write $w + cA$ for the sequence $w' \in \mathbb{Z}_p^n$ defined by

$$w'_j = \begin{cases} w_j + c, & j \in A; \\ w_j, & \text{otherwise.} \end{cases}$$

In this case, we say that w and w' are obtained from each other by a *shift on A*.

Claim 4.25. *Assume that w and w' are elements of $\mathbb{Z}_p^n$, and let $\xi = (\chi_w[\![X_M^{(i)}]\!])^*(\chi_{w'}[\![X_M^{(i)}]\!])$. If $w = w'$, then $\xi = \delta$. If $w \neq w'$, but w can be obtained from w' by a shift on $A_M^{(i)}$, then $|\xi| \leq \|U\|_{\mathrm{u}}$. Finally, if w cannot be obtained from w' by a shift on $A_M^{(i)}$, then $\xi = 0$.*

Proof. Arbitrarily enumerate the elements of $U = \{u_1, \ldots, u_m\}$ where $m = \delta p$. Denote, for the sake of brevity, $A = A_M^{(i)}$. Consider the decomposition $X_M^{(i)} = \bigsqcup_{k=1}^m X_k$, where

$$X_k = \left\{ w \in \mathbb{Z}_p^n \mid \sum\nolimits_{j\in A} w_j = u_k \right\}.$$

Fix an arbitrary element $a \in A$ and denote $\bar{w} = w - w_a A$ and $\bar{w}' = w' - w'_a A$. In both of them, $\bar{w}_a = \bar{w}'_a = 0$, and by an argument similar to Claim 4.19, we get that

$$(\chi_{\bar{w}}[\![X_k]\!])^*(\chi_{\bar{w}'}[\![X_k]\!]) = \begin{cases} 1/p, & \bar{w} = \bar{w}'; \\ 0, & \text{otherwise.} \end{cases} \tag{4.26}$$

If $x \in X_k$, then

$$\begin{aligned} \chi_w[\![x]\!] = \prod_{j=1}^n \chi_{w_j}[\![x_j]\!] &= \frac{1}{\sqrt{p^n}} \exp\left[\frac{2\pi\mathsf{i}}{p} \sum_{j=1}^n w_j x_j\right] \\ &= \frac{1}{\sqrt{p^n}} \exp\left[\frac{2\pi\mathsf{i}}{p}\Big(\sum_{j=1}^n \bar{w}_j x_j + w_a \sum_{j\in A} x_j\Big)\right] \\ &= \exp\Big(\frac{2\pi\mathsf{i}\; w_a u_k}{p}\Big)\chi_{\bar{w}}[\![x]\!]. \end{aligned}$$

Hence,

$$\begin{aligned} (\chi_w[\![X_M^{(i)}]\!])^*(\chi_{w'}[\![X_M^{(i)}]\!]) &= \sum_{k=1}^m (\chi_w[\![X_k]\!])^*(\chi_{w'}[\![X_k]\!]) \\ &= \sum_{k=1}^m \mathsf{e}^{2\pi\mathsf{i}(w'_a - w_a)u_k/p}(\chi_{\bar{w}}[\![X_k]\!])^*(\chi_{\bar{w}'}[\![X_k]\!]). \end{aligned} \tag{4.27}$$

If w' cannot be obtained from w by a shift on A, then $\bar{w} \neq \bar{w}'$ and (4.27) equals zero by (4.26). If $w = w'$, then (4.27) equals

$m/p = \delta$. Finally, if w' can be obtained from w by a shift on A but $w \neq w'$, then $\bar{w} = \bar{w}'$ and $w_a \neq w'_a$. By (4.26) and (4.20), we get that (4.27) does not exceed $\|U\|_{\mathrm{u}}$ in absolute value. □

Let $v \in Z^n$, and $S = \{j \in [n] \mid v_j \neq 0\}$. Let $v' \in Z^n$ and define S' similarly. By (4.10), (4.16), (4.22) and (4.24), we have

$$\begin{aligned} e_v^* \widehat{B}_M e_{v'} &= \frac{q^n \beta_S(M)\beta_{S'}(M)}{|X_M|} (e_v[\![X_M]\!])^* (e_{v'}[\![X_M]\!]) \\ &= \frac{\beta_S(M)\beta_{S'}(M)}{\delta^\ell} \prod_{i=1}^{\ell} (\chi_{v^{(i)}}[\![X_M^{(i)}]\!])^* (\chi_{v'^{(i)}}[\![X_M^{(i)}]\!]). \end{aligned} \tag{4.28}$$

By this and Claim 4.25, we have that

$$e_v^* \widehat{B}_M e_v = \beta_S(M)^2 = e_v^* \widetilde{B}_M e_v. \tag{4.29}$$

Call v and v' *equivalent*, if $\beta_S(M)$ and $\beta_{S'}(M)$ are both nonzero and, for each $i \in [\ell]$, $v^{(i)}$ can be obtained from $v'^{(i)}$ by a shift on $A_M^{(i)}$. By (4.28) and Claim 4.25, we have that $e_v^* \widehat{B}_M e_{v'}$ is nonzero only if v and v' are equivalent.

For each $i \in [\ell]$, there are at most $|A_M^{(i)}| \leq n$ shifts of $v^{(i)}$ on $A_M^{(i)}$ that have an element with an index in $A_M^{(i)}$ equal to 0. By (2.3c), the latter is a necessary condition for $\beta_S(M)$ being nonzero. Hence, for each $v \in Z^n$, there are at most n^ℓ elements of Z^n equivalent to it.

Thus, in the basis of e_vs, the matrix $\widehat{B}_M$ has the following properties. By (4.29), its diagonal entries equal the diagonal entries of $\widetilde{B}_M$, and the latter matrix is diagonal. Next, $\widehat{B}_M$ is block diagonal with the blocks of size at most n^ℓ. By (4.28) and Claim 4.25, the off-diagonal elements satisfy

$$|e_v^* \widehat{B}_M e_{v'}| \leq \frac{\|U\|_{\mathrm{u}}}{\delta} \beta_S(M)\beta_{S'}(M),$$

because $\|U\|_{\mathrm{u}} \leq \delta$. Since the values of $\beta_S(M)$ do not depend on p, and by Theorem 4.21, the off-diagonal elements of $\widehat{B}_M$ tend to zero as p tends to infinity. Since the sizes of the blocks also do not depend on p, the norm of $\widetilde{B}_M - \widehat{B}_M$ also tends to 0, as required in (4.23). This finishes the proof of Theorem 1.3.

Acknowledgements

A.B. would like to thank Troy Lee, Robin Kothari and Rajat Mittal for sharing their ideas on the limitations of learning graphs. In particular, the notion of the learning graph complexity of a certificate structure and the proof of Proposition 3.1 stem from these ideas.

A.B. is supported by Scott Aaronson's Alan T. Waterman Award from the National Science Foundation. This research was performed when A.B. was at the University of Latvia and was supported by the European Social Fund within the project "Support for Doctoral Studies at University of Latvia" and by FET-Open project QCS. A.R. acknowledges the support of Mike and Ophelia Lazaridis Fellowship and David R. Cheriton Graduate Scholarship.

References

Scott Aaronson and Yaoyun Shi, Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM* **51**(4) (2004), 595–605.

Andris Ambainis, Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences* **64**(4) (2002), 750–767.

Andris Ambainis, Quantum walk algorithm for element distinctness. *SIAM Journal on Computing* **37**(1) (2007), 210–239.

Aleksandrs Belovs, Span programs for functions with constant-sized 1-certificates. In *Proc. of 44th ACM STOC*, 2012a, 77–84.

Aleksandrs Belovs, Learning-graph-based quantum algorithm for k-distinctness. In *Proc. of 53rd IEEE FOCS*, 2012b, 207–216.

Aleksandrs Belovs and Troy Lee, Quantum algorithm for k-distinctness with prior knowledge on the input. 2011.

Aleksandrs Belovs and Robert Špalek, Adversary lower bound for the k-sum problem. In *Proc. of 4th ACM ITCS*, 2012, 323–328.

Stephen Boyd and Lieven Vandenberghe, *Convex optimization.* Cambridge University Press, 2004.

Gilles Brassard, Peter Høyer, and Alain Tapp, Quantum cryptanalysis of hash and claw-free functions. In *Proc. of 3rd LATIN*, vol. 1380 of *LNCS*. Springer, 1998, 163–169.

Harry Buhrman and Ronald de Wolf, Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science* **288** (2002), 21–43.

Andrew M. Childs and Jason M. Eisenberg, Quantum algorithms for subset finding. *Quantum Information & Computation* **5**(7) (2005), 593–604.

Mark Ettinger, Peter Høyer, and Emanuel Knill, The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters* **91**(1) (2004), 43–48.

Dmitry Gavinsky and Tsuyoshi Ito, A quantum query algorithm for the graph collision problem. 2012.

Bryan Gillespie, On randomness of subsets of $\mathbb{Z}_N$, as described by uniformity of Fourier coefficients. 2010.

Lov K. Grover, A fast quantum mechanical algorithm for database search. In *Proc. of 28th ACM STOC*, 1996, 212–219.

A. S. Hedayat, N. J. A. Sloane, and John Stufken, *Orthogonal arrays: theory and applications*. Springer, 1999.

Peter Høyer, Troy Lee, and Robert Špalek, Negative weights make adversaries stronger. In *Proc. of 39th ACM STOC*, 2007, 526–535.

Greg Kuperberg, A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing* **35** (2005), 170–188.

Troy Lee, Frédéric Magniez, and Miklos Santha, A learning graph based quantum query algorithm for finding constant-size subgraphs. 2011a.

Troy Lee, Rajat Mittal, Ben W. Reichardt, Robert Špalek, and Mario Szegedy, Quantum query complexity of the state conversion problem. In *Proc. of 52nd IEEE FOCS*, 2011b, 344–353.

Troy Lee, Frédéric Magniez, and Miklos Santha, Improved quantum query algorithms for triangle finding and associativity testing. In *Proc. of 24th ACM-SIAM SODA*, 2013, 1486–1502.

Frédéric Magniez, Miklos Santha, and Mario Szegedy, Quantum algorithms for the triangle problem. *SIAM Journal on Computing* **37**(2) (2007), 413–424.

Frédéric Magniez, Ashwin Nayak, Jérémie Roland, and Miklos Santha, Search via quantum walk. *SIAM Journal on Computing* **40**(1) (2011), 142–164.

Ben W. Reichardt, Reflections for quantum query algorithms. In *Proc. of 22nd ACM-SIAM SODA*, 2011, 560–569.

Robert Špalek and Mario Szegedy, All quantum adversary methods are equivalent. *Theory of Computing* **2** (2006), 1–18.

Terence Tao and Vav H. Vu, *Additive combinatorics*, vol. 105 of *Cambridge Studies in Advanced Mathematics*. 2006.

Shengyu Zhang, On the power of Ambainis lower bounds. *Theoretical Computer Science* **339**(2) (2005), 241–256.

Yechao Zhu, Quantum query complexity of subgraph containment with constant-sized certificates. *International Journal of Quantum Information* **10**(3) (2012).

Manuscript received 28 May 2013

Aleksandrs Belovs
Computer Science and Artificial Intelligence Laboratory,
Massachusetts Institute of Technology,
Cambridge, MA 02139, USA.
abelov@csail.mit.edu
http://people.csail.mit.edu/abelov/

Ansis Rosmanis
David R. Cheriton School of Computer Science and Institute for Quantum Computing,
University of Waterloo,
Waterloo, ON N2L 3G1, Canada.
arosmanis@uwaterloo.ca