Week 8 : Quantum Query Lower Bounds

Contents

1 Introduction

Over the previous chapters we have seen many algorithms and their corresponding query or time complexity. We saw that nearly all of the algorithms performed better by using resources (time or queries) lesser than the best known classical algorithms in solving problems of interest. For any given problem, the upper bound complexity of an algorithm solving the problem can be used to derive the the upper bound on the difficulty of the problem. But can we obtain some lower bound on the difficulty of the problem? Over the years, obtaining non-trivia lower bounds for computational problems has been challenging. Most of the work on non-trivial lower bounds of problems have been done on problems that are solved using the 'black box' model. This condition is true for both classical and quantum computation.

In this chapter we will primarily look into the techniques used in the black box model to obtain the lower bounds of problems. We will also derive the lower bound of Grover's search using those techniques. But first we introduce the 'black box' model.

Black box model is a computational model in which the input to the problem is given as a black box O_X that contains information about an unknown string X. We would be able to obtain information about X by querying the oracle O_X but not otherwise. The main goal usually is to compute some function F of X. In order to compute $F(X)$, we can use unitary operations and oracle queries in this model. Our ultimate aim is to use the least number of queries to obtain the enough amount of information about X using O_X so as to compute $F(X)$ with some surety.

The query complexity of a problem is defined as the number of queries made to an oracle O_X to compute the function $F(X)$ and the query complexity of an algorithm is defined as the number of queries made by the algorithm. It is important to note the difference between the two. The exact quantum query complexity of a problem, denoted by $Q_E(F)$, is defined as the minimum number of queries to O_X required by a quantum algorithm to compute the correct $F(X)$ with probability 1. The 2 sided error quantum query complexity of a problem, denoted by $Q_2(F)$, is defined as the minimum number of queries to O_X required by a quantum algorithm to compute the correct $F(X)$ with probability $\geq \frac{2}{3}$. For most of the problems, the query complexity in both the exact and errored setting will be similar. In the next section we will see the first technique that can be used to obtain lower bounds of the quantum query complexity of various problems.

2 Quantum Hybrid Method

Suppose that we have a quantum algorithm $\mathcal{A}$. Suppose we are also given an oracle O_X that contains information about an unknown string $X \in \{0,1\}^N$. For a state $|\phi\rangle = \sum_x \alpha_x |x\rangle$, the query magnitude at bit position j of $|\phi\rangle$ is defined as $q_j(|\phi\rangle) = \sum_{y \in Y_j} |\alpha_y|^2$ where Y_j is the set of all computational basis states y that query the bit position j of X. Let $\mathcal{A}$ make m queries to the oracle O_X in total and let the state of the system just before $i+1^{st}$ query is given by $|\phi_i\rangle$. Then the query magnitude at bit position j of A given the oracle O_X is defined as $q_j(X) = \sum_{k=0}^{m-1} q_j(|\phi_k\rangle)$.

Now let us define a set of hybrid runs. Let X and Y be two strings whose oracles O_X and O_Y are provided. Also let $\Delta(X,Y) = \{j : X_j \neq Y_j\}$. Let the k^{th} run of $\mathcal{A}$ is such that $\mathcal{A}$

uses O_X for the first k queries and O_Y for the rest $m-k$ queries. Let $|\phi_{k,p}\rangle$ denote the state of the system of k^{th} hybrid run of $\mathcal{A}$ just before $p+1^{st}$ query. It is clear that $|\phi_{k,0}\rangle = |\phi_0\rangle$ for all hybrid runs k, $|\phi_{m,m}\rangle = |\phi_X\rangle$ which is the output state if the algorithm $\mathcal{A}$ makes all m queries to O_X and $|\phi_{0,m}\rangle = |\phi_Y\rangle$ which is the output state if the algorithm $\mathcal{A}$ makes all m queries to O_Y.

Let us now compare the k^{th} and the $k+1^{th}$ hybrid runs of $\mathcal{A}$. It is clear that the first k queries are performed on O_X, and the last $m-k-1$ queries are performed on O_Y for both the hybrid runs of $\mathcal{A}$. The only difference is that the $k+1^{th}$ query of k^{th} hybrid run is queried to O_X and that of $k+1^{th}$ hybrid run is queried to O_Y. Now since the only difference is in the $k+1^{st}$ query, it follows that

$$||\,|\phi_{k,k+1}\rangle - |\phi_{k+1,k+1}\rangle\,||^2 \leq \textstyle\sum_{j\in\Delta(X,Y)} q_j(|\phi_k\rangle).$$

Now, since unitary evolution preserves dot product and since the last $m-k-1$ queries are done to the oracle O_Y, we have

$$||\,|\phi_{k,k+1}\rangle - |\phi_{k+1,k+1}\rangle\,|| = ||\,|\phi_{k,m}\rangle - |\phi_{k+1,m}\rangle\,||$$

Now, the 1-norm distance between $|\phi_X\rangle$ and $|\phi_y\rangle$ is given by

$$\begin{aligned}
||\,|\phi_x\rangle - |\phi_y\rangle\,|| &= ||\,|\phi_{m,m}\rangle - |\phi_{0,m}\rangle\,|| \\
&\leq \sum_k ||\,|\phi_{k,m}\rangle - |\phi_{k+1,m}\rangle\,|| \\
&\leq \sum_k \sqrt{\sum_{j\in\Delta(X,Y)} q_j(|\phi_k\rangle)} \\
&\leq \sqrt{m}\sqrt{\sum_k \sum_{j\in\Delta(X,Y)} q_j(|\phi_k\rangle)} \\
&= \sqrt{m}\sqrt{\sum_{j\in\Delta(X,Y)} \sum_k q_j(|\phi_k\rangle)} \\
&= \sqrt{m}\sqrt{\sum_{j\in\Delta(X,Y)} q_j(X)}
\end{aligned}$$

Using a lemma from Vazirani, we have that if $||\,|\phi'\rangle - |\phi\rangle\,|| \leq \epsilon$ then $||\mathcal{D}(|\phi'\rangle) - \mathcal{D}(|\phi\rangle)|| \leq 4\epsilon$ where $|\phi'\rangle$ is the final error vector, $|\phi\rangle$ is the actual final vector and $\mathcal{D}(\phi)$ is the distribution obtained on measuring ϕ in computational basis. A necessary condition for a probabilistic algorithm is that it outputs the correct solution with error probability bounded by $\frac{1}{3}$. In terms of total variational distance, the condition translates to $||\mathcal{D}(|\psi_X\rangle) - \mathcal{D}(|\psi_Y\rangle)|| \leq \frac{1}{3}$. Using this inequality and the inequality $||\,|\phi_x\rangle - |\phi_y\rangle\,|| \leq \sqrt{m}\sqrt{\sum_{j\in\Delta(X,Y)} q_j(X)}$, we can obtain a lower bound on the number of queries m made by the algorithm $\mathcal{A}$ so that $\mathcal{A}$ outputs the correct solution with error probability bounded by $\frac{1}{3}$.

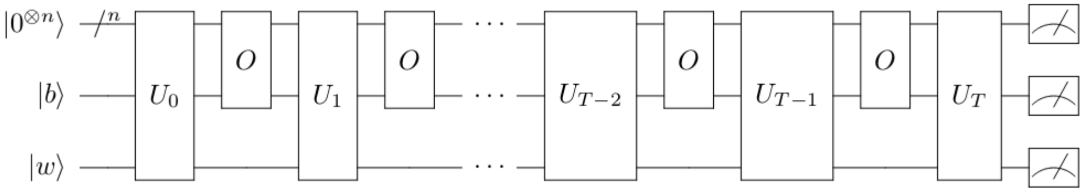

Figure 1: Generalized circuit of any quantum algorithm that make T queries

3 Polynomial Method

In this section we will see how the amplitudes of the final state of a T-query algorithm are closely related polynomials of degree T. But before diving into their relation, we first discuss a few preliminaries required to establish the relations. An N-variate multilinear polynomial p is a given as

$$p(x_0, x_1, .., x_{N-1}) = \sum_{S \subseteq \{0,1,...,N-1\}} a_S \prod_{i \in S} x_i$$

where $a_S \in \mathbb{C}$. The degree of p is the degree of the largest monomial $\prod_{i \in S} x_i$ such that $a_S \neq 0$. More formally $deg(p) = max\{|S| : a_S \neq 0\}$.

For an arbitrary function $F : \{0,1\}^N \longrightarrow \{0,1\}$ we say that a polynomial p represents the function F if $p(X) = F(X)$ for all $X \in \{0,1\}^N$. The degree of the function F, denoted by $deg(f)$, is defined as the degree of the polynomial p representing the function F. We say that a polynomial p approximates a function $F : \{0,1\}^N \longrightarrow \{0,1\}$ if $|p(X) - F(X)| \leq \frac{1}{3}$ for all $X \in \{0,1\}^N$ and the minimum degree over all the polynomials approximating F is denoted by $deg(F)$. It can be observed that the degree of a polynomial that *approximates* a function F is less than or equal to the degree of a polynomial that represents the same function F.

Let $N = 2^n$ for some $n \in \mathbb{N}$. Let O be an oracle containing information about an N-bit string $X = X_1 X_2 ... X_N$. Then the circuit of the black box model can represented as in Figure 1 where U_is are some unitary transformations. Let $|\psi_i\rangle$ be the state of the system after i^{th} unitary U_i. Let the input state to the circuit be $|0^{\otimes n}\rangle |0\rangle |0^m\rangle$ where the first register, say $|q\rangle$, is the query register, the second register of single qubit, say $|r\rangle$, is the output register and the third register, say $|w\rangle$, is the work register. Then the state of the register after the unitary U_0 can be written as

$$|\psi_0\rangle = \sum_{i \in \{0,1\}^n} \alpha_{i,0,0} |i\rangle |0\rangle |w\rangle + \alpha_{i,1,0} |i\rangle |1\rangle |w\rangle$$

where $\alpha_{i,0,0}$s and $\alpha_{i,0,0}$s are independent of X since there has been no oracle query made yet. So, we can notice that the degree of a polynomial representing the amplitudes $\alpha_{i,0,0}$ or $\alpha_{i,1,0}$ is 0. Proceeding ahead, the state of the system after the unitary U_1 can be given as $|\psi_1\rangle = U_1 O |\psi_0\rangle$. Now let us consider for just a single state of the computation basis. Then the effect of oracle on $\alpha_{i,0,0} |i\rangle |0\rangle |w\rangle + \alpha_{i,1,0} |i\rangle |1\rangle |w\rangle$ can be given as

$$\alpha_{i,0} |i\rangle |0\rangle |w\rangle + \alpha_{i,1,0} |i\rangle |1\rangle |w\rangle \longrightarrow$$
$$\big[(1 - x_i)\alpha_{i,0,0} + x_i \alpha_{i,1,0}\big] |i\rangle |0\rangle |w\rangle + \big[x_i \alpha_{i,0,0} + (1 - x_i)\alpha_{i,1,0}\big] |i\rangle |1\rangle |w\rangle$$

That is if $x_i = 0$, then output bit does not change but if $x_i = 1$ then the output bit changes. We can observe that the amplitudes are polynomials of X of degree atmost 1. The state ψ_1 can be given as

$$\begin{aligned}\psi_1 &= U_1\Big(\sum_{i\in\{0,1\}^n} \big[(1-x_i)\alpha_{i,0,0} + x_i\alpha_{i,1,0}\big] |i\rangle |0\rangle |w\rangle + \big[x_i\alpha_{i,0,0} + (1-x_i)\alpha_{i,1,0}\big] |i\rangle |1\rangle |w\rangle \Big) \\ &= U_1\Big(\sum_{i\in\{0,1\}^n} \big[\tilde{\alpha}_{i,0,1}(X) |i\rangle |0\rangle |w\rangle + \tilde{\alpha}_{i,1,1}(X) |i\rangle |1\rangle |w\rangle \,\big]\Big) \\ &= \sum_{i\in\{0,1\}^n} \big[\alpha_{i,0,1}(X) |i\rangle |0\rangle |w\rangle + \alpha_{i,1,1}(X) |i\rangle |1\rangle |w\rangle \,\big]\end{aligned}$$

We can observe that the new amplitudes $\alpha_{i,r,1}$ are a function of X. On similar application of the oracle, we would obtain the amplitudes $\alpha_{i,r,2}$ which are polynomials of X of degree is atmost 1 greater than the old amplitudes. Hence the new amplitudes $\alpha_{i,r,1}$ are of degree atmost 2. Then by using induction we can show that after T queries, the amplitudes are polynomials of X of degree atmost T. The proof by induction is requested as an exercise.

Imagine we have an algorithm that outputs the state $|\psi_T\rangle = \sum_{i\in\{0,1\}^n} \big[\alpha_{i,0,T}(X) |i\rangle |0\rangle |w\rangle + \alpha_{i,1,T}(X) |i\rangle |1\rangle |w\rangle \,\big]$ then the probability of obtaining $|r\rangle = |1\rangle$ on measurement is given by

$$p(X) = \sum_{i\in\{0,1\}^n} \big|\alpha_{i,1,T}(X)\big|^2$$

Since $deg(\alpha_{i,1,T}(X)) \leq T$ for all i, the degree of $\big|\alpha_{i,1,T}(X)\big|^2$ cannot exceed $2T$ and so the polynomial $p(X)$ is of degree atmost $2T$.

We previously discussed how a polynomial p approximates a function $F : \{0,1\}^N \longrightarrow \{0,1\}$. If we have a circuit used T queries to compute some function F of a string X where information about X is obtainable only through an oracle, then $p(X) = 1$ if and only if $F(X) = 1$. Let $Q_E(F)$ be exact quantum query complexity of computing $F(X)$. Now, we know $deg(F) = deg(p)$ and $deg(p) \leq 2T$. This implies $deg(F) \leq 2Q_E(F)$ or $Q_E(F) \geq deg(F)/2$. This provides a lower bound on the number of queries required to compute the function F of X. A similar bound can be proved for 2 sided error quantum query complexity.

4 Quantum Adversary Method

Quantum adversary method is yet another technique to obtain lower bounds of various computational decision problems. It is broadly based in the concept of block sensitivity of a Boolean function. Let us now formally define block sensitivity of a function f.

Let $f : \{0,1\}^n \longrightarrow \{0,1\}$ be a Boolean function and let $x \in \{0,1\}^n$. Let $B \subseteq \{0,...,n-1\}$ be a set of indices and let x^B be the string obtained by taking x and flipping the bits in bit positions $i \in B$. Then the function f is said to be sensitive to B on x if $f(x) \neq f(x^B)$. The block sensitivity $bs_x(f)$ of f on x is the maximum t such that $\exists$ t disjoint subsets $B_1, ..., B_t$ of B with the condition that f is sensitive to each B_i on x. The block sensitivity $b_x(F)$ of f is the maximum $b_x(f)$ over all $x \in \{0,1\}^n$.

Lower bounds for certain decision problems can be obtain by just using the block sensitivity of the decision functions. But they just form a special case of the quantum adversary method. Now, we present a simple version of the quantum adversary method.

Theorem 1 *Let $F : \{0,1\}^N \longrightarrow \{0,1\}$ be a function describing a decision problem. Let X be a subset of the set $F^{-1}(0)$ and Y be the subset of the set $F^{-1}(1)$. Let R be a binary relation such that $R \subseteq X \times Y$. If*

1. *for all $x \in X$, $\exists$ atleast m distinct $y \in Y$ such that $(x, y) \in R$,*
2. *for all $y \in Y$, $\exists$ atleast m' distinct $x \in X$ such that $(x, y) \in R$,*
3. *for all $x \in X$ and $i \in \{0, ..., N\}$, $\exists$ atmost l distinct $y \in Y$ such that $(x, y) \in R$ and $x_i \neq y_i$,*
4. *for all $y \in Y$ and $i \in \{0, ..., N\}$, $\exists$ atmost l' distinct $x \in X$ such that $(x, y) \in R$ and $x_i \neq y_i$,*

then the quantum query complexity of F is $\Omega\left(\sqrt{\frac{m \cdot m'}{l \cdot l'}}\right)$.

The proof for the same can be obtained from [Ambainis] [1]. We can observe that the effectiveness of the method depends on choosing the subsets X, Y and forming a relation R wisely so as to maximize $\frac{m \cdot m'}{l \cdot l'}$.

5 Exercises

1. Let $f : \{0,1\}^3 \longrightarrow \{0,1\}$ be a Boolean function such that $f(x) = 1$ if $x \in \{011, 101, 110, 111\}$ and $f(x) = 0$ otherwise. Find a polynomial that represents this function f.
2. Consider the 2-bit function $f(x) = x_1 \cdot x_2$. Find the block sensitivity of f.
3. Suppose we are given an oracle to a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ and a promise that either there is exactly one solution or no solution, i.e, $f(x) = 1$ for no x or just one x. Using quantum adversary method, obtain a non-trivial lower bound for the problem of deciding if there is one solution or no solution.
4. Given an oracle to a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ such that there is either no x such that $f(x) = 0$ or exactly k solutions for some $k < 2^{n-1}$, prove that any quantum algorithm needs atleast $\Omega(\sqrt{2^n/k})$ queries.

[1] Ambainis, Andris. "Quantum lower bounds by quantum arguments." Journal of Computer and System Sciences 64.4 (2002): 750-767.