SIAM J. COMPUT.
Vol. 38, No. 1, pp. 46–62

LOWER BOUNDS FOR RANDOMIZED AND QUANTUM QUERY COMPLEXITY USING KOLMOGOROV ARGUMENTS*

SOPHIE LAPLANTE† AND FRÉDÉRIC MAGNIEZ†

Abstract. We prove a very general lower bound technique for quantum and randomized query complexity that is easy to prove as well as to apply. To achieve this, we introduce the use of Kolmogorov complexity to query complexity. Our technique generalizes the weighted and unweighted methods of Ambainis and the spectral method of Barnum, Saks, and Szegedy. As an immediate consequence of our main theorem, it can be shown that adversary methods can only prove lower bounds for Boolean functions f in $O(\min(\sqrt{nC_0(f)}, \sqrt{nC_1(f)}))$, where C_0, C_1 is the certificate complexity and n is the size of the input.

Key words. quantum computing, lower bounds, query complexity, adversary method, Kolmogorov complexity

AMS subject classifications. 81P68, 68Q30, 68Q30

DOI. 10.1137/050639090

1. Introduction.

1.1. Overview. In this paper, we study lower bounds for randomized and quantum query complexity. In the query model, the input is accessed using oracle queries, and the query complexity of an algorithm is the number of calls to the oracle. Since it is difficult to obtain lower bounds on time directly, the query model is often used to prove concrete lower bounds, in classical as well as quantum computation.

The two main tools for proving lower bounds on randomized query complexity, the polynomial method [7] and the adversary method [2], were successfully extended to quantum computation. In the randomized setting, the adversary method is most often applied using Yao's minimax principle [21]. Using a different approach, which introduces the notion of quantum adversaries, Ambainis developed a general scheme in which it suffices to analyze combinatorial properties of the function in order to obtain a quantum lower bound. Recently, Aaronson [1] brought these combinatorial properties back to randomized computation, using Yao's minimax principle.

The most general method for proving lower bounds in quantum query complexity is the semidefinite programming method of Barnum, Saks, and Szegedy [5]. This method is in fact an exact characterization of the query complexity. However, the method is so general that it is very difficult to apply to obtain concrete lower bounds. Barnum, Saks, and Szegedy gave a weaker method derived from the semidefinite programming approach, using weight matrices and their largest eigenvalue. This spectral method can be thought of as a generalization of Ambainis's unweighted method. Other generalizations of Ambainis's unweighted method have been previously introduced [6, 3]. All of them use a weight function on the instances. The difficulty in applying these methods is finding a good weight function on the instances. Høyer,

*Received by the editors August 29, 2005; accepted for publication (in revised form) September 13, 2007; published electronically March 28, 2008. A preliminary version of this paper appeared in *Proceedings of the* 16*th Annual IEEE Conference on Computational Complexity*, 2004, pp. 294–304. Work was partially supported by the European Commission IST project QAP 015848 and by the ANR Blanc NT05-2_42239 AlgoQP.

http://www.siam.org/journals/sicomp/38-1/63909.html

†LRI, Univ. Paris-Sud, CNRS, Orsay, F-91405 France (laplante@lri.fr, magniez@lri.fr).

Neerbek, and Shi [15] were the first to use such weight assignments to prove lower bounds for searching in ordered lists and sorting.

This paper presents a new, very general adversary technique (Theorem 1.1) to prove lower bounds in quantum and randomized query complexity. We believed that this technique is simpler to prove and to apply. It is based on the framework of Kolmogorov complexity. This framework has proven to be very useful for proving negative results in other models of computation, for example, for the number of rounds and length of advice in random-self-reductions in [13, 4]. The techniques we use here are an adaptation of those techniques to the framework of query complexity. We expect that this framework will prove to be useful for negative results in other quantum models of computation, for instance, communication complexity, where we hope to give lower bounds for bounded round query complexity.

The proof of Theorem 1.1 is in two parts. The first part (divergence lemma) shows how fast the computations can diverge when they start on different inputs. This part depends on the model of computation (randomized or quantum). The quantum case of this lemma was first proven by Ambainis [2]. The second part (query information lemma) does not depend on the model of computation. It establishes the relationship between the Kolmogorov complexity of individual positions of the input and the probability that a given algorithm makes a query to this position. Whereas Aaronson [1] used a different approach to prove a version of Ambainis's method for randomized algorithms, here we use the same framework to establish lower bounds for both quantum and randomized query complexities (QQC and RQC).

We show that our method encompasses all previous adversary methods, including the quantum and randomized weighted methods [3, 1] (Theorem 4.2) and the spectral method [5] (Theorem 4.3). As an immediate consequence of our main theorem (observed by Troy Lee), our method can only prove lower bounds for arbitrary Boolean functions in $O(\min(\sqrt{nC_0(f)}, \sqrt{nC_1(f)}))$, where C_0 and C_1 is the certificate complexity of negative and positive instances, respectively, of f and n is the size of the input (Theorem 5.2). Prior to our work, it was known [3] that the unweighted Ambainis method [2, Theorem 5.1] could not prove bounds better than $\Omega(\sqrt{C_0(f)C_1(f)})$ for total functions; Szegedy [20] also proved independently that the semidefinite programming method could not prove lower bounds better than $O(\min(\sqrt{nC_0(f)}, \sqrt{nC_1(f)}))$, and Zhang [22] proved the same thing for Ambainis's weighted method.

We end the paper by giving some applications of our method to prove lower bounds for some graph properties: bipartiteness (Theorem 5.4) and connectivity (Theorem 5.3). The lower bound on connectivity was proven in [12] and the one on bipartiteness by Dürr and independently in [22]. We reprove it here to illustrate the simplicity of our method.

In recent developments, Špalek and Szegedy [19] showed that our method is equivalent to both the spectral method [5] as well as Ambainis's weighted method [3]. Subsequently, Laplante, Lee, and Szegedy showed that the square of the quantum adversary method was also a lower bound on formula size [16].

1.2. Main result. The conditional Kolmogorov complexity $\mathsf{K}(a|b)$ (defined formally in section 2.1) is the length of the shortest program which prints a given b as input. Our main result relates the query complexity of an algorithm A for f to the quantities $\{\mathsf{K}(i|x, A), \mathsf{K}(i|y, A) : x_i \neq y_i\}$ for any x, y such that $f(x) \neq f(y)$.

THEOREM 1.1. *There exists a constant $C > 0$ such that the following holds. Let Σ be a finite set, let $n \geq 1$ be an integer, and let $S \subseteq \Sigma^n$ and S' be sets. Let $f : S \to S'$. Let A be an algorithm that for all $x \in S$ computes f, with bounded error ε and at most T queries to the input. Then for every $x, y \in S$ with $f(x) \neq f(y)$:*

1. *if A is a quantum algorithm, then*

$$T \geq C \times \frac{1 - 2\sqrt{\varepsilon(1-\varepsilon)}}{\sum_{i:x_i \neq y_i} \sqrt{2^{-\mathsf{K}(i|x,A)-\mathsf{K}(i|y,A)}}};$$

2. *if A is a randomized algorithm, then*

$$T \geq C \times \frac{1 - 2\varepsilon}{\sum_{i:x_i \neq y_i} \min\left(2^{-\mathsf{K}(i|x,A)}, 2^{-\mathsf{K}(i|y,A)}\right)}.$$

We briefly describe the intuition behind the proof of Theorem 1.1. Consider an algorithm that purports to compute f, presented with two inputs x, y that lead to different outputs. The algorithm must query those positions where x and y differ with average probability of the order of $\frac{1}{T}$, or it will not successfully compute the function. On the other hand, the queries that are made with high average probability can be described succinctly given the input and the algorithm, by using the Shannon–Fano code. If we exhibit a pair of strings x, y for which there is no succinct description of any of the positions where x and y differ, then the number of queries must be large.

The same reasoning can be applied to classical and to quantum computing; the only difference is how fast two different input states cause the outputs to diverge to different outcomes.

To conclude the introduction we give a very simple application, for Grover search.

Example 1. Fix n and a quantum algorithm A for a Grover search for instances of length n. Let z be a binary string of length $\log n$, with $\mathsf{K}(z|A) \geq \log n$. Let j be the integer between 0 and $n-1$ whose binary expansion is z. Consider x, the all 0's string, and let y be everywhere 0 except at position $i = j + 1$, where it is 1. Then $\mathsf{K}(i|x, A) \geq \log n - O(1)$ and $\mathsf{K}(i|y, A) \geq 0$; therefore, $\mathsf{QQC}(\textsc{Search}) = \Omega(\sqrt{n})$.

2. Preliminaries.

2.1. Kolmogorov complexity. We use a few standard results in Kolmogorov complexity and information theory in this paper. We briefly review these here. The reader is invited to consult standard textbooks such as [17] for more background on Kolmogorov complexity and [9] for more on information theory. We denote the length of a finite string x by $|x|$. We assume that the Turing machine's alphabet is the same finite alphabet as the alphabet used to encode instances of the function under consideration. Letters x, y typically represent instances; i is an index into the binary representation of the instance; and p, q are probability distributions. Programs are denoted P, and the output of a Turing machine M on input x is written $M(x)$. When there are multiple inputs, we assume that a standard encoding of tuples is used.

Definition 2.1.

1. *A set of strings is* prefix-free *if no string is a prefix of another string in the set.*
2. *A universal Turing machine M is* prefix-free *if the set of programs $\{P : \exists x\, M(P, x) \neq \epsilon\}$, where ϵ is the empty string, is prefix-free.*
3. *Let M be a universal prefix-free Turing machine. Let x and y be finite strings. The* prefix-free Kolmogorov complexity *of x given y with respect to M is denoted $\mathsf{K}_M(x|y)$ and defined as follows:*

$$\mathsf{K}_M(x|y) = \min(|P| \text{ such that } M(P, y) = x).$$

In the rest of the paper M is a fixed universal prefix-free Turing machine, and we will write K instead of K_M. When y is the empty string, we write $\mathsf{K}(x)$ instead of $\mathsf{K}(x|y)$.

We first state standard bounds on conditional Kolmogorov complexity, where the last one is from [17, Theorem 3.9.1, p. 232].

PROPOSITION 2.2. *There exists a constant $c \geq 0$ such that, for every finite string σ,*

$$\mathsf{K}(x|\sigma) \leq \mathsf{K}(x) + c, \tag{2.1}$$

$$\mathsf{K}(x) \leq \mathsf{K}(\sigma) + K(x|\sigma) + c, \tag{2.2}$$

$$|\mathsf{K}(x,y) - \mathsf{K}(x) - \mathsf{K}(y|x,\mathsf{K}(x))| \leq c. \tag{2.3}$$

We shall also use the following bound.

PROPOSITION 2.3. *There is a constant $c \geq 0$ such that, for any three strings x, y, z,*

$$\mathsf{K}(z|x) \geq \mathsf{K}(x,y) - \mathsf{K}(x) - \mathsf{K}(y|z,x) + \mathsf{K}(z|x,y,\mathsf{K}(x,y)) - c.$$

Proof. Using the third bound of Proposition 2.2, there is a constant $c_1 \geq 0$ such that

$$|\mathsf{K}(a,b) - \mathsf{K}(a) - \mathsf{K}(b|a,\mathsf{K}(a))| \leq c_1.$$

Substituting x, y for a and z for b:

$$\mathsf{K}(x,y) + \mathsf{K}(z|x,y,\mathsf{K}(x,y)) - c_1 \leq \mathsf{K}(x,y,z) \leq \mathsf{K}(x) + \mathsf{K}(z|x) + \mathsf{K}(y|z,x) + c_2,$$

which gives the result, where the second inequality follows from the first and third bounds of Proposition 2.2. ∎

The main motivation for using prefix-free Kolmogrov complexity is the bound known as Kraft's inequality together with the last two bounds of Proposition 2.2.

PROPOSITION 2.4 (Kraft's inequality). *Let T be any prefix-free set of finite strings. Then $\sum_{P \in T} 2^{-|P|} \leq 1$. In particular, for any set of finite strings S and any finite string σ, $\sum_{x \in S} 2^{-\mathsf{K}(x|\sigma)} \leq 1$.*

A *source* $\mathcal{S}$ of finite strings is a pair (S, p), where S is a set of finite strings and p is a probability distribution over S.

PROPOSITION 2.5 (Shannon's coding theorem). *Consider a source $\mathcal{S}$ of finite strings where x occurs with probability $p(x)$. Then for any code for $\mathcal{S}$ the average code length is bounded below by the entropy of the source; that is, if x is encoded by the code word $c(x)$ of length $|c(x)|$, $H(\mathcal{S}) = \sum_{x:p(x)\neq 0} p(x) \log(\frac{1}{p(x)}) \leq \sum_{x:p(x)\neq 0} p(x)|c(x)|$.*

LEMMA 2.6. *Let $\mathcal{S}$ be a source as above. Then for any fixed finite string σ there exists a string x such that $p(x) \neq 0$ and $\mathsf{K}(x|\sigma) \geq \log(\frac{1}{p(x)})$.*

Proof. By Shannon's coding theorem,

$$H(\mathcal{S}) = \sum_{x:p(x)\neq 0} p(x) \log\left(\frac{1}{p(x)}\right) \leq \sum_{x:p(x)\neq 0} p(x)\mathsf{K}(x|\sigma),$$

because $\mathsf{K}(x|\sigma)$ is the length of an encoding of x. Therefore there exists x such that $p(x) \neq 0$ and $\mathsf{K}(x) \geq \log(\frac{1}{p(x)})$. ∎

The Shannon–Fano code is a prefix-free code that encodes each word x with $p(x) \neq 0$, using $\lceil \log(\frac{1}{p(x)}) \rceil$ bits. We will write $\log(\frac{1}{p(x)})$ to simplify notation. The code can easily be computed given a description of the probability distribution. We formalize this in the following proposition, letting $\mathsf{K}(x|\mathcal{S})$ denote the prefix-free Kolmogorov complexity of x given a finite description of $\mathcal{S}$.

PROPOSITION 2.7 (Shannon–Fano code). *There exists a constant $c \geq 0$ such that, for every source $\mathcal{S}$ as above, for all x such that $p(x) \neq 0$, $\mathsf{K}(x|\mathcal{S}) \leq \log(\frac{1}{p(x)}) + c$.*

2.2. Query models. The quantum query model was implicitly introduced by Deutsch, Jozsa, Simon, Bernstein, Vazirani, and Grover [11, 10, 18, 8, 14] and explicitly by Beals et al. [7]. In this model, as in its classical counterpart, we pay for accessing the oracle, but unlike the classical case, the machine can use the power of quantum parallelism to make queries in superposition. Access to the input $x \in \Sigma^n$, where Σ is a finite set, is achieved by way of a query operator O_x. The *query complexity* of an algorithm is the number of calls to O_x.

The state of a computation is represented by a register R composed of three subregisters: the *query register* $i \in \{0, \ldots, n\}$, the *answer register* $z \in \Sigma$, and the *work register* w. We denote a register using the ket notation $|R\rangle = |i\rangle|z\rangle|w\rangle$, or simply $|i, z, w\rangle$. In the quantum (resp., randomized) setting, the state of the computation is a complex (resp., nonnegative real) combination of all possible values of the registers. Let $\mathcal{H}$ denote the corresponding finite-dimensional vector space. We denote the state of the computation by a vector $|\psi\rangle \in \mathcal{H}$ over the basis $(|i, z, w\rangle)_{i,z,w}$. Furthermore, the state vectors are unit length for the ℓ_2 norm in the quantum setting and for the ℓ_1 norm in the randomized setting.

A *T-query algorithm* A is specified by a $(T+1)$-tuple $(U_0, U_1, \ldots, U_T)$ of matrices. When A is quantum (resp., randomized), the matrices U_i are unitary (resp., stochastic). The computation takes place as follows. The *query operator* is the unitary (resp., stochastic) matrix O_x that satisfies $O_x|i, z, w\rangle = |i, z \oplus x_i, w\rangle$ for every i, z, w, where by convention $x_0 = 0$. Initially the state is set to some fixed value $|0, 0, 0\rangle$. Then the sequence of transformations $U_0, O_x, U_1, O_x, \ldots, U_{T-1}, O_x, U_T$ is applied.

We say that the algorithm A *ε-computes* a function $f : S \to S'$, for some sets $S \subseteq \Sigma^n$ and S', if the observation of the last bits of the work register equals $f(x)$ with probability at least $1 - \varepsilon$ for every $x \in S$. Then $\mathsf{QQC}(f)$ (resp., $\mathsf{RQC}(f)$) is the minimum query complexity of quantum (resp., randomized) query algorithms that ε_0-compute f, where $\varepsilon_0 = 1/3$.

3. Proof of the main theorem. This section is devoted to the proof of the main theorem. We prove Theorem 1.1 in two main steps. Lemma 3.1 shows how fast the computations diverge when they start on different individual inputs, in terms of the query probabilities. This lemma depends on the model of computation. Lemma 3.2 establishes the relationship between the Kolmogorov complexity of individual positions of the input and the probability that a given algorithm makes a query to this position. This lemma is independent of the model of computation. Theorem 1.1 follows immediately by combining these two lemmas.

In the following two lemmas, let A be an ε-bounded error algorithm for f that makes at most T queries to the input. When A is a randomized algorithm, let $p_t^x(i)$ be the probability that A queries x_i at query t on input x. By analogy, when A is a quantum algorithm, the probability $p_t^x(i)$ is interpreted as the probability of observing i if the query register were measured at query t, that is, the square of the norm of the part of the state that queries x_i. Let $\overline{p}^x(i) = \frac{1}{T}\sum_{t=1}^{T} p_t^x(i)$ be the average query probability over all of the time steps up to time T. We assume henceforth without loss of generality that $\overline{p}^x(i) > 0$. (For example, we start by uniformly querying all positions and reverse the process.)

LEMMA 3.1 (divergence lemma). *For every input $x, y \in S$ such that $f(x) \neq f(y)$ the following hold.*

1. *For quantum algorithms:*

$$2T \sum_{i:x_i \neq y_i} \sqrt{\overline{p}^x(i)\overline{p}^y(i)} \geq 1 - 2\sqrt{\varepsilon(1-\varepsilon)}.$$

2. *For randomized algorithms:*

$$2T \sum_{i:x_i \neq y_i} \min\left(\overline{p}^x(i), \overline{p}^y(i)\right) \geq 1 - 2\varepsilon.$$

We defer the proof of Lemma 3.1 to the end of this section.

The next lemma relates the query probabilities to the Kolmogorov complexity of the strings. In this lemma and the results that follow, we assume that a finite description of the algorithm is given. Using the knowledge of A, we may assume without loss of generality that the function f that it computes is also given, as is the length n of the inputs. With additional care, the additive constants in all of the proofs can be made very small by adding to the auxiliary information made available to the description algorithms those constant-size programs that are described within the proofs.

LEMMA 3.2 (query information lemma). *There exists an absolute constant $c \geq 0$ such that, for every input $x \in S$ and position $i \in \{1, \ldots n\}$,*

$$\mathsf{K}(i|x, A) \leq \log\left(\frac{1}{\overline{p}^x(i)}\right) + c.$$

Proof. Let $\mathcal{S}_x$ be the source where i occurs with probability $\overline{p}^x(i)$. By Proposition 2.7, $\mathsf{K}(i|\mathcal{S}_x) \leq \log(\frac{1}{\overline{p}^x(i)}) + c$ for some absolute constant c. To complete the proof, it suffices to show that $\mathsf{K}(\mathcal{S}_x|x, A) = O(1)$ and apply the second bound of Proposition 2.2. Use x and A to compute the probabilities $(\overline{p}^x(i))_{1 \leq i \leq n}$. The probabilities can be computed in a finite number of steps because the dimension is finite, and the number of queries is bounded by T. □

From these two lemmas we derive the main theorem.

Proof of Theorem 1.1. By Lemma 3.2, there is a constant $c \geq 0$ such that, for any algorithm that makes at most T queries and any x, y, i,

$$\overline{p}^x(i) \leq 2^{-\mathsf{K}(i|x,A)+c} \quad \text{and} \quad \overline{p}^y(i) \leq 2^{-\mathsf{K}(i|y,A)+c}.$$

This is true in particular for all those i where $x_i \neq y_i$. Combining this with Lemma 3.1 concludes the proof of the main theorem with $C = 2^{-c-1}$. □

We now give the proof of Lemma 3.1. The proof of the quantum case is very similar to the proofs found in many papers which give quantum lower bounds on query complexity. To our knowledge, the randomized case is new despite the simplicity of its proof. Whereas Aaronson [1] used a different approach to prove a version of Ambainis's method for randomized algorithms, our lemma allows us to use the same framework to establish lower bounds for both quantum and randomized query complexities.

Proof of Lemma 3.1. Let $|\psi_t^x\rangle$ be the state of the ε-bounded error algorithm A just before the tth oracle query, on input x. By convention, $|\psi_{T+1}^x\rangle$ is the final state. When A is a quantum algorithm, $|\psi_t^x\rangle$ is a unit vector for the ℓ_2 norm; otherwise, it is a probabilistic distribution, that is, a nonnegative and unit vector for the ℓ_1 norm. Observe that the ℓ_1 distance is the total variation distance.

First we prove the quantum case. The starting state of A does not depend on the input, and thus before the first question we have $|\psi_1^x\rangle = |\psi_1^y\rangle$, so $\langle\psi_1^x|\psi_1^y\rangle = 1$. At the end of the computation, if the algorithm is correct with probability ϵ, then $|\langle\psi_{T+1}^x|\psi_{T+1}^y\rangle| \leq 2\sqrt{\epsilon(1-\epsilon)}$ [2]. At each time step, we consider how much the two states can diverge in the following claim, which we will prove after the end of this proof.

Claim 1 (quantum divergence).

$$|\langle\psi_t^x|\psi_t^y\rangle - \langle\psi_{t+1}^x|\psi_{t+1}^y\rangle| \leq 2 \sum_{i:x_i\neq y_i} \sqrt{p_t^x(i)p_t^y(i)}.$$

Over T time steps, the two states diverge as follows. The proof uses only Claim 1 and the Cauchy–Schwartz inequality.

$$\begin{aligned}
1 - 2\sqrt{\varepsilon(1-\varepsilon)} &\leq |\langle\psi_1^x|\psi_1^y\rangle - \langle\psi_{T+1}^x|\psi_{T+1}^y\rangle| \\
&\leq \sum_{t=1}^{T} |\langle\psi_t^x|\psi_t^y\rangle - \langle\psi_{t+1}^x|\psi_{t+1}^y\rangle| \\
&\leq \sum_{t=1}^{T} 2 \sum_{i:x_i\neq y_i} \sqrt{p_t^x(i)p_t^y(i)} \\
&\leq 2 \sum_{i:x_i\neq y_i} \sqrt{\sum_{t=0}^{T-1} p_t^x(i) \sum_{t=0}^{T-1} p_t^y(i)} \\
&= 2T \sum_{i:x_i\neq y_i} \sqrt{\overline{p}^x(i)\overline{p}^y(i)}.
\end{aligned}$$

Now we prove the randomized case. We use the ket notation for real-valued normalized vectors, for consistency in notation. Again, initially $|\psi_1^x\rangle = |\psi_1^y\rangle$. At the end of the computation, if the algorithm is correct with probability ϵ, then $\| \, |\psi_{T+1}^x\rangle - |\psi_{T+1}^y\rangle \, \|_1 \geq 1 - 2\epsilon$. At each time step, the distribution states now diverge according to the following claim, which we will prove after the end of this proof.

Claim 2 (randomized divergence).

$$\begin{aligned}
&\| \, |\psi_{t+1}^x\rangle - |\psi_{t+1}^y\rangle \, \|_1 \\
&\leq \| \, |\psi_t^x\rangle - |\psi_t^y\rangle \, \|_1 + 2 \sum_{i:x_i\neq y_i} \min\left(p_t^x(i), p_t^y(i)\right).
\end{aligned}$$

We now conclude the proof.

$$\begin{aligned}
1 - 2\varepsilon &\leq \sum_{t=1}^{T} \| \, |\psi_{t+1}^x\rangle - |\psi_{t+1}^y\rangle \, \|_1 - \| \, |\psi_t^x\rangle - |\psi_t^y\rangle \, \|_1 \\
&\leq \sum_{t=1}^{T} 2 \sum_{i:x_i\neq y_i} \min\left(p_t^x(i), p_t^y(i)\right) \\
&\leq 2T \sum_{i:x_i\neq y_i} \min\left(\overline{p}^x(i), \overline{p}^y(i)\right). \qquad \square
\end{aligned}$$

Proof of Claim 1. Let

$$\begin{aligned}
|\psi_t^x\rangle &= \sum_{i,z,w} \alpha_{i,z,w}|i,z,w\rangle, \text{ and} \\
|\psi_t^y\rangle &= \sum_{i,z,w} \beta_{i,z,w}|i,z,w\rangle.
\end{aligned}$$

After the tth query is made, the states $|\psi_t'^x\rangle = O_x|\psi_t^x\rangle$ and $|\psi_t'^y\rangle = O_y|\psi_t^y\rangle$ are

$$|\psi_t'^x\rangle = \sum_{i,z,w} \alpha_{i,z,w}|i, z \oplus x_i, w\rangle, \text{ and}$$
$$|\psi_t'^y\rangle = \sum_{i,z,w} \beta_{i,z,w}|i, z \oplus y_i, w\rangle.$$

Now, since the inner product is invariant under unitary transformations, we get

$$\langle\psi_{t+1}^x|\psi_{t+1}^y\rangle = \langle\psi_t'^x|\psi_t'^y\rangle,$$

and therefore

$$\begin{aligned}
&|\langle\psi_t^x|\psi_t^y\rangle - \langle\psi_{t+1}^x|\psi_{t+1}^y\rangle| \\
&= \left|\sum_{i,z,w} \overline{\alpha_{i,z,w}}\beta_{i,z,w} - \sum_{i,z,w} \overline{\alpha_{i,z\oplus x_i,w}}\beta_{i,z\oplus y_i,w}\right| \\
&= \left|\sum_{\substack{i,z,w \\ x_i \neq y_i}} \overline{\alpha_{i,z,w}}\beta_{i,z,w} - \overline{\alpha_{i,z\oplus x_i,w}}\beta_{i,z\oplus y_i,w}\right| \\
&\leq \sum_{i:x_i\neq y_i} \left(\left|\sum_{z,w} \overline{\alpha_{i,z,w}}\beta_{i,z,w}\right| + \left|\sum_{z,w} \overline{\alpha_{i,z\oplus x_i,w}}\beta_{i,z\oplus y_i,w}\right|\right) \\
&\leq 2 \sum_{i:x_i\neq y_i} \sqrt{\left(\sum_{z,w}|\alpha_{i,z,w}|^2\right)\left(\sum_{z,w}|\beta_{i,z,w}|^2\right)} \\
&\leq 2 \sum_{i:x_i\neq y_i} \sqrt{p_t^x(i)p_t^y(i)}. \qquad \square
\end{aligned}$$

Proof of Claim 2. Let us write the distributions using the same formalism as above, that is,

$$|\psi_t^x\rangle = \sum_{i,z,w} \alpha_{i,z,w}|i, z, w\rangle, \text{ and}$$
$$|\psi_t^y\rangle = \sum_{i,z,w} \beta_{i,z,w}|i, z, w\rangle.$$

Note that now the vectors are unit for the ℓ_1 norm. After the tth query is made, the states $|\psi_t'^x\rangle = O_x|\psi_t^x\rangle$ and $|\psi_t'^y\rangle = O_y|\psi_t^y\rangle$ are

$$|\psi_t'^x\rangle = \sum_{i,z,w} \alpha_{i,z,w}|i, z \oplus x_i, w\rangle, \text{ and}$$
$$|\psi_t'^y\rangle = \sum_{i,z,w} \beta_{i,z,w}|i, z \oplus y_i, w\rangle.$$

Now, since the ℓ_1 distance does not increase under stochastic matrices, we get

$$\| \, |\psi_{t+1}^x\rangle - |\psi_{t+1}^y\rangle \, \|_1 \leq \| \, |\psi_t'^x\rangle - |\psi_t'^y\rangle \, \|_1,$$

and therefore

$$\begin{aligned}
&\| \, |\psi_{t+1}^x\rangle - |\psi_{t+1}^y\rangle \, \|_1 \\
&= \left\| \sum_{i,z,w} (\alpha_{i,z,w}|i, z \oplus x_i, w\rangle - \beta_{i,z,w}|i, z \oplus y_i, w\rangle) \right\|_1 \\
&= \sum_i \left\| \sum_{z,w} (\alpha_{i,z,w}|i, z \oplus x_i, w\rangle - \beta_{i,z,w}|i, z \oplus y_i, w\rangle) \right\|_1 .
\end{aligned}$$

We now bound each term of the last sum separately. Fix any i. If $x_i = y_i$, then

$$\left\| \sum_{z,w} (\alpha_{i,z,w}|i, z \oplus x_i, w\rangle - \beta_{i,z,w}|i, z \oplus y_i, w\rangle) \right\|_1 = \sum_{z,w} |\alpha_{i,z,w} - \beta_{i,z,w}|.$$

If $x_i \neq y_i$, then

$$\begin{aligned}
&\left\| \sum_{z,w} (\alpha_{i,z,w}|i, z \oplus x_i, w\rangle - \beta_{i,z,w}|i, z \oplus y_i, w\rangle) \right\|_1 \\
&\leq \left\| \sum_{z,w} (\alpha_{i,z,w}|i, z \oplus y_i, w\rangle - \beta_{i,z,w}|i, z \oplus y_i, w\rangle) \right\|_1 \\
&\quad + \left\| \sum_{z,w} (\alpha_{i,z,w}|i, z \oplus x_i, w\rangle - \alpha_{i,z,w}|i, z \oplus y_i, w\rangle) \right\|_1 \\
&\leq \sum_{z,w} |\alpha_{i,z,w} - \beta_{i,z,w}| + 2 \sum_{z,w} |\alpha_{i,z,w}| \\
&= \sum_{z,w} |\alpha_{i,z,w} - \beta_{i,z,w}| + 2p_t^x(i).
\end{aligned}$$

In the same way we can prove that

$$\begin{aligned}
&\left\| \sum_{z,w} (\alpha_{i,z,w}|i, z \oplus x_i, w\rangle - \beta_{i,z,w}|i, z \oplus y_i, w\rangle) \right\|_1 \\
&\leq \sum_{z,w} |\alpha_{i,z,w} - \beta_{i,z,w}| + 2p_t^y(i).
\end{aligned}$$

We group together these upper bounds and conclude that

$$\begin{aligned}
&\| \, |\psi_{t+1}^x\rangle - |\psi_{t+1}^y\rangle \, \|_1 \\
&\leq \sum_{i,z,w} |\alpha_{i,z,w} - \beta_{i,z,w}| + 2 \sum_{i : x_i \neq y_i} \min \left(p_t^x(i), p_t^y(i) \right) \\
&= \| \, |\psi_t^x\rangle - |\psi_t^y\rangle \, \|_1 + 2 \sum_{i : x_i \neq y_i} \min \left(p_t^x(i), p_t^y(i) \right) . \qquad \square
\end{aligned}$$

4. Comparison with previous adversary methods. In this section, we reprove, as a corollary of Theorem 1.1, the previously known adversary lower bounds. Our framework also allows us to obtain somewhat stronger statements for free.

To obtain the previously known adversary methods as a corollary of Theorem 1.1, we must give a lower bound on terms $\mathsf{K}(i|x,A)$ and $\mathsf{K}(i|y,A)$. To this end, we apply Proposition 2.3 and give a lower bound on $\mathsf{K}(x,y)$ and upper bounds on $\mathsf{K}(x|i,y)$ and $\mathsf{K}(y|i,x)$. The lower bound on $\mathsf{K}(x,y)$ is obtained by applying Lemma 2.6, a consequence of Shannon's coding theorem, for an appropriate distribution. The upper bounds on $\mathsf{K}(x|i,y)$ and $\mathsf{K}(y|i,x)$ are obtained using the Shannon–Fano code for appropriate distributions.

The following lemma is the general formulation of the sketch above.

LEMMA 4.1. *There exists a constant $C>0$ such that the following holds. Let Σ be a finite set, let $n\geq 1$ be an integer, and let $S\subseteq\Sigma^n$. Let q be a probability distribution on S^2, let p be a probability distribution on S, and let $\{p'_{x,i} : x\in S, 1\leq i\leq n\}$ be a family of probability distributions on S. Assume that whenever $q(x,y)\neq 0$, then $p(x)$, $p(y)$, $p'_{y,i}(x)$, and $p'_{x,i}(y)$ are nonzero for every i such that $x_i\neq y_i$. Then for every finite string σ there exist $x,y\in S$, with $q(x,y)\neq 0$, such that*

$$\frac{1}{\sum_{i:x_i\neq y_i}\sqrt{2^{-\mathsf{K}(i|x,\sigma)-\mathsf{K}(i|y,\sigma)}}} \geq C\times\min_{i:x_i\neq y_i}\left(\frac{\sqrt{p(x)p'_{x,i}(y)\ p(y)p'_{y,i}(x)}}{q(x,y)}\right),$$

and (for the same $x,y\in S$)

$$\frac{1}{\sum_{i:x_i\neq y_i}\min\left(2^{-\mathsf{K}(i|x,\sigma)},2^{-\mathsf{K}(i|y,\sigma)}\right)} \geq C\times\min_{i:x_i\neq y_i}\left(\max\left(\frac{p(x)p'_{x,i}(y)}{q(x,y)},\frac{p(y)p'_{y,i}(x)}{q(x,y)}\right)\right).$$

Proof. In this proof, $c_1,\ldots,c_5$ are some appropriate nonnegative constants. By Lemma 2.6, there exists a pair (x,y) such that $q(x,y)\neq 0$ and

$$\mathsf{K}(x,y|\sigma,p,p')\geq\log\left(\frac{1}{q(x,y)}\right),$$

where p' stands for a complete description of all of the $p'_{x,i}$.

Fix x and y so that this holds. By using the Shannon–Fano code (Proposition 2.5),

$$\mathsf{K}(x|p)\leq\log\left(\frac{1}{p(x)}\right)+c_1$$

and

$$\mathsf{K}(y|x,i,p'_{x,i})\leq\log\left(\frac{1}{p'_{x,i}(y)}\right)+c_1$$

for any i such that $x_i \neq y_i$. By Proposition 2.3,

$$\begin{aligned}
&\mathsf{K}(i|x,\sigma)\\
&\geq \mathsf{K}(i|x,\sigma,p,p') - c_3\\
&\geq \mathsf{K}(x,y|\sigma,p,p') - \mathsf{K}(x|p) - \mathsf{K}(y|i,x,p'_{x,i})\\
&\quad + \mathsf{K}(i|x,y,\mathsf{K}(x,y),\sigma,p,p') - c_4\\
&\geq \log\left(\frac{1}{q(x,y)}\right) - \log\left(\frac{1}{p(x)}\right) - \log\left(\frac{1}{p'_{x,i}(y)}\right)\\
&\quad + \mathsf{K}(i|x,y,\mathsf{K}(x,y),\sigma,p,p') - c_5\\
&= \log\left(\frac{p(x)p'_{x,i}(y)}{q(x,y)}\right) + \mathsf{K}(i|x,y,\mathsf{K}(x,y),\sigma,p,p') - c_5.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\mathsf{K}(i|y,\sigma) \geq \log&\left(\frac{p(y)p'_{y,i}(x)}{q(x,y)}\right)\\
&+ \mathsf{K}(i|x,y,\mathsf{K}(x,y),\sigma,p,p') - c_5.
\end{aligned}$$

To conclude, consider the sum

$$\begin{aligned}
&\frac{1}{\sum_{i:x_i\neq y_i}\sqrt{2^{-\mathsf{K}(i|x,\sigma)-\mathsf{K}(i|y,\sigma)}}}\\
&\geq \frac{1}{\sum_{i:x_i\neq y_i}\sqrt{2^{-\log\left(\frac{p(x)p'_{x,i}(y)}{q(x,y)}\right)-\log\left(\frac{p(y)p'_{y,i}(x)}{q(x,y)}\right)-2\mathsf{K}(i|x,y,\mathsf{K}(x,y),\sigma,p,p')+2c_5}}}\\
&\geq \frac{1}{\sum_{i:x_i\neq y_i} 2^{c_5}\sqrt{\frac{q(x,y)}{p(x)p'_{x,i}(y)}\frac{q(x,y)}{p(y)p'_{y,i}(x)}}2^{-\mathsf{K}(i|x,y,\mathsf{K}(x,y),\sigma,p,p')}}\\
&\geq 2^{-c_5}\min_{i:x_i\neq y_i}\left(\frac{\sqrt{p(x)p'_{x,i}(y)p(y)p'_{y,i}(x)}}{q(x,y)}\right)\frac{1}{\sum_{i:x_i\neq y_i}2^{-\mathsf{K}(i|x,y,\mathsf{K}(x,y),\sigma,p,p')}}.
\end{aligned}$$

We apply Kraft's inequality (Proposition 2.4) to show that $\sum_{i:x_i\neq y_i} 2^{-\mathsf{K}(i|x,y,\mathsf{K}(x,y),\sigma,p,p')} \leq 1$. This concludes the proof of the first part of the lemma using Kraft's inequality and letting $C = 2^{-c_5}$. The second part is similar. ∎

4.1. Ambainis's weighted scheme.

THEOREM 4.2 (Ambainis's weighted method). *Let Σ be a finite set, let $n \geq 1$ be an integer, and let $S \subseteq \Sigma^n$ and S' be sets. Let $f : S \to S'$. Consider a weight scheme as follows:*

- *Every pair $(x,y) \in S^2$ is assigned a nonnegative weight $w(x,y)$ such that $w(x,y) = 0$ whenever $f(x) = f(y)$.*
- *Every triple (x,y,i) is assigned a nonnegative weight $w'(x,y,i)$ such that $w'(x,y,i) = 0$ whenever $x_i = y_i$ or $f(x) = f(y)$.*

For all x, i, let

$$wt(x) = \sum_y w(x,y) \quad \textit{and}$$
$$v(x,i) = \sum_y w'(x,y,i).$$

If $w'(x,y,i)w'(y,x,i) \geq w^2(x,y)$ *for all* x,y,i *such that* $x_i \neq y_i$, *then*

$$\mathsf{QQC}(f) = \Omega\left(\min_{\substack{x,y,i \\ w(x,y)\neq 0, x_i \neq y_i}} \left(\sqrt{\frac{wt(x)wt(y)}{v(x,i)v(y,i)}}\right)\right).$$

Furthermore, if $w'(x,y,i), w'(y,x,i) \geq w(x,y)$ *for all* x,y,i *such that* $x_i \neq y_i$, *then*

$$\mathsf{RQC}(f) = \Omega\left(\min_{\substack{x,y,i \\ w(x,y)\neq 0, x_i \neq y_i}} \left(\max\left(\frac{wt(x)}{v(x,i)}, \frac{wt(y)}{v(y,i)}\right)\right)\right).$$

The relation in Ambainis's original statement is implicit in this formulation, since it corresponds to the nonzero-weight pairs. A weaker version of the randomized case was proven independently by Aaronson [1] using a completely different approach. We show that Theorem 4.2 follows from Theorem 1.1.

Proof. We derive probability distributions q, p, p' from the weight schemes as follows. Let $W = \sum_{x,y} w(x,y)$. Define

$$\begin{aligned} q(x,y) &= \frac{w(x,y)}{W}, \\ p(x) &= \frac{wt(x)}{W}, \\ p'_{x,i}(y) &= \frac{w'(x,y,i)}{v(x,i)} \quad \text{for any } x,y,i. \end{aligned}$$

It is easy to check that, by construction and hypothesis, these distributions satisfy the conditions of Lemma 4.1. We may now rearrange and simplify the terms as follows:

$$\begin{aligned} \frac{\sqrt{p(x)p'_{x,i}(y)\ p(y)p'_{y,i}(x)}}{q(x,y)} &= \frac{\sqrt{\frac{wt(x)}{W}\frac{w'(x,y,i)}{v(x,i)}\ \frac{wt(y)}{W}\frac{w'(y,x,i)}{v(y,i)}}}{\frac{w(x,y)}{W}} \\ &= \frac{\sqrt{\frac{wt(x)}{v(x,i)}\ \frac{wt(y)}{v(y,i)} w'(x,y,i)w'(y,x,i)}}{w(x,y)} \\ &\geq \sqrt{\frac{wt(x)}{v(x,i)}\ \frac{wt(y)}{v(y,i)}}. \end{aligned}$$

The final line follows from the hypothesis $w'(x,y,i)w'(y,x,i) \geq w^2(x,y)$. The second part of the theorem is obtained by similar rearrangement and simplification. ∎

We conclude this section by sketching the proof of the unweighted version of Ambainis's adversary method, as it affords a simpler combinatorial proof that does not require Lemma 4.1. To simplify notation we omit additive constants and the usual auxiliary strings including A.

Let $R \subseteq S \times S$ be a relation on pairs of instances, where $(x,y) \in R \Longrightarrow f(x) \neq f(y)$, and let R_i be the restriction of R to pairs x,y for which $x_i \neq y_i$. Viewing the relation R as a bipartite graph, let l, l', m, m' be as follows:

- m is a lower bound on the degree of all $x \in X$,
- m' is a lower bound on the degree of all $y \in Y$,
- for any fixed x and $i, 1 \leq i \leq n$, the number of y adjacent to x for which $x_i \neq y_i$ is at most l,

- for any fixed y and $i, 1 \le i \le n$, the number of x adjacent to y for which $x_i \neq y_i$ is at most l'.

We make the following observations:

1. $|R| \ge \max\{m|X|, m'|Y|\}$, so $\exists x, y \in R$ such that $\mathsf{K}(x,y) \ge \max(\log(m|X|), \log(m'|Y|))$.
2. For all $x \in X, \mathsf{K}(x) \le \log(|X|)$, and $\mathsf{K}(y) \le \log(|Y|)$ for all $y \in Y$.
3. For all x, y, i with $(x,y) \in R_i, \mathsf{K}(y|i,x) \le \log(l)$ and similarly $\mathsf{K}(x|i,y) \le \log(l')$.

For any i with $x_i \neq y_i$, by Proposition 2.3,

$$\begin{aligned}\mathsf{K}(i|x) &\ge \mathsf{K}(x,y) - \mathsf{K}(x) - \mathsf{K}(y|i,x) \\ &\quad + \mathsf{K}(i|x,y,\mathsf{K}(x,y)) \\ &\ge \log(m|X|) - \log(|X|) - \log(l) \\ &\quad + \mathsf{K}(i|x,y,\mathsf{K}(x,y)) \\ &= \log\left(\frac{m}{l}\right) + \mathsf{K}(i|x,y,\mathsf{K}(x,y)).\end{aligned}$$

The same proof works to show that $\mathsf{K}(i|y) \ge \log(\frac{m'}{l'}) + \mathsf{K}(i|x,y,\mathsf{K}(x,y))$. By Theorem 1.1 and Kraft's inequality,

$$\mathsf{QQC}(f) = \Omega\left(\sqrt{\frac{mm'}{ll'}}\right).$$

4.2. Spectral lower bound. We now show how to prove the spectral lower bound of Barnum, Saks, and Szegedy [5] as a corollary of Theorem 1.1. Recall that for any matrix Γ, $\lambda(\Gamma)$ is the largest eigenvalue of Γ.

THEOREM 4.3 (Barnum–Saks–Szegedy spectral method). *Let Σ be a finite set, let $n \ge 1$ be an integer, and let $S \subseteq \Sigma^n$ and S' be sets. Let $f : S \to S'$. Let Γ be an arbitrary $S \times S$ nonnegative real symmetric matrix that satisfies $\Gamma(x,y) = 0$ whenever $f(x) = f(y)$. For $i = 1, \ldots, n$ let Γ_i be the matrix:*

$$\Gamma_i(x,y) = \begin{cases} 0 & \text{if } x_i = y_i, \\ \Gamma(x,y) & \text{otherwise.} \end{cases}$$

Then

$$\mathsf{QQC}(f) = \Omega\left(\frac{\lambda(\Gamma)}{\max_i \lambda(\Gamma_i)}\right).$$

Proof. Since Γ and Γ_i are nonnegative real symmetric matrices, they have an eigenvector with only nonnegative real entries for their respective largest eigenvalues. Let $|\alpha\rangle$ (resp., $|\alpha_i\rangle$) be this unit eigenvector of Γ (resp., Γ_i). We define the probability distributions q, p, p' as follows:

$$\begin{aligned} q(x,y) &= \frac{\Gamma(x,y)\langle x|\alpha\rangle\langle y|\alpha\rangle}{\langle\alpha|\Gamma|\alpha\rangle}, \\ p(x) &= \langle x|\alpha\rangle^2, \\ p'_{x,i}(y) &= \frac{\Gamma_i(x,y)\langle y|\alpha_i\rangle}{\langle x|\Gamma_i|\alpha_i\rangle}, \quad \text{for any } x, y, i. \end{aligned}$$

First we check that these are probability distributions. Distribution p also has weight 1 because $|\alpha\rangle$ is a unit vector. Since $|\alpha\rangle$ and $|y\rangle$ have real entries, $\langle y|\alpha\rangle = \langle\alpha|y\rangle$.

Then the distribution q has weight $\frac{1}{\langle\alpha|\Gamma|\alpha\rangle}\sum_{x,y}\langle\alpha|y\rangle\Gamma(x,y)\langle x|\alpha\rangle$, which is 1 since $\sum_x \Gamma(x,y)\langle x|\alpha\rangle = \langle y|\Gamma|\alpha\rangle$. Using the same argument, $p'_{x,i}$ also has weight 1.

Now, fix any x, y, i such that $x_i \neq y_i$ and $q(x,y) \neq 0$. Note that $\langle\alpha|\Gamma|\alpha\rangle = \lambda(\Gamma)$, $\Gamma_i|\alpha_i\rangle = \lambda(\Gamma_i)|\alpha_i\rangle$, and $\Gamma(x,y) = \Gamma_i(x,y)$. Then the fractions $\frac{p(x)p'_{x,i}(y)}{q(x,y)}$ and $\frac{p(y)p'_{y,i}(x)}{q(x,y)}$ are, respectively, $\frac{\lambda(\Gamma)}{\lambda(\Gamma_i)}\frac{\langle y|\alpha_i\rangle}{\langle x|\alpha_i\rangle}\frac{\langle x|\alpha\rangle}{\langle y|\alpha\rangle}$ and $\frac{\lambda(\Gamma)}{\lambda(\Gamma_i)}\frac{\langle x|\alpha_i\rangle}{\langle y|\alpha_i\rangle}\frac{\langle y|\alpha\rangle}{\langle x|\alpha\rangle}$. Taking the square root of their product gives the result using Lemma 4.1. □

5. Certificate complexity and adversary techniques. Let f be a Boolean function. For any positive instance $x \in \Sigma^n$ of f ($f(x)$=1), a *positive certificate* for $f(x)$ is the smallest subset of indices $I \subseteq [n]$ of x such that, for any y with $x_i = y_i$ for all $i \in I$, $f(y)$=1.

The 1-*certificate complexity* of f, denoted $C_1(f)$, is the size of the largest positive certificate for $f(x)$, over all positive instances x. The 0-*certificate complexity* is defined similarly for negative instances x of f ($f(x) = 0$).

Prior to our work, it was known that the best possible bound that could be proven using the unweighted adversary technique for total functions [2, Theorem 5.1] is $O(\sqrt{C_0(f)C_1(f)})$. Independently, Szegedy [20] showed that the best possible lower bound using the spectral method is $O(\min(\sqrt{nC_0(f)}, \sqrt{nC_1(f)}))$ for arbitrary functions, and Zhang [22] proved the same for Ambainis's weighted method.

The following lemma, due to Troy Lee, results in a very simple proof of the fact that our method and, hence, all of the known variants of the adversary method have lower bounds larger than $\min(\sqrt{nC_0(f)}, \sqrt{nC_1(f)})$ for arbitrary functions.

LEMMA 5.1. *There exists a constant $c \geq 0$ such that the following holds. Let Σ be a finite set, let $n \geq 1$ be an integer, and let $S \subseteq \Sigma^n$ be a set. Let $f : S \to \{0,1\}$. For every $x, y \in S$ with $f(x) = 0$ and $f(y) = 1$, there is an i_0 with $x_{i_0} \neq y_{i_0}$ for which $\mathsf{K}(i_0|x,f) \leq \log(C_0(f)) + c$, and similarly there is an i_1 with $x_{i_1} \neq y_{i_1}$ such that $\mathsf{K}(i_1|y,f) \leq \log(C_1(f)) + c$.*

Proof. Among the negative certificates for $f(x)$, let I be the lexicographically smallest one. By definition of the 0-certificate complexity, the size of I is at most $C_0(f)$. Since $f(x) \neq f(y)$, x and y must differ on some $i_0 \in I$. To describe i_0 given x, it suffices to give an index into I, which requires at most $\log(C_0(f)) + c$ bits. The same can also be done for y and $C_1(f)$. □

THEOREM 5.2. *Let Σ be a finite set, let $n \geq 1$ be an integer, and let $S \subseteq \Sigma^n$ be a set. Let $f : S \to \{0,1\}$. Then any quantum query lower bound for f given by Theorem* 1.1 *is in $O(\min(\sqrt{nC_0(f)}, \sqrt{nC_1(f)}))$.*

Proof. Let A be a quantum algorithm that computes f with bounded error by making at most T queries to the input and $x, y \in S$ such that $f(x) = 0$ and $f(y) = 1$. Then a description of f can be obtained from a description of A, so $\mathsf{K}(i|x,A) \leq \mathsf{K}(i|x,f) + O(1)$. By Lemma 5.1, there exists i_0 such that $x_{i_0} \neq y_{i_0}$, and $\mathsf{K}(i_0|x,f) \leq \log(C_0(f)) + O(1)$. For any $i, 1 \leq i \leq n$, $\mathsf{K}(i|y,A) \leq \log(n) + O(1)$. Therefore $K(i_0|x,A) + K(i_0|y,A) \leq \log(nC_0(f)) + O(1)$.

The lower bound given by Theorem 1.1 is $O\big(\frac{1}{\sum_{i:x_i\neq y_i}\sqrt{2^{-\mathsf{K}(i|x,A)-\mathsf{K}(i|y,A)}}}\big)$. Since $\sum_{i:x_i\neq y_i}\sqrt{2^{-\mathsf{K}(i|x,A)-\mathsf{K}(i|y,A)}} \geq \sqrt{2^{-\mathsf{K}(i_0|x,A)-\mathsf{K}(i_0|y,A)}}$, the bound is $O(\sqrt{nC_0(f)})$ Similarly, it can be shown that the bound is $O(\sqrt{nC_1(f)})$. □

In recent work, Špalek and Szegedy showed that, for total functions, the best lower bound one can achieve with any of the adversary methods is $\sqrt{C_0(f)C_1(f)}$ for any total function [19].

5.1. Applications to graph properties. Theorem 1.1 provides a simple and intuitive method to prove lower bounds for specific problems. We illustrate this by giving lower bounds for two graph properties: connectivity and bipartiteness. These are direct applications of Theorem 1.1 in that we analyze directly the complexity $\mathsf{K}(i|x, A)$ without defining relations or weights or distributions: We need only to consider a "typical" hard pair of instances. In this section, we omit additive and multiplicative constants that result from using small, constant-size programs, as well as the constant length auxiliary string A to simplify the proofs.

We consider graphs over n vertices $\{0, 1, \ldots, n-1\}$, where the graph is represented as an adjacency matrix.

5.1.1. Graph connectivity.

THEOREM 5.3 (see [12]). $\mathsf{QQC}(\textsc{GraphConnectivity}) = \Omega(n^{3/2})$.

Proof. We construct one negative and one positive instance of graph connectivity, using the incompressibility method, using the ideas of [12]. Let S be an incompressible string of length $\log(n-1)! + \log\binom{n}{2}$, chopped into two pieces S_1 and S_2 of length $\log(n-1)!$ and $\log\binom{n}{2}$, respectively. We think of S_1 as representing a Hamilton cycle $C = (\pi(0), \pi(1) \ldots \pi(n-1), \pi(0))$ through the n vertices, where π is a permutation over $\{0, 1, \ldots, n-1\}$ such that $\pi(0) = 0$. Let G contain the cycle C, so that $\mathsf{K}(G) = \mathsf{K}(\pi)$. We also think of S_2 as representing a pair of distinct vertices s, t. Let H be obtained from G by breaking the cycle into two cycles at s and t, that is, $H = G \setminus \{(\pi(s), \pi(s+1)), (\pi(t), \pi(t+1))\} \cup \{(\pi(s), \pi(t+1)), (\pi(s+1), \pi(t))\}$, where addition is modulo n.

We show that, for the four edges e where G and H differ, $\mathsf{K}(e|G) + \mathsf{K}(e|H) \geq 3\log n - 4$. Let e_-, e'_- be the edges removed from G and e_+, e'_+ be the edges added to G. Observe that, up to an additive constant, $\mathsf{K}(e_+|G) = \mathsf{K}(e'_+|G)$ and $\mathsf{K}(e_-|H) = \mathsf{K}(e'_-|H)$.

Assume without loss of generality that $e_- = (\pi(s), \pi(s+1))$ and that the smallest cycle of H contains $\pi(s)$. Let l be the length of this cycle. Observe that $\mathsf{K}(s|G) = \mathsf{K}(e_-|G)$ and $\mathsf{K}(e_-|H) = \mathsf{K}(\pi, s, t|H)$.

$$\begin{aligned}
\log(n-1)! + \log\binom{n}{2} &\leq \mathsf{K}(S) \\
&\leq \mathsf{K}(G) + \mathsf{K}(s|G) + \mathsf{K}(t|G) \\
&\leq \mathsf{K}(G) + \mathsf{K}(e_-|G) + \log n, \\
\mathsf{K}(e_-|G) &\geq \log\binom{n}{2} - \log n = \log\frac{n-1}{2}.
\end{aligned}$$

Furthermore,

$$\begin{aligned}
\mathsf{K}(H) &\leq \mathsf{K}(l) + \log\frac{(n-1)!}{(n-l)!} + \log(n-l-1)! \\
&\leq \log\left(\frac{n}{2}\right) + \log(n-1)! - \log(n-l) \\
&\leq \log(n-1)!\,.
\end{aligned}$$

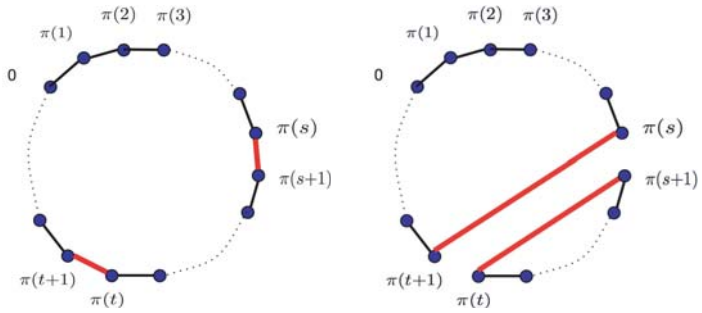

FIG. 5.1. *Graphs G, H for the graph lower bounds.*

Therefore,

$$\begin{aligned}\log(n-1)! + \log\binom{n}{2} &\le \mathsf{K}(S)\\ &\le \mathsf{K}(H) + \mathsf{K}(\pi, s, t|H)\\ &\le \mathsf{K}(H) + \mathsf{K}(e_-|H)\\ &\le \log(n-1)! + \mathsf{K}(e_-|H),\\ \mathsf{K}(e_-|H) &\ge \log\binom{n}{2}.\end{aligned}$$

For the added edges, e_+, e'_+, consider without loss of generality $e_+ = (\pi(s), \pi(t+1))$. Since S is incompressible, $\mathsf{K}(e_+|G) = \mathsf{K}(s,t|G) \ge \log\binom{n}{2}$. Furthermore, $\mathsf{K}(S) \le \mathsf{K}(H) + \mathsf{K}(e_+|H) + \mathsf{K}(e'_+|H)$ and $\mathsf{K}(e'_+|H) \le \log n$, so $\mathsf{K}(e_+|H) \ge \log\binom{n}{2} - \log n = \log\frac{n-1}{2}$. The same proof shows that $\mathsf{K}(e'_+|H) \ge \log\frac{n-1}{2}$. ∎

5.1.2. Bipartiteness. The following lower bound was proven by Dürr and independently in [22].

THEOREM 5.4. $\mathsf{QQC}(\textsc{Bipartiteness}) = \Omega(n^{3/2})$.

Proof. The proof is similar to the one of Theorem 5.3 except that we construct G to be an even cycle on $n = 2m$ vertices and H will be composed of two odd cycles on the same vertex set (see Figure 5.1).

Let S be an incompressible string of length $\log(n-1)! + \log(\binom{n}{2} - 1)$, chopped into two pieces S_1 and S_2 of length $\log(n-1)!$ and $\log(\binom{n}{2} - 1)$, respectively. We think of S_1 as representing a Hamilton cycle $C = (\pi(0) = 0, \pi(1) \dots \pi(n-1), \pi(0))$ through the n vertices and S_2 as representing a pair of distinct vertices s, t, with $s \not\equiv t \pmod 2$. Let G contain the cycle C, and let H be obtained from G by breaking the cycle into two odd cycles at s and t, that is, $H = G \setminus \{(\pi(s), \pi(s+1)), (\pi(t), \pi(t+1))\} \cup \{(\pi(s), \pi(t+1)), (\pi(s+1), \pi(t))\}$.

The same analysis as Theorem 5.3 yields the lower bound $\mathsf{QQC}(\textsc{Bipartiteness}) = \Omega(n^{3/2})$, as claimed. ∎

Acknowledgments. We thank Troy Lee, Christoph Dürr for many useful discussions, and Andris Ambainis for his helpful answers to our questions.

REFERENCES

[1] S. Aaronson, *Lower bounds for local search by quantum arguments*, SIAM J. Comput., 35 (2006), pp. 804–824.
[2] A. Ambainis, *Quantum lower bounds by quantum arguments*, J. Comput. System Sci., 64 (2002), pp. 750–767.
[3] A. Ambainis, *Polynomial degree vs. quantum query complexity*, in Proceedings of the 44th IEEE Symposium on Foundations of Computer Science, 2003, pp. 230–239.
[4] L. Babai and S. Laplante, *Stronger separations for random-self-reducibility, rounds, and advice*, in Proceedings of the IEEE Conference on Computational Complexity, 1999, pp. 98–104.
[5] H. Barnum, M. Saks, and M. Szegedy, *Quantum query complexity and semi-definite programming*, in Proceedings of the 18th IEEE Conference on Computational Complexity, 2003, pp. 179–193.
[6] H. Barnum and M. Saks, *A lower bound on the quantum query complexity of read-once functions*, J. Comput. System Sci., 69 (2004), pp. 244–258.
[7] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. Wolf, *Quantum lower bounds by polynomials*, J. ACM, 48 (2001), pp. 778–797.
[8] E. Bernstein and U. Vazirani, *Quantum complexity theory*, SIAM J. Comput., 26 (1997), pp. 1411–1473.
[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley-Interscience, New York, 1991.
[10] D. Deutsch and R. Jozsa, *Rapid solution of problems by quantum computation*, Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci., 439 (1992), pp. 553–558.
[11] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. R. Soc. of Lond. Ser. A Math. Phys. Eng. Sci., 400 (1985), pp. 97–117.
[12] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla, *Quantum query complexity of some graph problems*, SIAM J. Comput., 35 (2006), pp. 1310–1328.
[13] J. Feigenbaum, L. Fortnow, S. Laplante, and A. V. Naik, *On coherence, random-self-reducibility, and self-correction*, Comput. Complexity, 7 (1998), pp. 174–191.
[14] L. Grover, *A fast quantum mechanical algorithm for database search*, in Proceedings of the 28th ACM Symposium on Theory of Computing, 1996, pp. 212–219.
[15] P. Høyer, J. Neerbek, and Y. Shi, *Quantum complexities of ordered searching, sorting, and element distinctness*, Algorithmica, 34 (2002), pp. 429–448.
[16] S. Laplante, T. Lee, and M. Szegedy, *The quantum adversary method and classical formula size lower bounds*, Comput. Complexity, 16 (2006), pp. 163–196.
[17] M. Li and P. Vitányi, *An introduction to Kolmogorov complexity and its applications*, in Graduate Texts in Computer Science, 2nd ed., Springer, New York, 1997.
[18] D. Simon, *On the power of quantum computation*, SIAM J. Comput., 26 (1997), pp. 1474–1483.
[19] R. Špalek and M. Szegedy, *All quantum adversary methods are equivalent*, Theory Comput., 2 (2006), pp. 1–18.
[20] M. Szegedy, *On the quantum query complexity of detecting triangles in graphs*, Technical report quant-ph/0310107, arXiv archive, 2003.
[21] A. Yao, *Probabilistic computations: Toward a unified measure of complexity*, in Proceedings of the 18th IEEE Symposium on Foundations of Computer Science, 1977, pp. 222–227.
[22] S. Zhang, *On the power of Ambainis lower bounds*, Theoret. Comput. Sci., 339 (2005), pp. 241–256.