Adversary Lower Bounds for Nonadaptive Quantum Algorithms

Pascal Koiran[1], Jürgen Landes[2], Natacha Portier[1], and Penghui Yao[3]

[1] LIP*, Ecole Normale Supérieure de Lyon, Université de Lyon
{Pascal.Koiran,Natacha.Portier}@ens-lyon.fr
[2] School of Mathematics, University of Manchester
juergen_landes@yahoo.de
[3] State Key Laboratory of Computer Science, Chinese Academy of Sciences
phyao1985@gmail.com

Abstract. We present general methods for proving lower bounds on the query complexity of nonadaptive quantum algorithms. Our results are based on the adversary method of Ambainis.

1 Introduction

In this paper we present general methods for proving lower bounds on the query complexity of nonadaptive quantum algorithms. A nonadaptive algorithm makes all its queries simultaneously. By contrast, an unrestricted (adaptive) algorithm may choose its next query based on the results of previous queries. In classical computing, classes of problems for which adaptivity does not help have been identified [4, 10] and it is known that this question is connected to a longstanding open problem [15] (see [10] for a more extensive discussion). In quantum computing, the study of nonadaptive algorithms seems especially relevant since some of the best known quantum algorithms (namely, Simon's algorithms and some other hidden subgroup algorithms) are nonadaptive. This is nevertheless a rather understudied subject in quantum computing.

The paper that is most closely related to the present work is [14] (and [8] is another related paper). In [14] the authors use an "algorithmic argument" (this is a kind of Kolmogorov argument) to give lower bounds on the nonadaptive quantum query complexity of ordered search, and of generalizations of this problem. The model of computation that they consider is less general than ours (more on this in section 2).

The two methods that have proved most successful in the quest for quantum lower bounds are the polynomial method (see for instance [5, 2, 11, 12]) and the adversary method of Ambainis. It is not clear how the polynomial method might take the nonadaptivity of algorithms into account. Our results are therefore based on the adversary method, in its weighted version [3]. We provide

* UMR 5668 ENS Lyon, CNRS, UCBL associée à l'INRIA. Work done when Landes and Yao were visiting LIP with financial support from the program MEST-CT-2004-504029 MATHLOGAPS.

W. Hodges and R. de Queiroz (Eds.): WoLLIC 2008, LNAI 5110, pp. 226–237, 2008.

two general lower bounds which yield optimal results for a number of problems: search in an ordered or unordered list, element distinctness, graph connectivity or bipartiteness. To obtain our first lower bound we treat the list of queries performed by a nonadaptive algorithm as one single "super query". We can then apply the adversary method to this 1-query algorithm. Interestingly, the lower bound that we obtain is very closely related to the lower bounds on *adaptive* probabilistic query complexity due to Aaronson [1], and to Laplante and Magniez [13]. Our second lower bound requires a detour through the so-called minimax (dual) method and is based on the fact that in a nonadaptive algorithm, the probability of performing any given query is independent of the input.

2 Definition of the Model

In the black box model, an algorithm accesses its input by querying a function x (the *black box*) from a finite set Γ to a (usually finite) set Σ. At the end of the computation, the algorithm decides to accept or reject x, or more generally produces an output in a (usually finite) set S'. The goal of the algorithm is therefore to compute a (partial) function $F : S \to S'$, where $S = \Sigma^\Gamma$ is the set of black boxes. For example, in the *Unordered Search* problem $\Gamma = [N] = \{1, \ldots, N\}$, $\Sigma = \{0, 1\}$ and F is the OR function: $F(x) = \bigvee_{1 \le i \le N} x(i)$.

Our second example is *Ordered Search*. The sets Γ and Σ are as in the first example, but F is now a partial function: we assume that the black box satisfies the promise that there exists an index i such that $x(j) = 1$ for all $j \ge i$, and $x(j) = 0$ for all $j < i$. Given such an x, the algorithm tries to compute $F(x) = i$.

A quantum algorithm $\mathcal{A}$ that makes T queries can be formally described as a tuple $(U_0, \ldots, U_T)$, where each U_i is a unitary operator. For $x \in S$ we define the unitary operator O_x (the "call to the black box") by $O_x|i\rangle|\varphi\rangle|\psi\rangle = |i\rangle|\varphi \oplus x(i)\rangle|\psi\rangle$. The algorithm $\mathcal{A}$ computes the final state $U_T O_x U_{T-1} \ldots U_1 O_x U_0 |0\rangle$ and makes a measurement of some of its qubits. The result of this measure is by definition the outcome of the computation of $\mathcal{A}$ on input x. For a given ε, the query complexity of a function F, denoted $Q_{2,\varepsilon}$, is the smallest query complexity of a quantum algorithm computing F with probability of error at most ε.

In the sequel, the quantum algorithms as described above will also be called ad*adaptive* to distinguish them from nonadaptive quantum algorithms. Such an algorithm performs all its queries at the same time. A nonadaptive black-box quantum algorithm $\mathcal{A}$ that makes T queries can therefore be defined by a pair (U, V) of unitary operators. For $x \in S$ we define the unitary operator O_x^T by

$$O_x^T |i_1, \ldots, i_T\rangle|\varphi_1, \ldots, \varphi_T\rangle|\psi\rangle = |i_1, \ldots, i_T\rangle|\varphi_1 \oplus x(i_1), \ldots, \varphi_T \oplus x(i_T)\rangle|\psi\rangle.$$

The algorithm $\mathcal{A}$ computes the final state $V O_x^T U |0\rangle$ and makes a measurement of some of its qubits. As in the adaptive case, the result of this measure is by definition the outcome of the computation of $\mathcal{A}$ on input x. For a given ε, the nonadaptive query complexity of a function F, denoted $Q_{2,\varepsilon}^{na}$, is

the smallest query complexity of a nonadaptive quantum algorithm computing F with probability of error at most ε. Our model is more general than the model of [14]. In that model, the $|\varphi\rangle$ register must remain set to 0 after application of U. After application of O_x^T, the content of this register is therefore equal to $|x(i_1), \ldots, x(i_T)\rangle$ rather than $|\varphi_1 \oplus x(i_1), \ldots, \varphi_T \oplus x(i_T)\rangle$.

It is easy to verify that for every nonadaptive quantum algorithm $\mathcal{A}$ of query complexity T there is an adaptive quantum algorithm $\mathcal{A}'$ that makes the same number of queries and computes the same function, so that $Q_{2,\varepsilon} \leq Q_{2,\varepsilon}^{na}$. Indeed, consider for every $k \in [T]$ the unitary operator A_k which maps the state $|i_1, \ldots, i_T\rangle|\varphi_1, \ldots, \varphi_T\rangle$ to

$$|i_k\rangle|\varphi_k\rangle|i_1, \ldots, i_{k-1}, i_{k+1}, \ldots i_T\rangle|\varphi_1, \ldots, \varphi_{k-1}, \varphi_{k+1}, \ldots, \varphi_T\rangle.$$

If the nonadaptive algorithm $\mathcal{A}$ is defined by the pair of unitary operators (U, V), then the adaptive algorithm $\mathcal{A}'$ defined by the tuple of unitary operators

$$(U_0, \ldots, U_T) = (A_1 U, A_2 A_1^{-1}, \ldots, A_T A_{T-1}^{T-1}, V A_T^{-1})$$

computes the same function.

3 A Direct Method

3.1 Lower Bound Theorem and Applications

The main result of this section is Theorem 3. It yields an optimal $\Omega(N)$ lower bound on the nonadaptive quantum query complexity of Unordered Search and Element Distinctness. First we recall the weighted adversary method of Ambainis and some related definitions. The constant $C_\varepsilon = (1-2\sqrt{\varepsilon(1-\varepsilon)})/2$ will be used throughout the paper.

Definition 1. *The function $w : S^2 \to R_+$ is a* **valid weight function** *if every pair $(x, y) \in S^2$ is assigned a non-negative weight $w(x, y) = w(y, x)$ that satisfies $w(x, y) = 0$ whenever $F(x) = F(y)$. We then define for all $x \in S$ and $i \in \Gamma$: $wt(x) = \sum_y w(x, y)$ and $v(x, i) = \sum_{y:\ x(i) \neq y(i)} w(x, y)$.*

Definition 2. *The pair $(w,\ w')$ is a* **valid weight scheme** *if:*

- *Every pair $(x, y) \in S^2$ is assigned a non-negative weight $w(x, y) = w(y, x)$ that satisfies $w(x, y) = 0$ whenever $F(x) = F(y)$.*
- *Every triple $(x, y, i) \in S^2 \times \Gamma$ is assigned a non-negative weight $w'(x, y, i)$ that satisfies $w'(x, y, i) = 0$ whenever $x(i) = y(i)$ or $F(x) = F(y)$, and $w'(x, y, i)w'(y, x, i) \geq w^2(x, y)$ for all x, y, i with $x(i) \neq y(i)$.*

We then define for all $x \in S$ and $i \in \Gamma$ $wt(x) = \sum_y w(x, y)$ and $v(x, i) = \sum_y w'(x, y, i)$.

Of course these definitions are relative to the partial function F.

Remark 1. Let w be a valid weight function and define w' such that if $x(i) \neq y(i)$ then $w'(x,y,i) = w(x,y)$ and $w'(x,y,i) = 0$ otherwise. Then (w,w') is a valid weight scheme and the functions wt and v defined for w in Definition 1 are exactly those defined for (w,w') in Definition 2.

Theorem 1 (weighted adversary method of Ambainis [3]). *Given a probability of error ε and a partial function F, the quantum query complexity $Q_{2,\varepsilon}(F)$ of F as defined in section 2 satisfies:*

$$Q_{2,\varepsilon}(F) \geq C_\varepsilon \max_{(w,w')\ valid} \min_{\substack{x,y,i \\ w(x,y)>0 \\ x(i)\neq y(i)}} \sqrt{\frac{wt(x)wt(y)}{v(x,i)v(y,i)}}.$$

A probabilistic version of this lower bound theorem was obtained by Aaronson [1] and by Laplante and Magniez [13].

Theorem 2. *Fix the probability of error to $\varepsilon = 1/3$. The probabilistic query complexity $P_2(F)$ of F satisfies the lower bound $P_2(F) = \Omega(L_P(F))$, where*

$$L_P(F) = \max_w \min_{\substack{x,y,i \\ w(x,y)>0 \\ x(i)\neq y(i)}} \max\left(\frac{wt(x)}{v(x,i)}, \frac{wt(y)}{v(y,i)}\right).$$

Here w ranges over the set of valid weight functions.

We now state the main result of this section.

Theorem 3 (nonadaptive quantum lower bound, direct method). *The nonadaptive query complexity $Q^{na}_{2,\varepsilon}(F)$ of F satisfies the lower bound $Q^{na}_{2,\varepsilon}(F) \geq C^2_\varepsilon L^{na}_Q(F)$, where*

$$L^{na}_Q(F) = \max_w \max_{s\in S'} \min_{\substack{x,i \\ F(x)=s}} \frac{wt(x)}{v(x,i)}.$$

Here w ranges over the set of valid weight functions.

The following theorem, which is an unweighted adversary method for nonadaptive algorithm, is a consequence of Theorem 3.

Theorem 4. *Let $F : \Sigma^\Gamma \to \{0;1\}$, $X \subseteq F^{-1}(0)$, $Y \subseteq F^{-1}(1)$ and let $R \subset X \times Y$ be a relation such that:*

- *for every $x \in X$ there are at least m elements $y \in Y$ such that $(x,y) \in R$,*
- *for every $y \in Y$ there are at least m' elements $x \in X$ such that $(x,y) \in R$,*
- *for every $x \in X$ and every $i \in \Gamma$ there are at most l elements $y \in Y$ such that $(x,y) \in R$ and $x(i) \neq y(i)$,*
- *for every $y \in X$ and every $i \in \Gamma$ there are at most l' elements $x \in X$ such that $(x,y) \in R$ and $x(i) \neq y(i)$.*

Then $Q^{na}_{2,\varepsilon}(F) \geq C^2_\varepsilon \max(\frac{m}{l}, \frac{m'}{l'})$.

Proof. As in [3] and [13] we set $w(x,y) = w(y,x) = 1$ for all $(x,y) \in R$. Then $wt(x) \geq m$ for all $x \in A$, $wt(y) \geq m'$ for all $y \in B$, $v(x,i) \leq l$ and $v(y,i) \leq l'$. □

For the Unordered Search problem defined in Section 2 we have $m = N$ and $l = l' = m' = 1$. Theorem 4 therefore yields an optimal $\Omega(N)$ lower bound. The same bound can be obtained for the Element Distinctness problem. Here the set X of negative instances is made up of all one-to-one functions $x : [N] \to [N]$ and Y contains the functions $y : [N] \to [N]$ that are not one-to-one. We consider the relation R such that $(x,y) \in R$ if and only if there is a unique i such that $x(i) \neq y(i)$. Then $m = 2, l = 1, m' = N(N-1)$ and $l' = N - 1$.

As pointed out in [13], the $\Omega(\max(m/l, m'/l'))$ lower bound from Theorem 4 is also a lower bound on $P_2(F)$. There is a further connection:

Proposition 1. *For any function F we have $L_P(F) \geq L_Q^{na}(F)$. That is, ignoring constant factors, the lower bound on $P_2(F)$ given by Theorem 2 is at least as high as the lower bound on $Q_{2,\varepsilon}^{na}(F)$ given by Theorem 3.*

Proof. Pick a weight function w_Q which is optimal for the "direct method" of Theorem 3. That is, w_Q achieves the lower bound $L_Q^{na}(F)$ defined in this theorem. Let s_Q be the corresponding optimal choice for $s \in S'$. We need to design a weight function w_P which will show that $L_P(F) \geq L_Q^{na}(F)$. One can simply define w_P by: $w_P(x,y) = w_Q(x,y)$ if $F(x) = s_Q$ or $F(y) = s_Q$; $w_P(x,y) = 0$ otherwise. Indeed, for any i and any pair (x,y) such that $w_P(x,y) > 0$ we have $F(x) = s_Q$ or $F(y) = s_Q$, so that $\max(wt(x)/v(x,i), wt(y)/v(y,i)) \geq L_Q^{na}(F)$. □

The nonadaptive quantum lower bound from Theorem 3 is therefore rather closely connected to adaptive probabilistic lower bounds: it is sandwiched between the weighted lower bound of Theorem 2 and its unweighted $\max(m/l, m'/l')$ version. Proposition 1 also implies that Theorem 3 can at best prove an $\Omega(\log N)$ lower bound on the nonadaptive quantum complexity of Ordered Search. Indeed, by binary search the adaptive probabilistic complexity of this problem is $O(\log N)$. In section 4 we shall see that there is in fact a $\Omega(N)$ lower bound on the nonadaptive quantum complexity of this problem.

Remark 2. The connection between nonadaptive quantum complexity and adaptive probabilistic complexity that we have pointed out in the paragraph above is only a connection between the *lower bounds* on these quantities. Indeed, there are problems with a high probabilistic query complexity and a low nonadaptive quantum query complexity (for instance, Simon's problem [16, 10]). Conversely, there are problems with a low probabilistic query complexity and a high nonadaptive quantum query complexity (for instance, Ordered Search).

3.2 Proof of Theorem 3

As mentioned in the introduction, we will treat the tuple $(i_1, \ldots, i_k)$ of queries made by a nonadaptive algorithm as a single "super query" made by an ordinary quantum algorithm (incidentally, this method could be used to obtain lower bounds on quantum algorithm that make several rounds of parallel queries as in [8]). This motivates the following definition.

Definition 3. *Let Σ, Γ and S be as in section 2. Given an integer $k \geq 2$, we define:*

- ${}^k\Sigma = \Sigma^k$, ${}^k\Gamma = \Gamma^k$ *and* ${}^kS = \left(\Sigma^k\right)^{\Gamma^k}$.
- *To the black box $x \in S$ we associate the "super box" ${}^kx \in {}^kS$ such that if $I = (i_1, \ldots, i_k) \in \Gamma^k$ then ${}^kx(I) = (x(i_1), \ldots, x(i_k))$.*
- ${}^kF({}^kx) = F(x)$.
- *If w is a weight function for F we define a weight function W for ${}^kF$ by $W({}^kx, {}^ky) = w(x, y)$.*

Assume for instance that $\Sigma = \{0; 1\}$, $\Gamma = [3]$, $k = 2$, and that x is defined by: $x(1) = 0$, $x(2) = 1$ and $x(3) = 0$. Then we have ${}^2x(1,1) = (0,0)$, ${}^2x(1,2) = (0,1)$, ${}^2x(1,3) = (0,0)$ ...

Lemma 1. *If w is a valid weight function for F then W is a valid weight function for ${}^kF$ and the minimal number of queries of a quantum algorithm computing ${}^kF$ with error probability ε satisfies:*

$$Q_{2,\varepsilon}({}^kF) \geq C_\varepsilon \cdot \min_{\substack{{}^kx, {}^ky, I \\ W({}^kx, {}^ky) > 0 \\ {}^kx(I) \neq {}^ky(I)}} \sqrt{\frac{WT({}^kx)WT({}^ky)}{V({}^kx, I)V({}^ky, I)}}.$$

Proof. Every pair $(x, y) \in S^2$ is assigned a non-negative weight $W({}^kx, {}^ky) = W({}^ky, {}^kx) = w(x, y) = w(y, x)$ that satisfies $W({}^kx, {}^ky) = 0$ whenever $F(x) = F(y)$. Thus we can apply Theorem 1 and we obtain the announced lower bound. □

Lemma 2. *Let x be a black-box and w a weight function. For any integer k and any tuple $I = (i_1, \ldots, i_k)$ we have*

$$\frac{WT({}^kx)}{V({}^kx, I)} \geq \frac{1}{k} \min_{j \in [k]} \frac{wt(x)}{v(x, i_j)}.$$

Proof. Let $m = \min_{j \in [k]} \frac{wt(x)}{v(x, i_j)}$. We have $WT({}^kx) = wt(x)$ and:

$$\begin{aligned} V({}^kx, I) &= \sum_{{}^ky : {}^kx(i) \neq {}^ky(i)} W({}^kx, {}^ky) \\ &\leq \sum_{y : x(i_1) \neq y(i_1)} w(x, y) + \cdots + \sum_{y : x(i_k) \neq y(i_k)} w(x, y) \\ &= v(x, i_1) + \cdots + v(x, i_k) \leq k \max_{j \in [k]} v(x, i_j). \end{aligned}$$

□

Lemma 3. *If w is a valid weight function:*

$$Q^{na}_{2,\varepsilon}(F) \geq C^2_\varepsilon \min_{\substack{x, y \\ F(x) \neq F(y)}} \max\left(\min_i \frac{wt(x)}{v(x, i)}, \min_i \frac{wt(y)}{v(y, i)}\right).$$

Proof. Let w be an arbitrary valid weight function and k be an integer such that

$$k < C_\varepsilon^2 \min_{\substack{x,y \\ F(x)\neq F(y)}} \max\left(\min_i \frac{wt(x)}{v(x,i)}, \min_i \frac{wt(y)}{v(y,i)}\right).$$

We show that an algorithm computing ${}^kF$ with probability of error $\leq \varepsilon$ must make strictly more one than query to the "super box" ${}^kx$. This will prove that for every such k we have $Q_{2,\varepsilon}^{na}(F) > k$ and thus our result.

For every x and I we have

$$\frac{WT({}^kx)}{V({}^kx, I)} \geq 1$$

and thus by lemma 2 for every x, y and $I = (i_1, \ldots, i_k)$:

$$\begin{aligned}
\frac{WT({}^kx)}{V({}^kx,I)}\frac{WT({}^ky)}{V({}^kx,I)} &= \min\left(\frac{WT({}^kx)}{V({}^kx,I)}, \frac{WT({}^ky)}{V({}^kx,I)}\right)\max\left(\frac{WT({}^kx)}{V({}^kx,I)}, \frac{WT({}^ky)}{V({}^kx,I)}\right) \\
&\geq \max\left(\frac{WT({}^kx)}{V({}^kx,I)}, \frac{WT({}^ky)}{V({}^kx,I)}\right) \\
&\geq \frac{1}{k}\max\left(\min_{j\in[k]} \frac{wt(x)}{v(x,i_j)}, \min_{l\in[k]} \frac{wt(y)}{v(x,i_l)}\right).
\end{aligned}$$

In order to apply Lemma 1 we observe that:

$$\begin{aligned}
\min_{\substack{{}^kx,{}^ky,I \\ W({}^kx,{}^ky)>0 \\ {}^kx(I)\neq{}^ky(I)}} \frac{WT({}^kx)WT({}^ky)}{V({}^kx,I)V({}^ky,I)} &\geq \frac{1}{k} \min_{\substack{x,y,i_1,\ldots,i_k \\ w(x,y)>0 \\ \exists m\ x(i_m)\neq y(i_m)}} \max\left(\min_{j\in[k]} \frac{wt(x)}{v(x,i_j)}, \min_{l\in[k]} \frac{wt(y)}{v(x,i_l)}\right) \\
&\geq \frac{1}{k} \min_{\substack{x,y \\ F(x)\neq F(y)}} \max\left(\min_i \frac{wt(x)}{v(x,i)}, \min_i \frac{wt(y)}{v(x,i)}\right)
\end{aligned}$$

By hypothesis on k, this expression is greater than $1/C_\varepsilon^2$. Thus according to Lemma 1 we have $Q_{2,\varepsilon}({}^kF) > 1$, and $Q_{2,\varepsilon}^{na}(F) > k$. □

We can now complete the proof of Theorem 3. Suppose without loss of generality that $F(S) = [m]$ and define for every $l \in [m]$:

$$a_l = C_\varepsilon^2 \min_{\substack{x,i \\ F(x)=l}} \frac{wt(x)}{v(x,i)}.$$

Suppose also without loss of generality that $a_1 \leq \cdots \leq a_m$. It follows immediately from the definition that

$$a_2 = C_\varepsilon^2 \min_{\substack{x,y \\ F(x)\neq F(y)}} \max\left(\min_i \frac{wt(x)}{v(x,i)}, \min_i \frac{wt(y)}{v(x,i)}\right),$$

and

$$a_m = C_\varepsilon^2 \max_{l \in F(S)} \min_{\substack{x,i \\ F(x)=l}} \frac{wt(x)}{v(x,i)}.$$

By Lemma 3 we have $Q_{2,\varepsilon}^{na}(F) \geq a_2$, but we would like to show that $Q_{2,\varepsilon}^{na}(F) \geq a_m$. We proceed by reduction from the case when there are only two classes (i.e., $m = 2$). Let G be defined by

$$G(1) = \cdots = G(m-1) = 1$$

and $G(m) = m$. Applying Lemma 3 to GoF, we obtain that $Q_{2,\varepsilon}^{na}(GoF) \geq a_m$. But because the function GoF is obviously easier to compute than F, we have $Q_{2,\varepsilon}^{na}(F) \geq Q_{2,\varepsilon}^{na}(GoF)$ and thus $Q_{2,\varepsilon}^{na}(F) \geq a_m$ as desired.

4 From the Dual to the Primal

Our starting point in this section is the minimax method of Laplante and Magniez [13, 17] as stated in [9]:

Theorem 5. *Let $p : S \times \Sigma \to \mathbb{R}^+$ be the set of $|S|$ probability distributions such that $p_x(i)$ is the average probability of querying i on input x, where the average is taken over the whole computation of an algorithm $\mathcal{A}$. Then the query complexity of $\mathcal{A}$ is greater or equal to:*

$$C_\varepsilon \max_{\substack{x,y \\ F(x)\neq F(y)}} \frac{1}{\sum\limits_{\substack{i \\ x(i)\neq y(i)}} \sqrt{p_x(i)p_y(i)}}.$$

Theorem 5 is the basis for the following lower bound theorem. It can be shown that up to constant factors, the lower bound given by Theorem 6 is always as good as the lower bound given by Theorem 3.

Theorem 6 (nonadaptive quantum lower bound, primal-dual method). *Let $F : S \to S'$ be a partial function, where as usual $S = \Sigma^\Gamma$ is the set of black-box functions. Let*

$$DL(F) = \min_p \max_{\substack{x,y \\ F(x)\neq F(y)}} \frac{1}{\sum\limits_{\substack{i \\ x(i)\neq y(i)}} p(i)}$$

and

$$PL(F) = \max_w \frac{\sum\limits_{x,y} w(x,y)}{\max\limits_i \sum\limits_{\substack{x,y \\ x_i \neq y_i}} w(x,y)}$$

where the min *in the first formula is taken over all probability distributions p over Γ, and the* max *in the second formula is taken over all valid weight functions w. Then $DL(F) = PL(F)$ and we have the following nonadaptive query complexity lower bound:*

$$Q_{2,\varepsilon}(F) \geq C_\varepsilon DL(F) = C_\varepsilon PL(F).$$

Proof. We first show that $Q_{2,\varepsilon}(F) \geq C_\varepsilon DL(F)$. Let $\mathcal{A}$ be a nonadaptive quantum algorithm for F. Since $\mathcal{A}$ is nonadaptive, the probability $p_x(i)$ of querying i on input x is independent of x. We denote it by $p(i)$. Theorem 5 shows that the query complexity of $\mathcal{A}$ is greater or equal to

$$C_\varepsilon \max_{\substack{x,y \\ F(x)\neq F(y)}} \frac{1}{\sum\limits_{\substack{i \\ x(i)\neq y(i)}} p(i)}.$$

The lower bound $Q_{2,\varepsilon}(F) \geq C_\varepsilon DL(F)$ follows by minimizing over p.

It remains to show that $DL(F) = PL(F)$. Let

$$L(F) = \min_p \max_{\substack{x,y \\ F(x)\neq F(y)}} \sum_{\substack{i \\ x(i)=y(i)}} p(i).$$

We observe that $L(F)$ is the optimal solution of the following linear program: minimize μ subject to the constraints

$$\forall x, y \text{ such that } f(x) \neq f(y) : \ \mu - \sum_{\substack{i \\ x(i)\neq y(i)}} p(i) \geq 0,$$

$$\text{and to the constraints } \sum_{i=1}^{N} p(i) = 1 \text{ and } \forall i \in [N] : \ p(i) \geq 0.$$

Clearly, its solution set is nonempty. Thus $L(f)$ is the optimal solution of the dual linear program: maximize ν subject to the constraints

$$\forall i \in [N] : \ \nu - \sum_{\substack{x,y \\ x_i=y_i}} w(x,y) \leq 0$$

$$\forall x, y : \ w(x,y) \geq 0, \text{ and } w(x,y) = 0 \text{ if } F(x) = F(y)$$

$$\text{and to the constraint} \sum_{x,y} w(x,y) = 1.$$

Hence $L(F) = \max\limits_w \min\limits_i \dfrac{\sum\limits_{x_i=y_i} w(x,y)}{\sum\limits_{x,y} w(x,y)}$ and $DL(F) = \frac{1}{1-L(F)} = PL(F)$. □

4.1 Application to Ordered Search and Connectivity

Proposition 1. *For any error bound $\varepsilon \in [0, \frac{1}{2})$ we have*

$$Q^{na}_{2,\varepsilon}(\textit{Ordered Search}) \geq C_\varepsilon(N-1).$$

Proof. Consider the weight function $w(x,y) = \begin{cases} 1 & \text{if } |F(y) - F(x)| = 1, \\ 0 & \text{otherwise.} \end{cases}$ Thus $w(x,y) = 1$ when the leftmost 1's in x and y are adjacent. Hence $\sum_{x,y} w(x,y) = 2(N-2)+2$. Moreover, if $w(x,y) \neq 0$ and $x_i \neq y_i$ then $\{F(x), F(y)\} = \{i, i+1\}$. Therefore, $\max_i \sum_{\substack{x,y \\ x_i \neq y_i}} w(x,y) = 2$ and the result follows from Theorem 6. □

Our second application of Theorem 6 is to the graph connectivity problem. We consider the adjacency matrix model: $x(i,j) = 1$ if ij is an edge of the graph. We consider undirected, loopless graph so that we can assume $j < i$. For a graph on n vertices, the black box x therefore has $N = n(n-1)/2$ entries. We denote by G_x the graph represented by x.

Theorem 7. *For any error bound $\varepsilon \in [0, \frac{1}{2})$, we have*

$$Q^{na}_{2,\varepsilon}(\textit{Connectivity}) \geq C_\varepsilon n(n-1)/8.$$

Proof. We shall use essentially the same weight function as in ([6], Theorem 8.3). Let X be the set of all adjacency matrices of a unique cycle, and Y the set of all adjacency matrices with exactly two (disjoint) cycles. For $x \in X$ and $y \in Y$, we set $w(x,y) = 1$ if there exist 4 vertices $a, b, c, d \in [n]$ such that the only differences between G_x and G_y are that:

1. ab, cd are edges in G_x but not in G_y.
2. ac, bd are edges in G_y but not in G_x.

We claim that

$$\max_{ij} \sum_{\substack{x \in X, y \in Y \\ x(i,j) \neq y(i,j)}} w(x,y) = \frac{8}{n(n-1)} \sum_{\substack{x \in X, y \in Y \\ x(i,j) \neq y(i,j)}} w(x,y). \tag{1}$$

The conclusion of Theorem 7 will then follow directly from Theorem 6. By symmetry, the function that we are maximizing on the left-hand side of (1) is in fact independent of the edge ij. We can therefore replace the max over ij by an average over ij: the left-hand side is equal to

$$\frac{1}{N} \sum_{x \in X, y \in Y} w(x,y) |\{ij;\ x(i,j) \neq y(i,j)\}|.$$

Now, the condition $x(i,j) \neq y(i,j)$ holds true if and only if ij is one of the 4 edges ab, cd, ac, bd defined at the beginning of the proof. This finishes the proof of (1), and of Theorem 7. □

A similar argument can be used to show that testing whether a graph is bipartite also requires $\Omega(n^2)$ queries.

5 Some Open Problems

For the "1-to-1 versus 2-to-1" problem, one would expect a higher quantum query complexity in the nonadaptive setting than in the adaptive setting. This may be difficult to establish since the adaptive lower bound [2] is based on the polynomial method. Hidden Translation [7] (a problem closely connected to the dihedral hidden subgroup problem) is another problem of interest. No lower bound is known in the adaptive setting, so it would be natural to look first for a nonadaptive lower bound. Finally, one would like to identify some classes of problems for which adaptivity does not help quantum algorithms.

Acknowledgements. This work has benefited from discussions with Sophie Laplante, Troy Lee, Frédéric Magniez and Vincent Nesme.

References

1. Aaronson, S.: Lower bounds for local search by quantum arguments. In: Proc. STOC 2004, pp. 465–474. ACM Press, New York (2004)
2. Aaronson, S., Shi, Y.: Quantum Lower Bounds for the Collision and the Element Distinctness Problems. Journal of the ACM 51(4), 595–605 (2004)
3. Ambainis, A.: Polynomial degree vs. quantum query complexity. J. Comput. Syst. Sci. 72(2), 220–238 (2006)
4. Bar-Yossef, Z., Kumar, R., Sivakumar, D.: Sampling Algorithms: lower bounds and applications. In: Proc. STOC 2001, pp. 266–275. ACM Press, New York (2001)
5. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. Journal of the ACM 48(4), 778–797 (2001)
6. Dürr, C., Heiligman, M., Høyer, P., Mhalla, M.: Quantum query complexity of some graph problems. SIAM J. Comput. 35(6), 1310–1328 (2006)
7. Friedl, K., Ivanyos, G., Magniez, F., Santha, M., Sen, P.: Hidden translation and orbit coset in quantum computing. In: STOC 2003: Proceedings of the thirty-fifth annual ACM symposium on Theory of computing (2003)
8. Grover, L.K., Radhakrishnan, J.: Quantum search for multiple items using parallel queries. arXiv (2004)
9. Hoyer, P., Spalek, R.: Lower bounds on quantum query complexity. EATCS Bulletin 87, 78–103 (2005)
10. Koiran, P., Nesme, V., Portier, N.: On the probabilistic query complexity of transitively symmetric problems, `http://perso.ens-lyon.fr/pascal.koiran`
11. Koiran, P., Nesme, V., Portier, N.: A quantum lower bound for the query complexity of Simon's problem. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 1287–1298. Springer, Heidelberg (2005)
12. Koiran, P., Nesme, V., Portier, N.: The quantum query complexity of abelian hidden subgroup problems. Theoretical Computer Science 380, 115–126 (2007)
13. Laplante, S., Magniez, F.: Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. SIAM journal on Computing (to appear)
14. Nishimura, H., Yamakami, T.: An algorithmic argument for nonadaptive query complexity lower bounds on advised quantum computation (extended abstract). In: Fiala, J., Koubek, V., Kratochvíl, J. (eds.) MFCS 2004. LNCS, vol. 3153, pp. 827–838. Springer, Heidelberg (2004)

15. Rosenberg, A.L.: On the time required to check properties of graphs: A problem. SIGACT News, 15–16 (1973)
16. Simon, D.R.: On the power of quantum computation. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 116–123 (1994)
17. Spalek, R., Szegedy, M.: All quantum adversary methods are equivalent. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 1299–1311. Springer, Heidelberg (2005)