The approximate degree, the quantum query complexity and the total influence

Yaoyun Shi* and Shengyu Zhang †

Abstract

In this note we show that the quantum query complexity is lower bounded by the total influence for any biased probability p. The same lower bounds holds for the approximate degree (with a log factor loss). This proves the quantum version of a recent result by O'Donnell and Servedio [8], and generalizes a result by Shi [12], who showed the special case of $p = 1/2$. Interestingly, the quantum lower bound does not use the assumption of monotonicity which O'Donnell and Servedio [8] used for the randomized result.

1 Introduction

The effect of symmetry on the *query complexity*, or called *decision tree complexity*, has drawn much attention from early 1970's. The most famous example is the Aanderaa-Rosenberg Conjecture [11], which says that any monotone n-node graph property has the deterministic decision tree complexity $\binom{n}{2}$. While this was settled (up to a constant factor) [6, 10], its randomized variant – which says that the randomized query complexity for any monotone graph property is $\Omega(n^2)$ – is still open. Yao made the first breakthrough by using the graph packing technique [13] to give a $\Omega(n \log^{1/12}(n))$ lower bound, and later King [5] and Hajnal [4] improved the result to $\Omega(n^{4/3})$ by more elaborative usage of the graph packing technique. This method seemed to be pushed to its limit: The only further improvement over the past two decades was by Chakrabarti and Khot [3] who proved a lower bound of $\Omega(n^{4/3} \log^{1/3}(n))$ along the same approach.

It is also natural to consider the quantum variant, *i.e.* the question whether any monotone graph property has the quantum query complexity $\Omega(n)$. Using the similar technique, Santha and Yao proved the $\Omega(n^{2/3})$ lower bound for the quantum query complexity (unpublished).

Very recently, O'Donnell, Saks, Schramm and Servedio used the *influence* of variables to give a new and much simpler proof of the $\Omega(n^{4/3})$ randomized lower bound [7]. We now give more details about this different approach.

For Boolean function $f : \{0,1\}^n \to \{0,1\}$, let μ_p be the distribution on $\{0,1\}^n$ *s.t.* $\mu_p(x) = p^{|x|}q^{n-|x|}$, where $q = 1-p$ and $|x|$ is the number of 1's in x. In other words, the distribution is obtained by independently letting each $x_i = 1$ with probability p. Define the influence of the i-th variable to be $\inf_i(f,p) = \mathbf{Pr}_{x\sim\mu_p}[f(x) \neq f(x^i)]$, where x^i is obtained from x by flipping the i-th variable of x, and $x \sim \mu_p$ means that x is drawn from the distribution p. The total influence is then defined as the summation of the influences of all variables, *i.e.* $\inf(f,p) = \sum_i \inf_i(f,p)$.

*Department of Electrical Engineering and Computer Science, University of Michigan, 1301 Beal Avenue, Ann Arbor, MI 48109-2122, USA. Email: shiyy@eecs.umich.edu

†Computer Science Department and Institute for Quantum Information, 1200 E California Bl., Pasadena, CA 91125, USA. Email: szhang@caltech.edu This work was mostly done when the author was a graduate student in Computer Science Department at Princeton University, supported in part by NSF grants CCR-0310466 and CCF-0426582.

Denote by $R(f)$ the error-free randomized decision tree complexity of f and by $Q_2(f)$ the 2-sided bounded error quantum query complexity of f. For more details about the decision tree and quantum query models, we refer to [2] as an excellent survey. What O'Donnell, Saks, Schramm and Servedio [7] showed is that

$$R(f) \geq \frac{\mathbf{Var}[f]}{pq \max_i \inf_i(f,p)}, \tag{1}$$

for any Boolean function f and any p. Another recent result by O'Donnell and Servedio [8] is

$$R(f) \geq pq \inf(f,p)^2, \tag{2}$$

for any *monotone* Boolean function f and any p. Using these two, one gets $R(f) \geq N^{2/3}/p_c^{1/3}$ for any monotone function f that is variant to any permutation from a transitive group, where p_c is a critical probability, *i.e.* $\mathbf{E}_{x\sim\mu_{p_c}}[f(x)] = 1/2$. Here N is the number of variables, corresponding to $\binom{n}{2}$ in graph properties, in the setting of which the lower bound is actually $\Omega(n^{4/3}/p_c^{1/3})$.

Since it is widely believed that the quantum and randomized query complexities for any total Boolean function is quadratically related, it is natural to conjecture

$$Q_2(f) \geq \Omega\left(\sqrt{\frac{\mathbf{Var}[f]}{pq \max_i \inf_i(f,p)}}\right) \tag{3}$$

for any Boolean function f and

$$Q_2(f) \geq \Omega(\sqrt{pq} \inf(f,p)) \tag{4}$$

for any monotone Boolean function f. Combining inequalities (3) and (4) we have $Q_2(f) \geq n^{2/3}$. Shi showed (4) in the case of $p = 1/2$ for any Boolean function [12].

In this note we prove (4) for any f (not necessarily monotone), generalizing Shi's result [12]. There are two main techniques for proving quantum lower bounds, one is the polynomial method [9], using the fact that the approximate degree is a lower bound for the quantum query complexity; the other is the quantum adversary method [1]. In this paper we will give two proofs for Inequality (4), one by each method. The one using the polynomial method only shows the case of monotone functions, and it has a log factor loss. However, it implies that the lower bounds not only holds for the quantum query complexity but also holds for the approximate degree. The proof using the quantum adversary method gives exactly the inequality (4) in a simple way. Interestingly, unlike the result (2) and our first proof mentioned above, the assumption of monotonicity is not needed in the second proof. This implies that the quantum lower bound of $\Omega(n^{2/3})$ actually hold not only for monotone transitive functions, but for all balanced transitive functions, unless the quantum and randomized query complexities have a super-quadratic gap, which is widely believed to be false for total functions.

2 Proofs

2.1 Proof by the polynomial method

Proposition 1 *For monotone f and any $p \in (0,1)$,*

$$Q_2(f) = \Omega\left(\frac{\sqrt{pq}\inf(f,p)}{\log n}\right) \tag{5}$$

where $q = 1 - p$.

Proof By simple probability amplification, we know that $Q_2(f)\log n \geq Q_{1/2n}(f)$, where $Q_{1/2n}(f)$ is the quantum query complexity with $1/2n$ error probability. (The standard definition of the quantum query complexity, $Q_2(f)$, only requires a small constant error probability.) Denote by $\widetilde{deg}_{1/2n}(f)$ a lowest degree of the polynomial approximating f with error no more than $1/2n$ for any input. Since $Q_{1/2n}(f) = \Omega(\widetilde{deg}_{1/2n}(f))$, it is enough to show that $\widetilde{deg}_{1/2n}(f) = \Omega(\sqrt{pq}\inf(f,p))$.

We will use Bernstein's Inequality, which says that any polynomial $r(t)$ with degree d and $\|r\|_{[-1,1]} = 1$ has $d \geq \sqrt{1-t^2}|r'(t)|$, $\forall t \in (-1,1)$. Denote by f_ϵ the best polynomial to approximate f up to ϵ, and let $\phi_p(f_\epsilon) = \mathbf{E}_{x\sim\mu_p}[f_\epsilon(x)]$. We will use Bernstein's Inequality for $\phi_p(f_\epsilon)$. By some simple scaling $t = 2p-1$, we know that $\sqrt{1-t^2} = 2\sqrt{pq}$. So it is enough to lower bound $\frac{d\phi_p(f_\epsilon)}{dp}$ by $\inf(f,p)$.

Let $\vec{p} = (p_1,...,p_n)$ and $\phi_{\vec{p}}(f_\epsilon) = \mathbf{E}_{x\sim\mu_p}[f_\epsilon(x)]$. Then $\frac{d\phi_p(f_\epsilon)}{dp} = \sum_i \frac{\partial\phi_{\vec{p}}(f_\epsilon)}{\partial p_i}|_{p_i=p}$ by chain law. We use $x_{[n]-i}$ to denote $x_1...x_{i-1}x_{i+1}...x_n$, and use $x_{[n]-i}\circ b$ to denote $x_1...x_{i-1}bx_{i+1}...x_n$ for $b \in \{0,1\}$. Fix $\epsilon = 1/2n$, then

$$\begin{aligned}
\frac{\partial\phi_{\vec{p}}(f_\epsilon)}{\partial p_i} &= (\partial\sum_x \mu_{\vec{p}}(x)f_\epsilon(x))/\partial p_i & (6)\\
&= (\partial\sum_{x:x_i=1}\mu_{\vec{p}}(x_{[n]-i})p_i f_\epsilon(x) + \sum_{x:x_i=0}\mu_{\vec{p}}(x_{[n]-i})(1-p_i)f_\epsilon(x))/\partial p_i & (7)\\
&= \sum_{x:x_i=1}\mu_{\vec{p}}(x_{[n]-i})f_\epsilon(x) - \sum_{x:x_i=0}\mu_{\vec{p}}(x_{[n]-i})f_\epsilon(x) & (8)\\
&= \sum_{x_{[n]-i}}\mu_{\vec{p}}(x_{[n]-i})(f_\epsilon(x_{[n]-i}\circ 1) - f_\epsilon(x_{[n]-i}\circ 0)) & (9)\\
&= \sum_{x_{[n]-i}\nsim i}\mu_{\vec{p}}(x_{[n]-i})\left[f_\epsilon(x_{[n]-i}\circ 1) - f_\epsilon(x_{[n]-i}\circ 0)\right] & (10)\\
&\quad + \sum_{x_{[n]-i}\sim i}\mu_{\vec{p}}(x_{[n]-i})\left[(f_\epsilon(x_{[n]-i}\circ 1) - f_\epsilon(x_{[n]-i}\circ 0)\right] & (11)
\end{aligned}$$

where $x_{[n]-i}\sim i$ means $x_{[n]-i}$ is sensitive at i, *i.e.* $f(x_{[n]-i}\circ 1) \neq f(x_{[n]-i}\circ 0)$. Since f_ϵ approximates f, we know that for $x_{[n]-i}\nsim i$, $-2\epsilon \leq f_\epsilon(x_{[n]-i}\circ 1) - f_\epsilon(x_{[n]-i}\circ 0) \leq 2\epsilon$. And for $x_{[n]-i}\sim i$, we have $f(x_{[n]-i}\circ 1) = 1$ and $f(x_{[n]-i}\circ 0) = 0$ because f is monotone, and thus $f_\epsilon(x_{[n]-i}\circ 1) - f_\epsilon(x_{[n]-i}\circ 0) \geq 1-2\epsilon$. Therefore,

$$\frac{\partial\phi_{\vec{p}}(f_\epsilon)}{\partial p_i} \geq \sum_{x_{[n]-i}\nsim i}\mu_{\vec{p}}(x_{[n]-i})(-2\epsilon) + \sum_{x_{[n]-i}\sim i}\mu_{\vec{p}}(x_{[n]-i})(1-2\epsilon). \tag{12}$$

Note that $\sum_{x_{[n]-i}\sim i}\mu_{\vec{p}}(x_{[n]-i})|_{\vec{p}=(p,...,p)}$ is nothing but $\inf_i(f,p)$, so

$$\frac{\partial\phi_{\vec{p}}(f_\epsilon)}{\partial p_i}|_{\vec{p}=(p,...,p)} \geq (1-\inf_i(f,p))(-2\epsilon) + \inf_i(f,p)(1-2\epsilon) = \inf_i(f,p) - 2\epsilon. \tag{13}$$

Now

$$\frac{d\phi_p(f_\epsilon)}{dp} = \sum_i \frac{\partial\phi_{\vec{p}}(f_\epsilon)}{\partial p_i}|_{\vec{p}=(p,...,p)} \geq \sum_i(\inf(f,p) - 2\epsilon) = \inf(f,p) - 2n\epsilon = \inf(f,p) - 1. \tag{14}$$

□

2.2 Proof by the quantum adversary method

Basically, the quantum adversary method first picks a relation, *i.e.* a set of 0 and 1 input pairs, and assign a weight to each pair. It turns out that the initial total weight decreases by a constant fraction after the computation. So by upper bounding the average progress by one query, we can give a lower bound of the number of queries.

Theorem 2 *We have for any Boolean function f and any $p \in (0,1)$ that*

$$Q_2(f) \geq \Omega(\sqrt{pq}\,\mathrm{inf}(f,p)) \tag{15}$$

Proof Consider the set $\{(x, x^{(i)}) : f(x) \neq f(x^{(i)})\}$. Put weight $w(x, x^{(i)}) = p(x)$. Use $x \sim i$ to denote that $f(x) \neq f(x^i)$. Let $|\psi_x^{(k)}\rangle$ be the state after exactly k queries, and let $\delta_k = \sum_{x,i:x\sim i} p(x)|\langle\psi_x^{(k)}|\psi_{x^{(i)}}^{(k)}\rangle|$. Then

$$\delta_0 = \sum_{x,i:x\sim i} p(x) \cdot |\langle\psi_x^{(0)}|\psi_{x^{(i)}}^{(0)}\rangle| = \sum_i \mathbf{Pr}_x[x \sim i] = \sum_i \mathrm{inf}_i(f,p) = \mathrm{inf}(f,p). \tag{16}$$

and $\delta_T = \sum_{x,i:x\sim i} p(x) \cdot |\langle\psi_x^{(T)}|\psi_{x^{(i)}}^{(T)}\rangle| \leq \epsilon\ \mathrm{inf}(f,p)$. The standard analysis of oracle operation tells us that the average progress $|\delta_k - \delta_{k+1}| = \sum_{x,i:x\sim i} p(x) 2 \left|\langle P_i\psi_x^{(k)}|P_i\psi_{x^{(i)}}^{(k)}\rangle\right|$, where P_i is the projector onto the subspace spanned by index i, *i.e.* $P_i(\sum_{j,z} \alpha_{j,z}|j,z\rangle) = \sum_z \alpha_{i,z}|i,z\rangle$. Therefore,

$$|\delta_k - \delta_{k+1}| \leq 2 \sum_{x,i:x\sim i} p(x) \left\| P_i|\psi_x^{(k)}\rangle \right\| \cdot \left\| P_i|\psi_{x^{(i)}}^{(k)}\rangle \right\| \tag{17}$$

$$\leq 2\sqrt{\left(\sum_{x,i:x\sim i} p(x) \left\| P_i|\psi_x^{(k)}\rangle \right\|^2\right)\left(\sum_{x,i:x\sim i} p(x) \left\| P_i|\psi_{x^{(i)}}^{(k)}\rangle \right\|^2\right)} \tag{18}$$

where both steps are by Cauchy-Schwartz Inequality. Furthermore, let $y = x^{(i)}$ and the above quantity is equal to

$$= 2\sqrt{\left(\sum_x p(x) \sum_{i:x\sim i} \left\| P_i|\psi_x^{(k)}\rangle \right\|^2\right)\left(\sum_{y,i:y\sim i} p(y^{(i)}) \left\| P_i|\psi_y^{(k)}\rangle \right\|^2\right)} \tag{19}$$

$$\leq 2\sqrt{\sum_{y,i:y\sim i} p(y^{(i)}) \left\| P_i|\psi_y^{(k)}\rangle \right\|^2} \tag{20}$$

$$= 2\sqrt{\sum_{y,i:y\sim i, y_i=1} p(y)\frac{q}{p} \left\| P_i|\psi_y^{(k)}\rangle \right\|^2 + \sum_{y,i:y\sim i, y_i=0} p(y)\frac{p}{q} \left\| P_i|\psi_y^{(k)}\rangle \right\|^2} \tag{21}$$

$$\leq 2\sqrt{\frac{q}{p} + \frac{p}{q}} \tag{22}$$

$$\leq \frac{2}{\sqrt{pq}} \tag{23}$$

So $T \geq \Omega(\sqrt{pq}\ \mathrm{inf}(f,p))$. □

Acknowledgement

S.Z. thanks Nicholas Pippenger, Alexander Razborov and Andrew Yao for carefully reading the manuscript (as part of his Ph.D. thesis) and giving many detailed suggestions to improving the presentation of the paper.

References

[1] A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64:750–767, 2002.

[2] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: A survey. *Theoretical Computer Science*, 288:21–43, 2002.

[3] A. Chakrabarti and S. Khot. Improved lower bounds on the randomized complexity of graph properties. In *Proceedings of the 28th International Colloquium on Automata, Languages and Programming (ICALP)*, pages 285–296, 2001.

[4] Péter Hajnal. An $\omega(n^{4/3})$ lower bound on the randomized complexity of graph properties. *Combinatorica*, 11(2):131–143, 1991.

[5] V. King. Lower bounds on the complexity of graph properties. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC)*, pages 468–476, 1988.

[6] D. Kirkpatrick. Determining graph properties from matrix representations. In *Proceedings of the Sixth Annual ACM Symposium on Theory of Computing (STOC)*, pages 84–90, 1974.

[7] R. O'Donnell, M. Saks, O. Schramm, and R. Servedio. Every decision tree has an influential variable. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 31–39, 2005.

[8] R. O'Donnell and R. Servedio. Learning monotone functions from random examples in polynomial time. *manuscript*.

[9] R. Cleve M. Mosca R. de Wolf R. Beals, H. Buhrman. Quantum lower bounds by polynomials. *Journal of the ACM*, 48:778–797, 2001.

[10] R. Rivest and J. Vuillemin. On recognizing graph properties from adjacency matrices. *Theoretical Computer Science*, 3(3):371–384, 1976.

[11] A. Rosenberg. On the time required to recognize properties of graphs: a problem. *SIGACT News*, 5(4):15–16, 1973.

[12] Y. Shi. Lower bounds of quantum black-box complexity and degree of approximating polynomials by influence of Boolean variables. *Information Processing Letters*, 75(1-2):79–83, 2000.

[13] A. Yao. Lower bounds to randomized algorithms for graph properties. *Journal of Computer and System Sciences*, 42(3):267–287, 1991.