Available online at www.sciencedirect.com
SCIENCE DIRECT®

Theoretical Computer Science 339 (2005) 241–256

Theoretical Computer Science

www.elsevier.com/locate/tcs

On the power of Ambainis lower bounds

Shengyu Zhang*

Computer Science Department, Princeton University, 35 Olden Street, Princeton, NJ 08544, USA

Received 28 May 2004; accepted 13 January 2005

Communicated by D-Z. Du

Abstract

The polynomial method and the Ambainis lower bound (or *Alb*, for short) method are two main quantum lower bound techniques. While recently Ambainis showed that the polynomial method is not tight, the present paper aims at studying the power and limitation of *Alb*'s. We first use known *Alb*'s to derive $\Omega(n^{1.5})$ lower bounds for BIPARTITENESS, BIPARTITENESS MATCHING and GRAPH MATCHING, in which the lower bound for BIPARTITENESS improves the previous $\Omega(n)$ one. We then show that all the three known Ambainis lower bounds have a limitation $\sqrt{N}\min\{C_0(f), C_1(f)\}$, where $C_0(f)$ and $C_1(f)$ are the 0- and 1-certificate complexities, respectively. This implies that for many problems such as TRIANGLE, k-CLIQUE, BIPARTITENESS and BIPARTITE/GRAPH MATCHING which draw wide interest and whose quantum query complexities are still open, the best known lower bounds cannot be further improved by using Ambainis techniques. Another consequence is that all the Ambainis lower bounds are not tight. For total functions, this upper bound for *Alb*'s can be further improved to $\min\{\sqrt{C_0(f)C_1(f)}, \sqrt{N \cdot CI(f)}\}$, where $CI(f)$ is the size of max intersection of a 0- and a 1-certificate set. Again this implies that Alb's cannot improve the best known lower bound for some specific problems such as AND-OR TREE, whose precise quantum query complexity is still open. Finally, we generalize the three known *Alb*'s and give a new *Alb* style lower bound method, which may be easier to use for some problems.

Keywords: Quantum computing; Quantum query complexity; Lower bound technique; Quantum adversary method

1. Introduction

Quantum computing has received a great deal of attention in the last decade because of the potentially high speedup over classical computation. Among others, the query model

* Tel.: +1 6092580419; fax: +1 6092581771.
E-mail address: szhang@cs.princeton.edu.

0304-3975/$ - see front matter © 2005 Published by Elsevier B.V.
doi:10.1016/j.tcs.2005.01.019

is extensively studied, partly because it is a natural quantum analog of classical decision tree complexity, and partly because many known quantum algorithms fall into this framework [13,14,16,18,19,28,29,32]. In the query model, the input is accessed by querying an oracle, and the goal is to minimize the number of queries made. We are most interested in double-side bounded-error computation, where the output is correct with probability at least 2/3 for all inputs. We use $Q_2(f)$ to denote minimal number of queries for computing f with double sided bound-error. For more details on the quantum query model, we refer to [6,15] as excellent surveys.

Two main lower bound techniques for $Q_2(f)$ are the polynomial method by Beals et al. [11] and Ambainis lower bounds [4,5], the latter of which is also called quantum adversary method. Many lower bounds have recently been proven by applying the polynomial method [1,11,22,24,27] and Ambainis lower bounds [2,4,5,17,31]. Recently, Aaronson even uses Ambainis lower bound technique to achieve lower bounds for some classical problems [2]. Given the usefulness of the two methods, it is interesting to know how tight they are. In a recent work [5], Ambainis proves that polynomial method is not tight, by showing a function with polynomial degree M and quantum query complexity $\Omega(M^{1.321\cdots})$. So a natural question is the power of Ambainis lower bounds. We show that all known Ambainis lower bounds are not tight either, among other results.

There are several known versions of Ambainis lower bounds, among which the three Ambainis theorems are widely used partly because they have simple forms and are thus easy to use. The first two *Alb*'s are given in [4] as follows.

Theorem 1 (*Ambainis [4]*). *Let* $f : \{0,1\}^N \to \{0,1\}$ *be a function and* X, Y *be two sets of inputs* s.t. $f(x) \neq f(y)$ *if* $x \in X$ *and* $y \in Y$. *Let* $R \subseteq X \times Y$ *be a relation* s.t.
(1) $\forall x \in X$, *there are at least* m *different* $y \in Y$ s.t. $(x, y) \in R$.
(2) $\forall y \in Y$, *there are at least* m' *different* $x \in X$ s.t. $(x, y) \in R$.
(3) $\forall x \in X, \forall i \in [N]$, *there are at most* l *different* $y \in Y$ s.t. $(x, y) \in R, x_i \neq y_i$.
(4) $\forall y \in Y, \forall i \in [N]$, *there are at most* l' *different* $x \in X$ s.t. $(x, y) \in R, x_i \neq y_i$.
Then $Q_2(f) = \Omega(\sqrt{mm'/ll'})$.

Theorem 2 (*Ambainis [4]*). *Let* $f : I^N \to \{0,1\}$ *be a Boolean function where* I *is a finite set, and* X, Y *be two sets of inputs* s.t. $f(x) \neq f(y)$ *if* $x \in X$ *and* $y \in Y$. *Let* $R \subseteq X \times Y$ *satisfy*
(1) $\forall x \in X$, *there are at least* m *different* $y \in Y$ s.t. $(x, y) \in R$.
(2) $\forall y \in Y$, *there are at least* m' *different* $x \in X$ s.t. $(x, y) \in R$.
Denote

$$l_{x,i} = |\{y : (x, y) \in R, x_i \neq y_i\}|, \quad l_{y,i} = |\{x : (x, y) \in R, x_i \neq y_i\}|$$

$$l_{\max} = \max_{x,y,i:(x,y)\in R, i\in[N], x_i\neq y_i} l_{x,i} l_{y,i}.$$

Then $Q_2(f) = \Omega(\sqrt{mm'/l_{\max}})$.

Obviously, Theorem 2 generalizes Theorem 1. In [5], Ambainis gives another (weighted) approach to generalize Theorem 1. We restate it in a form similar to Theorem 1.

Definition 3. Let $f : I^N \to \{0, 1\}$ be a Boolean function where I is a finite set. Let X, Y be two sets of inputs *s.t.* $f(x) \neq f(y)$ if $x \in X$ and $y \in Y$. Let $R \subseteq X \times Y$ be a relation. A weight scheme for X, Y, R consists of three weight functions $w(x, y) > 0$, $u(x, y, i) > 0$ and $v(x, y, i) > 0$ satisfying

$$u(x, y, i)v(x, y, i) \geqslant w^2(x, y) \tag{1}$$

for all $(x, y) \in R$ and $i \in [N]$ with $x_i \neq y_i$. We further denote

$$w_x = \sum_{y:(x,y)\in R} w(x, y), \quad w_y = \sum_{x:(x,y)\in R} w(x, y)$$

$$u_{x,i} = \sum_{y:(x,y)\in R, x_i \neq y_i} u(x, y, i), \quad v_{y,i} = \sum_{x:(x,y)\in R, x_i \neq y_i} v(x, y, i).$$

Theorem 4 (*Ambainis [5]*). *Let $f : I^N \to \{0, 1\}$ where I is a finite set, and $X \subseteq f^{-1}(0)$, $Y \subseteq f^{-1}(1)$ and $R \subseteq X \times Y$. Let w, u, v be a weight scheme for X, Y, R. Then*

$$Q_2(f) = \Omega\left(\sqrt{\min_{x\in X, i\in[N]} \frac{w_x}{u_{x,i}} \cdot \min_{y\in Y, j\in[N]} \frac{w_y}{v_{y,j}}}\right).$$

Denote by $Alb_1(f)$, $Alb_2(f)$ and $Alb_3(f)$ the best lower bound for function f achieved by Theorem 1, 2 and 3, respectively. [1] Note that in the three Alb's, there are many parameters (X, Y, R, u, v, w) to be set. By setting these parameters in an appropriate way, one can get good lower bounds for many problems. In particular, we consider the following three graph properties. [2]

(1) BIPARTITENESS: *Given an undirected graph, decide whether it is a bipartite graph.*
(2) GRAPH MATCHING: *Given an undirected graph, decide whether it has a perfect matching.*
(3) BIPARTITE MATCHING: *Given an undirected bipartite graph, decide whether it has a perfect matching.*

We show by using Alb_2 that all these three graph properties have a $\Omega(n^{1.5})$ lower bound, where n is the number of vertices. For BIPARTITENESS, this improves the previous result of $\Omega(n)$ lower bound (in a preliminary version of [20]).

Since Alb_2 and Alb_3 generalizes Alb_1 in different ways, it is interesting to compare their powers. It turns out that $Alb_2(f) \leqslant Alb_3(f)$.

However, even Alb_3 has a limitation: we show that $Alb_3(f)$ is no more than $\sqrt{N \cdot C_-(f)}$ where $C_-(f) = \min\{C_0(f), C_1(f)\}$ with $C_0(f)$ and $C_1(f)$ being the 0- and 1-certificate complexity of f, respectively. This has two immediate consequences. First, it gives a negative answer to the open problem whether Alb_2 or Alb_3 is tight, because for ELEMENT DISTINCTNESS, we know that $Q_2(f) = \Omega(N^{2/3})$ by Shi's result in [27], but $\sqrt{N \cdot C_-(f)}$ is only $\sqrt{2N}$.

Second, for some problems whose precise quantum query complexities are still unknown, our theorem implies that the best known lower bound cannot be further improved by using

[1] To make the later results more precise, we actually use $Alb_i(f)$ to denote the value inside the $\Omega()$ notation. For example, $Alb_1(f) = \max_{(X,Y,R)} \sqrt{mm'/ll'}$.

[2] In this paper, all the graph property problems are given by adjacency matrix input.

Ambainis lower bound techniques, no matter how we choose the parameters in the Alb theorems. For example TRIANGLE/k-CLIQUE (k is constant) are the problems to decide whether an n-node graph contains a triangle/k-node clique. It is easy to get a $\Omega(n)$ lower bound for both of them. By our theorem, however, we know that this is the best possible by using Ambainis lower bound techniques. Also the $\Omega(n^{1.5})$ lower bound for BIPARTITENESS, BIPARTITE MATCHING and GRAPH MATCHING cannot be further improved by Alb's either, because $C_1(f) = \mathrm{O}(n)$ for all of them.

If f is a total function, the above upper bound of Alb's can be further tightened in two ways. The first one is $Alb_3(f) \leqslant \sqrt{N \cdot CI(f)}$, where $CI(f)$ is the size of the largest intersection of a 0-certificate set and a 1-certificate set, so $CI(f) \leqslant C_-(f)$. The second approach leads to another result $Alb_3(f) \leqslant \sqrt{C_0(f)C_1(f)}$. Both the results imply that for AND-OR TREE, a problem whose quantum query complexity is still open [5], the current best $\Omega(\sqrt{N})$ lower bound [9] cannot be further improved by using Ambainis lower bounds. The second result also give an positive answer to the open question whether $Alb_3(f) = \mathrm{O}(\sqrt{C_0(f)C_1(f)})$.

Finally, it is natural to consider combining the different approaches that Alb_2 and Alb_3 use to generalize Alb_1, and get a further generalized one. Based on this idea, we give a new and more general lower bound theorem, which we call Alb_4. Compared with Alb_3, this may be easier to use.

1.1. Related work

In the open problems part of [5], Ambainis mentions the $\sqrt{C_0(f)C_1(f)}$ limitation of Alb_1, and asks for new quantum lower bound techniques higher than $\sqrt{C_0(f)C_1(f)}$. However, it is not shown in [5] whether Alb_2 and Alb_3 are also bounded by the $\sqrt{C_0(f)C_1(f)}$ limitation for total function f, and actually even whether $Alb_2(f) = \mathrm{O}(\sqrt{C_0(f)C_1(f)})$ was still open at the time, according to a private communication between Ambainis and us.

Recently Spalek and Szegedy independently show in [30] that the all quantum adversary methods, including Alb_3 by Ambainis [5], Alb_4 in an earlier version of the present paper [33], and another quantum adversary method proposed in [10], are actually equivalent. Using this fact, they gave a simple proof that all of them cannot prove quantum lower bounds better than $\Omega(\sqrt{N \cdot C_-(f)})$ for general function and not better than $\Omega(\sqrt{C_0(f)C_1(f)})$ for total functions.

The theorem $Alb_3(f) \leqslant \sqrt{N \cdot C_-(f)}$ is also derived by Laplante and Magniez by using Kolmogorov complexity in [20]. And the $\Omega(n^{1.5})$ lower bound for Matching is independently obtained by Berzina, Dubrovsky, Freivalds, Lace and Scegulnaja in [12], and the same lower bound for Bipartiteness is independently obtained by Durr (cited in [20]).

2. Old Ambainis lower bounds

In this section we first use Alb_2 to derive $\Omega(n^{1.5})$ lower bounds for BIPARTITENESS, BIPARTITE MATCHING and GRAPH MATCHING, then show that Alb_3 has actually at least the same power as Alb_2.

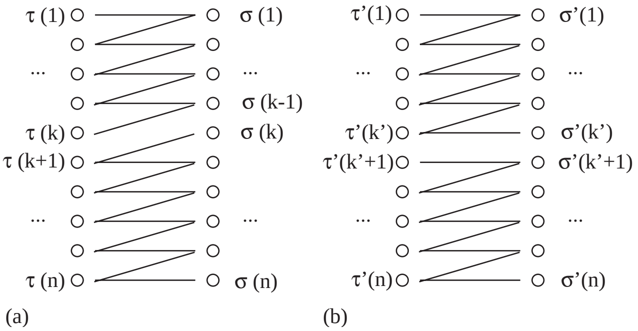

Fig. 1. X and Y.

Theorem 5. *All the three graph properties* Bipartiteness, Bipartite Matching *and* Graph Matching *have $Q_2(f) = \Omega(n^{1.5})$.*

Proof. 1. Bipartiteness. The proof is very similar to the one for proving $\Omega(n^{1.5})$ lower bound of Graph Connectivity by Durr et al. [17]. Without loss of generality, we assume n is even, because otherwise we can use the following argument on arbitrary $n-1$ (out of total n) nodes and leave the n^{th} node isolated. Let

$X = \{G : G$ is composed of a single n-length cycle$\}$,

$Y = \{G : G$ is composed of two cycles each with length being an odd number between $n/3$ and $2n/3\}$, and

$R = \{(G, G') \in X \times Y : \exists$ four nodes v_1, v_2, v_3, v_4 *s.t.* the only difference between graphs G and G' is that (v_1, v_2), (v_3, v_4) are edges in G but not in G' and (v_1, v_3), (v_2, v_4) are edges in G' but not in $G\}$.

Note that a graph is bipartite if and only if it contains no cycle with odd length. Therefore, any graph in X is a bipartite graph because n is even, and any graph in Y is not bipartite graph because it contains two odd-length cycles. Then all the remaining analysis is the same as calculation in the proof for Graph Connectivity (undirected graph and matrix input) in [17], and finally $Alb_2(\text{Bipartiteness}) = \Omega(n^{1.5})$.

2. Bipartite Matching. Let X be the set of the bipartite graphs like Fig. 1(a) where τ and σ are two permutations of $\{1, \ldots, n\}$, and $n/3 \leqslant k \leqslant 2n/3$. Let Y be the set of the bipartite graphs like Fig. 1(b), where τ' and σ' are two permutations of $\{1, \ldots, n\}$, and also $n/3 \leqslant k' \leqslant 2n/3$. It is easy to see that all graphs in X have no perfect matching, while all graphs in Y have a perfect matching.

Let R be the set of all pairs of $(x, y) \in X \times Y$ as in Fig. 2, where graph y is obtained from x by choosing two horizontal edges $(\tau(i), \sigma(i))$, $(\tau(j), \sigma(j))$, removing them, and adding two edges $(\tau(i), \sigma(j))$, $(\tau(j), \sigma(i))$.

Now it is not hard to calculate the $m, m', l_{\max}$ in Alb_2. For example, to get m we study x in two cases. When $n/3 \leqslant k \leqslant n/2$, any edge $(\tau(i), \sigma(i))$ where $i \in [k - n/3, k]$ has at least $n/6$ choices for edge $(\tau(j), \sigma(j))$ because the only requirement for choosing is that $k' \in [n/3, 2n/3]$ and $k' = i + n - j$. The case when $n/2 \leqslant k \leqslant 2n/3$ can be handled symmetrically. Thus $m = \Theta(n^2)$. The same argument yields $m' = \Theta(n^2)$. Finally, for $l_{\max}$,

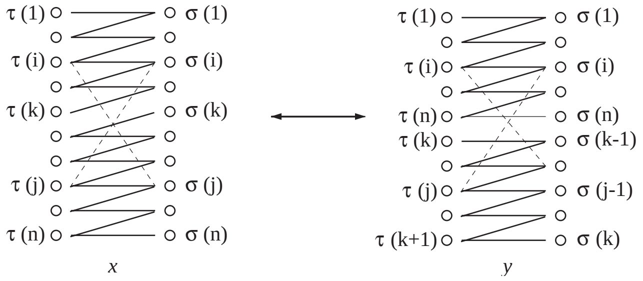

Fig. 2. $R \subseteq X \times Y$.

we note that if the edge $e = (\tau(i), \sigma(i))$ for some i, then $l_{x,e} = \mathrm{O}(n)$ and $l_{y,e} = 1$; if the edge $e = (\tau(i), \sigma(j))$ for some i, j, then $l_{x,e} = 1$ and $l_{y,e} = \mathrm{O}(n)$. For all other edges e, $l_{x,e} = l_{y,e} = 0$. Putting all cases together, we have $l_{\max} = \mathrm{O}(n)$. Thus by Theorem 2, we know that Alb_2(BIPARTITE MATCHING) $= \Omega(n^{1.5})$.

3. GRAPH MATCHING. This can be easily shown either by using the same (X, Y, R) as the proof for BIPARTITENESS, because a cycle with odd length has no matching, or by noting that BIPARTITE MATCHING is a special case of GRAPH MATCHING. □

It is interesting to note that we can also prove the above theorem by Alb_3. For example, for BIPARTITE MATCHING, we choose X, Y, R in the same way, and let $w(x, y) = 1$ for all $(x, y) \in R$. Let $u(x, y, e) = 1/\sqrt{n}$ if e is a horizontal edge $(\tau(i), \sigma(i))$ in x, and $u(x, y, e) = \sqrt{n}$ if $e = (\tau(i), \sigma(j))$ or $e = (\tau(j), \sigma(i))$ in x. Thus $u_{x,e} = \Theta(\sqrt{n})$ for all edges e, it is the same for $v_{y,e}$, thus $w_x/u_{x,e} = \Theta(n^{1.5})$, $w_y/v_{y,e} = \Theta(n^{1.5})$, and $Q_2(f) = \Omega(n^{1.5})$ by Alb_3.

This coincidence is not accidental. Actually it turns out that we can always show a lower bound by Alb_3 provided that it can be shown by Alb_2.

Theorem 6. $Alb_2(f) \leqslant Alb_3(f)$.

Proof. For any X, Y, R in Theorem 2, we set the weight functions in Theorem 3 as follows. Let $w(x, y) = 1$, $u(x, y, i) = \sqrt{l_{\max}}/l_{x,i}$ and $v(x, y, i) = \sqrt{l_{\max}}/l_{y,i}$. It's easy to check that

$$u(x, y, i)v(x, y, i) = \frac{l_{\max}}{l_{x,i} l_{y,i}} \geqslant 1 = w(x, y).$$

Now that $u(x, y, i)$ is independent on y, so we have $u_{x,i} = l_{x,i} u(x, y, i) = \sqrt{l_{\max}}$. Symmetrically, it follows that $v_{y,i} = \sqrt{l_{\max}}$. Thus, by denoting $m_x = |\{y : (x, y) \in R\}|$ and $m_y = |\{x : (x, y) \in R\}|$, we have

$$\min_{x,i} \frac{w_x}{u_{x,i}} \min_{y,i} \frac{w_y}{v_{y,i}} = \min_{x,i} \frac{m_x}{\sqrt{l_{\max}}} \min_{y,i} \frac{m_y}{\sqrt{l_{\max}}} = \frac{m}{\sqrt{l_{\max}}} \frac{m'}{\sqrt{l_{\max}}} = \frac{mm'}{l_{\max}}$$

which means that for any X, Y, R in Theorem 2, the lower bound result can be also achieved by Theorem 3. □

3. Limitations of Ambainis lower bounds

In this section, we show some bounds for the Alb's in terms of certificate complexity. We consider Boolean functions.

Definition 7. For an N-ary Boolean function $f : I^N \to \{0, 1\}$ and an input $x \in I^N$, a certificate set CS_x of f on x is a set of indices such that $f(x) = f(y)$ whenever $y_i = x_i$ for all $i \in CS_x$. The certificate complexity $C(f, x)$ of f on x is the size of a smallest certificate set of f on x. The b-certificate complexity of f is $C_b(f) = \max_{x:f(x)=b} C(f, x)$. The certificate complexity of f is $C(f) = \max\{C_0(f), C_1(f)\}$. We further denote $C_-(f) = \min\{C_0(f), C_1(f)\}$.

3.1. A general limitation for Ambainis lower bounds

In this subsection, we give an upper bound for $Alb_3(f)$, which implies a limitation of all the three known Ambainis lower bound techniques.

Theorem 8. *$Alb_3(f) \leqslant \sqrt{N \cdot C_-(f)}$, for any N-ary Boolean function f.*

Proof. Actually we prove a stronger result: for any (X, Y, R, u, v, w) as in Theorem 3,

$$\min_{(x,y)\in R, i\in[N]} \frac{w_x w_y}{u_{x,i} v_{y,i}} \leqslant NC_-(f).$$

With out loss of generality, we assume that $C_-(f) = C_0(f)$, and $X \subseteq f^{-1}(0)$ and $Y \subseteq f^{-1}(1)$. We can actually further assume that $R = X \times Y$, because otherwise we just let $R' = X \times Y$, and set new weight functions as follows.

$$u'(x, y, i) = \begin{cases} u(x, y, i) & (x, y) \in R, \\ 0 & \text{otherwise}, \end{cases}$$

$$v'(x, y, i) = \begin{cases} v(x, y, i) & (x, y) \in R, \\ 0 & \text{otherwise}, \end{cases}$$

$$w'(x, y) = \begin{cases} w(x, y) & (x, y) \in R, \\ 0 & \text{otherwise}. \end{cases}$$

Then it is easy to see that it satisfies (1) so it is also a weight scheme. And for these new weight functions, we have $u'_{x,i} = \sum_{y:(x,y)\in R', x_i \neq y_i} u'(x, y, i) = \sum_{y:(x,y)\in R, x_i\neq y_i} u(x, y, i) = u_{x,i}$ and similarly $v'_{y,i} = v_{y,i}$ and $w'_x = w_x$, $w'_y = w_y$.[3] It follows that $w_x w_y / u_{x,i} v_{y,i} = w'_x w'_y / u'_{x,i} v'_{y,i}$, thus we can use (X', Y', R', u', v', w') to derive the same lower bound as we use (X, Y, R, u, v, w).

[3] Note that the function values of u', v', w' are zero when $(x, y) \neq R$, which does not conform to the definition of weight scheme. But actually Theorem 3 also holds for $u \geqslant 0$, $v \geqslant 0$, $w \geqslant 0$ as long as $u_{x,i}$, $v_{y,i}$, w_x, w_y are all strictly positive for any x, y, i. This can be seen from the proof of Alb_4 in Section 4.

So we now suppose $R = X \times Y$ and prove that $\exists x \in X, y \in Y, i \in [N]$, *s.t.*

$$w_x w_y \leqslant N \cdot C_0(f) u_{x,i} v_{y,i}.$$

Suppose the claim is not true. Then for all $x \in X, y \in Y, i \in [N]$, we have

$$w_x w_y > N \cdot C_0(f) u_{x,i} v_{y,i}. \tag{2}$$

We first fix i for the moment. And for each $x \in X$, we fix a smallest certificate set CS_x of f on x. Clearly $|CS_x| \leqslant C_0(f)$. We sum (2) over $\{x \in X : i \in CS_x\}$ and $\{y \in Y\}$. Then we get

$$\left(\sum_{x\in X:\ i\in CS_x} w_x\right)\left(\sum_{y\in Y} w_y\right) > N \cdot C_0(f)\left(\sum_{x\in X:\ i\in CS_x} u_{x,i}\right)\left(\sum_{y\in Y} v_{y,i}\right). \tag{3}$$

Note that $\sum_{y\in Y} w_y = \sum_{x\in X, y\in Y} w(x,y) = \sum_{x\in X} w_x$, and that $\sum_{y\in Y} v_{y,i} = \sum_{x\in X, y\in Y: x_i\neq y_i} v(x,y,i) = \sum_{x\in X} v_{x,i}$ where $v_{x,i} = \sum_{y\in Y: x_i\neq y_i} v(x,y,i)$. Inequality (3) now turns to

$$\begin{aligned}\left(\sum_{x\in X:\ i\in CS_x} w_x\right)\left(\sum_{x\in X} w_x\right) &> N \cdot C_0(f)\left(\sum_{x\in X:\ i\in CS_x} u_{x,i}\right)\left(\sum_{x\in X} v_{x,i}\right)\\ &\geqslant N \cdot C_0(f)\left(\sum_{x\in X:\ i\in CS_x} u_{x,i}\right)\left(\sum_{x\in X:\ i\in CS_x} v_{x,i}\right)\\ &\geqslant N \cdot C_0(f)\left(\sum_{x\in X:\ i\in CS_x} \sqrt{u_{x,i}v_{x,i}}\right)^2\end{aligned}$$

by the Cauchy–Schwartz Inequality. We further note that

$$\begin{aligned}u_{x,i}v_{x,i} &= \left(\sum_{y\in Y: x_i\neq y_i} u(x,y,i)\right)\left(\sum_{y\in Y: x_i\neq y_i} v(x,y,i)\right)\\ &\geqslant \left(\sum_{y\in Y: x_i\neq y_i} \sqrt{u(x,y,i)v(x,y,i)}\right)^2\\ &\geqslant \left(\sum_{y\in Y: x_i\neq y_i} w(x,y)\right)^2\\ &= (w_{x,i})^2\end{aligned}$$

where we define $w_{x,i} = \sum_{y\in Y: x_i\neq y_i} w(x,y)$. Thus

$$\left(\sum_{x\in X:\ i\in CS_x} w_x\right)\left(\sum_{x\in X} w_x\right) > N \cdot C_0(f)\left(\sum_{x\in X:\ i\in CS_x} w_{x,i}\right)^2. \tag{4}$$

Now we sum (4) over $i = 1, \ldots, N$, and note that

$$\sum_i \sum_{x\in X:\ i\in CS_x} w_x = \sum_{x\in X} \sum_{i: i\in CS_x} w_x \leqslant C_0(f) \sum_{x\in X} w_x$$

because $|CS_x| \leqslant C_0(f)$ for each x. We have

$$\left(\sum_{x\in X} w_x\right)^2 > N \sum_{i=1}^{N} \left(\sum_{x\in X:\ i\in CS_x} w_{x,i}\right)^2 .$$

By the arithmetic-square average inequality (or by Cauchy–Schwartz Inequality)

$$N(a_1^2 + \cdots + a_N^2) \geqslant (a_1 + \cdots + a_N)^2,$$

we have

$$\left(\sum_{x\in X} w_x\right)^2 > \left(\sum_{x\in X, i\in[N]:\ i\in CS_x} w_{x,i}\right)^2 = \left(\sum_{x\in X, i\in[N], y\in Y:\ i\in CS_x, x_i\neq y_i} w(x,y)\right)^2$$

$$= \left(\sum_{x\in X, y\in Y}\ \sum_{i\in[N]:\ i\in CS_x, x_i\neq y_i} w(x,y)\right)^2 .$$

But by the definition of certificate, we know that for any x and y there is at least one index $i \in CS_x$ *s.t.* $x_i \neq y_i$. Therefore, we derive an inequality

$$\left(\sum_{x\in X} w_x\right)^2 > \left(\sum_{x\in X, y\in Y} w(x,y)\right)^2 = \left(\sum_{x\in X} w_x\right)^2$$

which is a contradiction, as desired. □

We add some comments about this upper bound of Alb_3. First, this bound looks weak at first glance because the $\sqrt{N}$ factor seems too large. But in fact it is necessary. Consider the problem of INVERT A PERMUTATION [4],[4] where $C_0(f) = C_1(f) = 1$ but even the $Alb_2(f) = \Omega(\sqrt{N})$.

Second, the quantum query complexity of ELEMENT DISTINCTNESS is known to be $\Theta(N^{2/3})$. The lower bound part is obtained by Shi [27] (for large range) and Ambainis [7] (for small range); the upper bound part is obtained by Ambainis [8]. Observe that $C_1(f) = 2$ thus $\sqrt{NC_1(f)} = \Theta(N)$, we derive the following interesting corollary from the above theorem.

Corollary 9. *Alb_3 is not tight.*

We make some remarks on the quantity $\sqrt{N \cdot C_-(f)}$ to end this subsection. A function f is symmetric if $f(x_1 \ldots x_N) = f(x_{\sigma(1)} \ldots x_{\sigma(n)})$ for any input x and any permutation σ on $[N]$. In [11], Beals et al. prove that $Q_2(f) = \Theta(\sqrt{N(N-\Gamma(f))})$ by using Paturi's result $\widetilde{deg}(f) = \Theta(\sqrt{N(N-\Gamma(f))})$ [23], where $\Gamma(f) = \min\{|2k-n+1| : f_k \neq k_{k+1}, 0 \leqslant k \leqslant n-1\}$. It is not hard to show that $\Gamma(f) = N - \Theta(C_-(f))$ for symmetric function f. Thus we know that both $\widetilde{deg}(f)$ and $Q_2(f)$ are $\Theta(\sqrt{N \cdot C_-(f)})$ for symmetric function f.

[4] The original problem is not a Boolean function, but we can define a Boolean-valued version of it. Instead of finding the position i with $x_i = 1$, we are to decide whether i is odd or even. The original proof of the $\Omega(\sqrt{N})$ lower bound still holds.

3.2. Two better upper bounds for total functions

It turns out that if the function is total, then the upper bound can be further tightened. We introduce a new measure which basically characterizes the size of intersection of a 0 and 1-certificate sets.

Definition 10. For any function f, if there is a certificate set assignment $CS : \{0,1\}^N \to 2^{[N]}$ such that for any inputs x, y with $f(x) \neq f(y)$, $|CS_x \cap CS_y| \leqslant k$, then k is called a candidate certificate intersection complexity of f. The minimal candidate certificate intersection complexity of f is called the certificate intersection complexity of f, denoted by $CI(f)$. In other words,

$$CI(f) = \min_{CS} \max_{x,y: f(x) \neq f(y)} |CS_x \cap CS_y|.$$

Now we give the following theorem which improves Theorem 8 for total functions. Note that $CI(f) \leqslant C_-(f)$ by the definition of $CI(f)$.

Theorem 11. *$Alb_3(f) \leqslant \sqrt{N \cdot CI(f)}$, for any N-ary total Boolean function f.*

Proof. Again, we prove a stronger result that for any (X, Y, R, u, v, w) in Theorem 3,

$$\min_{(x,y)\in R, i\in[N]} \frac{w_x w_y}{u_{x,i} v_{y,i}} \leqslant N \cdot CI(f).$$

Similar to the proof for Theorem 8, we assume without loss of generality that $R = X \times Y$ and for all $x \in X$, $y \in Y$, we have

$$w_x w_y > N \cdot CI(f)\, u_{x,i} v_{y,i}. \tag{5}$$

We shall show a contradiction as follows. Fix i and sum (5) over $\{x \in X : i \in CS_x\}$ and $\{y \in Y : i \in CS_y\}$, we get

$$\begin{aligned}
&\sum_{x\in X, y\in Y:\, i\in CS_x\cap CS_y} w_x w_y \\
&\quad > N \cdot CI(f) \left(\sum_{x\in X:\, i\in CS_x} u_{x,i}\right)\left(\sum_{y\in Y:\, i\in CS_y} v_{y,i}\right) \\
&\quad = N \cdot CI(f) \left(\sum_{x\in X, y\in Y:\, i\in CS_x, x_i\neq y_i} u(x,y,i)\right) \\
&\qquad \cdot \left(\sum_{x\in X, y\in Y:\, i\in CS_y, x_i\neq y_i} v(x,y,i)\right) \\
&\quad \geqslant N \cdot CI(f) \left(\sum_{x\in X, y\in Y:\, i\in CS_x\cap CS_y, x_i\neq y_i} u(x,y,i)\right) \\
&\qquad \times \left(\sum_{x\in X, y\in Y:\, i\in CS_x\cap CS_y, x_i\neq y_i} v(x,y,i)\right)
\end{aligned}$$

$$\geqslant N \cdot CI(f) \left(\sum_{x\in X, y\in Y:\ i\in CS_x\cap CS_y, x_i\neq y_i} \sqrt{u(x,y,i)v(x,y,i)} \right)^2$$

$$\geqslant N \cdot CI(f) \left(\sum_{x\in X, y\in Y:\ i\in CS_x\cap CS_y, x_i\neq y_i} w(x,y) \right)^2 .$$

Now sum over $i = 1, \ldots, N$, we get

$$\sum_{x\in X, y\in Y, i\in[N]:\ i\in CS_x\cap CS_y} w_x w_y$$
$$> N \cdot CI(f) \sum_{i=1}^{N} \left(\sum_{x\in X, y\in Y:\ i\in CS_x\cap CS_y, x_i\neq y_i} w(x,y) \right)^2$$
$$\geqslant CI(f) \left(\sum_{x\in X, y\in Y, i\in[N]:\ i\in CS_x\cap CS_y, x_i\neq y_i} w(x,y) \right)^2 .$$

Note that for total function f, if $f(x) \neq f(y)$, there is at least one position $i \in CS_x \cap CS_y$ *s.t.* $x_i \neq y_i$. Thus

$$\sum_{x\in X, y\in Y, i\in[N]:\ i\in CS_x\cap CS_y, x_i\neq y_i} w(x,y) \geqslant \sum_{x\in X, y\in Y} w(x,y).$$

On the other hand, by the definition of $CI(f)$, we have

$$\sum_{x\in X, y\in Y, i\in[N]:\ i\in CS_x\cap CS_y} w_x w_y \leqslant CI(f) \sum_{x\in X, y\in Y} w_x w_y$$
$$= CI(f) \left(\sum_{x\in X, y\in Y} w(x,y) \right)^2 .$$

Therefore we get a contradiction

$$CI(f) \left(\sum_{x\in X, y\in Y} w(x,y) \right)^2 > CI(f) \left(\sum_{x\in X, y\in Y} w(x,y) \right)^2$$

as desired. □

AND-OR TREE is a famous problem in both classical and quantum computation. In the problem, there is a complete binary tree with height $2n$. Any node in odd levels is labeled with AND and any node in even levels is labeled with OR. The $N = 4^n$ leaves are the input variables, and the value of the function is the value that we get at the root, with value of each internal node calculated from the values of its two children in the common AND/OR interpretation. The classical randomized decision tree complexity for AND-OR TREE is known to be $\Theta((\frac{1+\sqrt{33}}{4})^n) = \Theta(N^{0.753\ldots})$ by Saks and Wigderson in [25] and Santha in [26]. The best known quantum lower bound is $\Omega(\sqrt{N})$ by Barnum and Saks in [9] and best known quantum upper bound is the same as the best classical randomized one. Note that $C_-(\text{AND-OR TREE}) = 2^n = \sqrt{N}$ and thus $\sqrt{NC_-(f)} = N^{3/4}$. So if we only use

Theorem 8, it seems that we still have chances to improve the known $\Omega(\sqrt{N})$ lower bound by Alb_3. But by Theorem 11 we know that actually it is impossible.

Corollary 12. $Alb_3(\text{AND-OR TREE}) \leqslant \sqrt{N}$.

Proof. It is sufficient to prove that there is a certificate assignment CS *s.t.* $|CS_x \cap CS_y| = 1$ for any $f(x) \neq f(y)$. In fact, by a simple induction, we can prove that the standard certificate assignment satisfies this property. The base case is trivial. For the induction step, we note that for an AND connection of two subtrees, the 0-certificate set of the new larger tree can be chosen as any one of the two 0-certificate sets of the two subtrees, and the 1-certificate set of the new larger tree can be chosen as the union of the two 1-certificate sets of the two subtrees. As a result, the intersection of the two new certificate sets is not enlarged. The OR connection of two subtrees is analyzed in the same way. Thus the intersection of the final 0- and 1-certificate sets is of size 1. □

We can tighten the $\sqrt{N \cdot C_-(f)}$ upper bound in another way and get the following result which also implies Corollary 12.

Theorem 13. *$Alb_3(f) \leqslant \sqrt{C_0(f)C_1(f)}$, for any total Boolean function f.*

Proof. For any (X, Y, R, u, v, w) in Theorem 3, we assume without loss of generality that $X \subseteq f^{-1}(0)$, $Y \subseteq f^{-1}(1)$ and $R = X \times Y$. We are to prove $\exists x, y, i, j$ *s.t.* $w_x w_y \leqslant C_0(f)C_1(f)u_{x,i}v_{y,j}$. Suppose this is not true, i.e. for all $x \in X$, $y \in Y$, $i, j \in [N]$, $w_x w_y > C_0(f)C_1(f)u_{x,i}v_{y,j}$. First fix x, y and sum over $i \in CS_x$ and $j \in CS_y$. Since $|CS_x| \leqslant C_0(f)$, $|CS_y| \leqslant C_1(f)$, we have

$$w_x w_y > \sum_{i \in CS_x} u_{x,i} \sum_{j \in CS_y} v_{y,j}.$$

Now we sum over $x \in X$ and $y \in Y$,

$$\begin{aligned}\left(\sum_{x \in X} w_x\right)\left(\sum_{y \in Y} w_y\right) &> \left(\sum_{x \in X, i \in CS_x} u_{x,i}\right)\left(\sum_{y \in Y, j \in CS_y} v_{y,j}\right) \\ &= \left(\sum_{x \in X, y \in Y, i \in [N]: x_i \neq y_i, i \in CS_x} u(x, y, i)\right) \\ &\quad \times \left(\sum_{x \in X, y \in Y, j \in [N]: x_j \neq y_j, j \in CS_y} v(x, y, j)\right).\end{aligned}$$

Since f is total, there is at least one $i_0 \in CS_x \cap CS_y$ *s.t.* $x_{i_0} \neq y_{i_0}$.

$$\begin{aligned}\left(\sum_{x \in X} w_x\right)\left(\sum_{y \in Y} w_y\right) &> \left(\sum_{x \in X, y \in Y} u(x, y, i_0)\right)\left(\sum_{x \in X, y \in Y} v(x, y, i_0)\right) \\ &\geqslant \left(\sum_{x \in X, y \in Y} \sqrt{u(x, y, i_0)v(x, y, i_0)}\right)^2\end{aligned}$$

$$
\begin{aligned}
&\geqslant \left(\sum_{x\in X, y\in Y} w(x,y) \right)^2 \\
&= \left(\sum_{x\in X} w_x \right) \left(\sum_{y\in Y} w_y \right)
\end{aligned}
$$

which is a contradiction. □

Finally, we remark that even these two improved upper bounds of $Alb_3(f)$ are not always tight. For example, Sun, Yao and Zhang prove [31] that graph property SCORPION, directed graph property SINK and a circular function all have $Q_2(f) = \tilde{\Theta}(\sqrt{n})$, but both $\sqrt{C_0(f)C_1(f)}$ and $\sqrt{N \cdot CI(f)}$ are $\Theta(n)$.

4. A further generalized Ambainis lower bound

While Alb_2 and Alb_3 use different ideas to generalize Alb_1, it is natural to combine both and get a further generalization. The following theorem is a result in this direction. This theorem is to Theorem 3 is as Theorem 2 is to Theorem 1. The proof is similar to the ones in [4,5], with inner products substituted for density operators to make it look easier. [5]

Theorem 14. *Let $f : I^N \to \{0,1\}$ where I is a finite set, and X, Y be two sets of inputs* s.t. *$f(x) \neq f(y)$ if $x \in X$ and $y \in Y$. Let $R \subseteq X \times Y$. Let w, u, v be a weight scheme for X, Y, R. Then*

$$
Q_2(f) = \Omega\left(\sqrt{\min_{(x,y)\in R, i\in[N], x_i\neq y_i} \frac{w_x w_y}{u_{x,i} v_{y,i}}} \right).
$$

Proof. The query computation is a sequence of operations $U_0 \to O_x \to U_1 \to \cdots \to U_T$ on some fixed initial state, say $|0\rangle$. Note that here T is the number of queries. Denote $|\psi_x^k\rangle = U_{k-1}O_x \ldots U_1 O_x U_0 |0\rangle$. Note that $|\psi_x^0\rangle = |0\rangle$ for all input x. Because the computation is correct with high probability $(1-\varepsilon)$, for any $(x,y) \in R$, the two final states have to have some distance to let the measurement distinguish them. In other words, we can assume that $|\langle \psi_x^T | \psi_y^T \rangle| \leqslant c$ for some constant $c < 1$. Now suppose that

$$
|\psi_x^{k-1}\rangle = \sum_{i,a,z} \alpha_{i,a,z} |i,a,z\rangle, \quad |\psi_y^{k-1}\rangle = \sum_{i,a,z} \beta_{i,a,z} |i,a,z\rangle,
$$

where i is for the index address, a is for the answer, and z is the workspace. Then the oracle works as follows.

$$
\begin{aligned}
O_x |\psi_x^{k-1}\rangle &= \sum_{i,a,z} \alpha_{i,a,z} |i, a\oplus x_i, z\rangle = \sum_{i,a,z} \alpha_{i,a\oplus x_i,z} |i,a,z\rangle, \\
O_y |\psi_y^{k-1}\rangle &= \sum_{i,a,z} \beta_{i,a,z} |i, a\oplus y_i, z\rangle = \sum_{i,a,z} \beta_{i,a\oplus y_i,z} |i,a,z\rangle.
\end{aligned}
$$

[5] This idea was mentioned in Ambainis' original paper [4] and was also used in some other papers such as [19].

So we have

$$\begin{aligned}\langle\psi_x^k|\psi_y^k\rangle &= \sum_{i,a,z}\alpha^*_{i,a\oplus x_i,z}\beta_{i,a\oplus y_i,z}\\ &= \sum_{i,a,z:x_i=y_i}\alpha^*_{i,a\oplus x_i,z}\beta_{i,a\oplus y_i,z}+\sum_{i,a,z:x_i\neq y_i}\alpha^*_{i,a\oplus x_i,z}\beta_{i,a\oplus y_i,z}\\ &= \langle\psi_x^{k-1}|\psi_y^{k-1}\rangle+\sum_{i,a,z:x_i\neq y_i}\alpha^*_{i,a\oplus x_i,z}\beta_{i,a\oplus y_i,z}-\sum_{i,a,z:x_i\neq y_i}\alpha^*_{i,a,z}\beta_{i,a,z}.\end{aligned}$$

Thus

$$\begin{aligned}1-c = 1-|\langle\psi_x^T|\psi_y^T\rangle| &= \sum_{k=1}^T\left(|\langle\psi_x^{k-1}|\psi_y^{k-1}\rangle|-|\langle\psi_x^k|\psi_y^k\rangle|\right)\\ &\leqslant \sum_{k=1}^T|\langle\psi_x^{k-1}|\psi_y^{k-1}\rangle-\langle\psi_x^k|\psi_y^k\rangle|\\ &= \sum_{k=1}^T\left|\sum_{i,a,z:x_i\neq y_i}(\alpha^*_{i,a\oplus x_i,z}\beta_{i,a\oplus y_i,z}-\alpha^*_{i,a,z}\beta_{i,a,z})\right|\\ &\leqslant \sum_{k=1}^T\sum_{i,a,z:x_i\neq y_i}(|\alpha_{i,a\oplus x_i,z}||\beta_{i,a\oplus y_i,z}|+|\alpha_{i,a,z}||\beta_{i,a,z}|).\end{aligned}$$

Summing up the inequalities for all $(x,y)\in R$, with weight $w(x,y)$ multiplied, yields

$$\begin{aligned}&(1-c)\sum_{(x,y)\in R}w(x,y)\\ &\leqslant\sum_{k=1}^T\sum_{(x,y)\in R}\sum_{i,a,z:x_i\neq y_i}w(x,y)(|\alpha_{i,a\oplus x_i,z}||\beta_{i,a\oplus y_i,z}|+|\alpha_{i,a,z}||\beta_{i,a,z}|)\\ &\leqslant\sum_{k=1}^T\sum_{(x,y)\in R}\sum_{i,a,z:x_i\neq y_i}\sqrt{u(x,y,i)v(x,y,i)}(|\alpha_{i,a\oplus x_i,z}||\beta_{i,a\oplus y_i,z}|\\ &\quad+|\alpha_{i,a,z}||\beta_{i,a,z}|)\\ &=\sum_{k=1}^T\sum_{i,a,z}\sum_{(x,y)\in R:x_i\neq y_i}\sqrt{u(x,y,i)v(x,y,i)}(|\alpha_{i,a\oplus x_i,z}||\beta_{i,a\oplus y_i,z}|\\ &\quad+|\alpha_{i,a,z}||\beta_{i,a,z}|)\end{aligned}$$

by (1). We then use inequality $2AB\leqslant A^2+B^2$ to get

$$\begin{aligned}&\sqrt{u(x,y,i)v(x,y,i)}|\alpha_{i,a\oplus x_i,z}||\beta_{i,a\oplus y_i,z}|\\ &\leqslant\frac{1}{2}\left(u(x,y,i)\sqrt{\frac{v_{y,i}}{u_{x,i}}\frac{w_x}{w_y}}|\alpha_{i,a\oplus x_i,z}|^2+v(x,y,i)\sqrt{\frac{u_{x,i}}{v_{y,i}}\frac{w_y}{w_x}}|\beta_{i,a\oplus y_i,z}|^2\right),\end{aligned}$$

and

$$\begin{aligned}&\sqrt{u(x,y,i)v(x,y,i)}|\alpha_{i,a,z}||\beta_{i,a,z}|\\ &\leqslant\frac{1}{2}\left(u(x,y,i)\sqrt{\frac{v_{y,i}}{u_{x,i}}\frac{w_x}{w_y}}|\alpha_{i,a,z}|^2+v(x,y,i)\sqrt{\frac{u_{x,i}}{v_{y,i}}\frac{w_y}{w_x}}|\beta_{i,a,z}|^2\right).\end{aligned}$$

Denote $A = \min_{x,y,i:(x,y)\in R, x_i \neq y_i} w_x w_y / u_{x,i} v_{y,i}$. Note that

$$\sum_{y:(x,y)\in R, x_i\neq y_i} u(x,y,i) = u_{x,i}, \qquad \sum_{x:(x,y)\in R, x_i\neq y_i} v(x,y,i) = v_{y,i}$$

by the definition of $u_{x,i}$ and $v_{y,i}$, we have

$$\begin{aligned}
(1-c)\sum_{(x,y)\in R} w(x,y) &\leqslant \frac{1}{2}\sum_{k=1}^{T}\sum_{i,a,z}\left[\sum_{x\in X}\sqrt{\frac{u_{x,i}v_{y,i}}{w_x w_y}}w_x(|\alpha_{i,a\oplus x_i,z}|^2 + |\alpha_{i,a,z}|^2)\right.\\
&\quad\left. + \sum_{y\in Y}\sqrt{\frac{u_{x,i}v_{y,i}}{w_x w_y}}w_y(|\beta_{i,a\oplus y_i,z}|^2 + |\beta_{i,a,z}|^2)\right]\\
&\leqslant \frac{1}{2}\sum_{k=1}^{T}\left[\sum_{x\in X}\sqrt{1/A}w_x\sum_{i,a,z}(|\alpha_{i,a\oplus x_i,z}|^2 + |\alpha_{i,a,z}|^2)\right.\\
&\quad\left. + \sum_{y\in Y}\sqrt{1/A}w_y\sum_{i,a,z}(|\beta_{i,a\oplus y_i,z}|^2 + |\beta_{i,a,z}|^2)\right]\\
&= \sqrt{1/A}\sum_{k=1}^{T}\left(\sum_{x\in X} w_x + \sum_{y\in Y} w_y\right)\\
&= 2T\sqrt{1/A}\sum_{(x,y)\in R} w(x,y)
\end{aligned}$$

by noting that $\sum_x w_x = \sum_y w_y = \sum_{(x,y)\in R} w(x,y)$. Therefore, $T = \Omega(\sqrt{A})$. □

We denote by $Alb_4(f)$ the best possible lower bound for function f achieved by this theorem. It is easy to see that Alb_4 generalizes Alb_3. However, according to a recent result by Spalek and Szegedy [30], Alb_3, Alb_4 and the quantum adversary method proposed by Barnum, Saks and Szegedy in [10] are all equivalent. Thus we cannot use Alb_4 to get better lower bounds than using Alb_3. However, Alb_4 may be easier to use in some cases.

Acknowledgements

This research was supported in part by NSF grant CCR-0310466. The author would like to thank Andrew Yao who introduced the quantum algorithm and quantum query complexity area to me, and made invaluable comments to this paper. Yaoyun Shi and Xiaoming Sun also read a preliminary version of the present paper and both, esp. Yaoyun Shi, gave many invaluable comments and corrections. Thanks also to Andris Ambainis for telling that it is still open whether $Alb_2(f) \leqslant \sqrt{C_0(f)C_1(f)}$ is true for total functions, and to Mario Szegedy for sending me a preliminary version of [30].

References

[1] S. Aaronson, Quantum lower bound for the collision problem, in: Proc. 34th Annu. ACM Symp. on Theory of Computing, 2002, pp. 635–642.

[2] S. Aaronson, Lower bounds for local search by quantum arguments, in: Proc. 36th Annu. ACM Symp. on Theory of Computing, 2004, pp. 465–474.

[4] A. Ambainis, Quantum lower bounds by quantum arguments, J. Comput. System Sci. 64 (2002) 750–767.

[5] A. Ambainis, Polynomial degree vs quantum query complexity, in: Proc. 44th Annu. IEEE Symp. on Foundations of Computer Science, 2003, pp. 230–239.

[6] A. Ambainis, Quantum query algorithms and lower bounds, Proc. FOTFS III, to appear.

[7] A. Ambainis, Quantum lower bounds for collision and element distinctness with small range, quant-ph/0305179.

[8] A. Ambainis, Quantum walk algorithmn for element distinctness, Proc. 45th Annu. IEEE Symp. on Foundations of Computer Science, 2004, pp. 22–31.

[9] H. Barnum, M. Saks. A lower bound on the quantum query complexity of read-once functions, J. Comput. System Sci. 69 (2) (2004) 244–258.

[10] H. Barnum, M. Saks, M. Szegedy, Quantum query complexity and semidefinite programming, in: Proc. 18th Annu. IEEE Conf. on Computational Complexity, 2003, pp. 179–193.

[11] R. Beals, H. Buhrman, R. Cleve, M. Mosca, R. deWolf, Quantum lower bounds by polynomials, J. ACM 48 (2001) 778–797.

[12] Berzina, Dubrovsky, Freivalds, Lace, Scegulnaja, Quantum query complexity for some graph problems, in: Proc. 30th Conf. on Current Trends in Theory and Practice of Computer Science, 2004, pp. 140–150.

[13] H. Buhrman, R. Cleve, A. Wigderson, Quantum vs. classical communication and computation, in: Proc. 34th Annu. ACM Symp. on Theory of Computing, 1998, pp. 63–68.

[14] H. Buhrman, Ch. Durr, M. Heiligman, P. Hoyer, F. Magniez, M. Santha, R. de Wolf, Quantum algorithms for element distinctness, in: Proc. 18th Annu. IEEE Conf. on Computational Complexity, 2001, pp. 131–137.

[15] H. Buhrman, R. de Wolf, Complexity measures and decision tree complexity: a survey, Theoret. Comput. Sci. 288 (1) (2002) 21–43.

[16] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, Proc. Royal Society of London A 439 (1992) 553–558.

[17] C. Durr, M. Heiligman, P. Hoyer, M. Mhalla, Quantum query complexity of some graph problems, in: Proc. 31st Int. Coll. on Automata, Languages, and Programming, 2004, pp. 481–493.

[18] L. Grover, A fast quantum mechanical algorithm for database search, in: Proc. 28th Annu. ACM Symp. on the Theory of Computing, 1996, pp. 212–219.

[19] P. Hoyer, J. Neerbek, Y. Shi, Quantum lower bounds of ordered searching, sorting and element distinctness, Algorithmica 34 (2002) 429–448.

[20] S. Laplante, F. Magniez, Lower bounds for randomized and quantum query complexity using Kolmogorov arguments, Proc. 19th Annu. IEEE Conf. on Computational Complexity, 2004, pp. 294–304. Preliminary version at quant-ph/0311189.

[22] A. Nayak, F. Wu, The quantum query complexity of approximating the median and related statistics, in: Proc. 31st Annu. ACM Symp. on the Theory of Computing, 1999, pp. 384–393.

[23] R. Paturi, On the degree of polynomials that approximate symmetric Boolean functions, in: Proc. 24th Annu. ACM Symp. on the Theory of Computing, 1992, pp. 468–474.

[24] A. Razborov, Quantum communication complexity of symmetric predicates, Izvestiya of the Russian Academy of Science, Mathematics, 2002.

[25] M. Saks, A. Wigderson, Probabilistic Boolean decision trees and the complexity of evaluating game trees, in: Proc. 27th Annu. Symp. on Foundations of Computer Science, 1986, pp. 29–38.

[26] M. Santha, On the Monte Carlo Boolean decision tree complexity of read-once formulae, in: Proc. 6th Annu. Struct. in Complexity Theory Conference, 1991, pp. 180–187.

[27] Y. Shi, Quantum lower bounds for the collision and the element distinctness problems, in: Proc. 43rd Symp. on Foundations of Computer Science, 2002, pp. 513–519.

[28] P. Shor, Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (1997) 1484–1509.

[29] D. Simon, On the power of quantum computation, SIAM J. Comput. 26 (1997) 1474–1483.

[30] R. Spalek, M. Szegedy, All quantum adversary methods are equivalent. quant-ph/0409116.

[31] X. Sun, A.C. Yao, S. Zhang, Graph property and circular functions: how low can quantum query complexity go?, in: Proc. 19th Annu. IEEE Conf. on Computational Complexity, 2004, pp. 286–293.

[32] W. van Dam, Quantum oracle interrogation: getting all information for almost half the price, in: Proc. 39th IEEE Symp. on Foundations of Computer Science, 1998, pp. 362–367.

[33] S. Zhang, On the power of Ambainis' lower bounds, quant-ph/0311060.