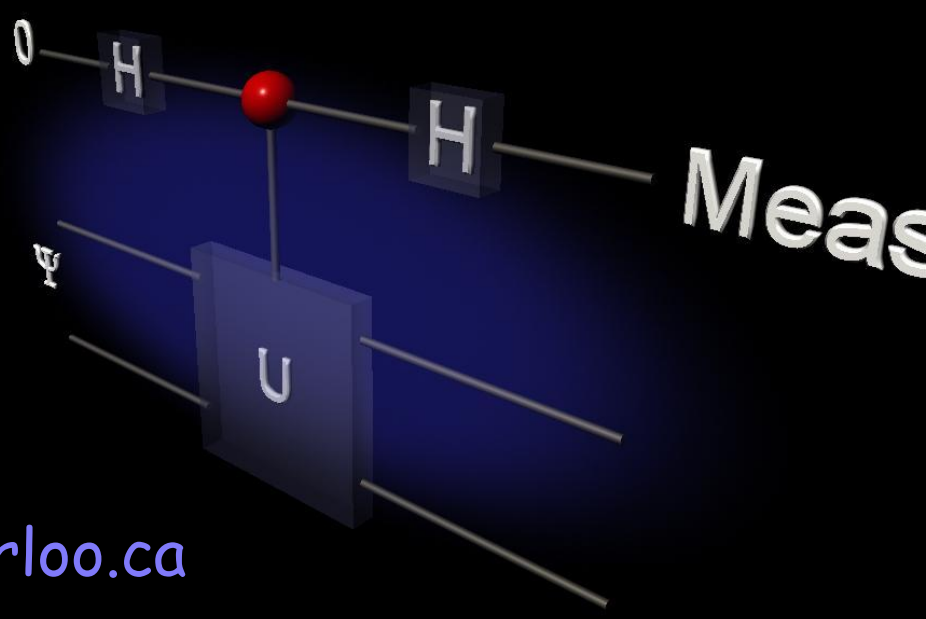
Introduction to Quantum Information Processing



CO481 CS467 PHYS467

Michele Mosca mmosca@iqc.uwaterloo.ca

Tuesdays and Thursdays 10am-11:15am

IQC Institute for Quantum Computing

UNIVERSITY OF WATERLOO

PI PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

Black-box Lower Bounds

Lower bounds

- We want to classify problems according to their computational complexity
- We need then upper bounds and lower bounds for computational complexity
- Algorithms give us upper bounds
- We also want lower bounds

Lower bounds

- What are the limitations of any realistic algorithmic process for solving a specific problem?
- For example, how many elementary steps are necessary to factor n-bit integers?
- Lower bounds depends on the exact model of computation (e.g. what is an elementary step?)
- Lower bounds for time complexity are very hard to obtain. We consider a different measure for our lower bounds; one that sheds some light on actual lower bounds.

- Suppose we have a function f from $\{0,1\}^n$ to $\{0,1\}$
  - We wish to decide if there exists an input string j such that f(j)=1.
  - Suppose we wish to decide if there are more solutions to f(x)=1 or f(x)=0.
- Suppose we have a function f from $\{0,1\}^n$ to $\{0,1\}^m$
- Suppose we promise that f(j) = f(j+r) for some hidden period r. We wish to find r.
- How well can a quantum algorithm solve these problems without looking into the internal structure of f?

- If we do not probe the internal structure of f, we can reformulate these problems as follows.

Let $X_j = f(j)$.

$X=X_0, X_1, \ldots, X_{N-1}$, $N=2^n$

- Determine OR(X)
- Determine MAJORITY(X)
- Determine the period of the sequence $X_0, X_1, \ldots, X_{N-1}$

Black-box quantum setting

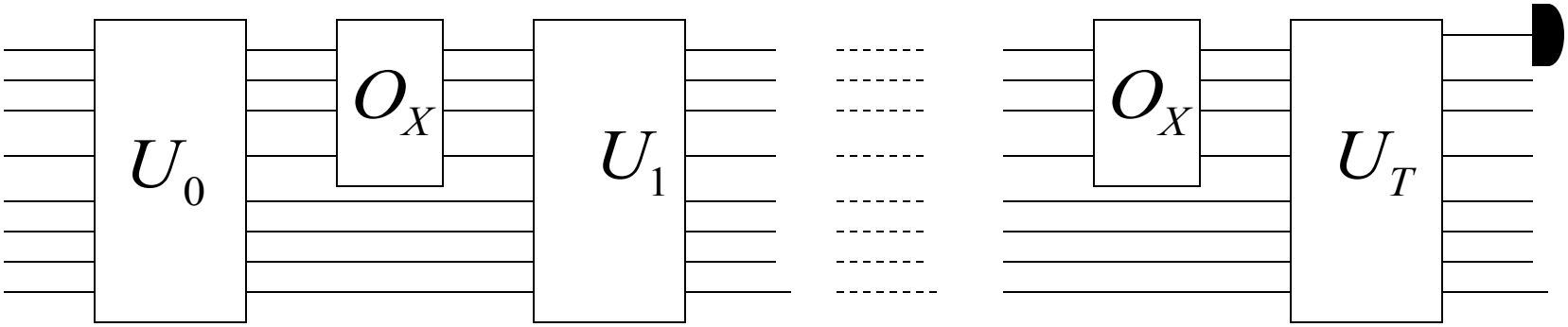
- We have a function F from $\{0,1\}^N$ to $\{0,1\}$
- We have access to the input $X=\{X_1, \ldots, X_N\}$ in a black-box way
- More exactly, access to an oracle Ox that implements

$$|j\rangle|b\rangle \xrightarrow{O_X} |j\rangle|b \oplus X_j\rangle$$

- We can perform unitaries during the computation

Black-box quantum setting

- An algorithm that performs T calls to the oracle O will work in the following way, wlog:



- The methods we will study give us a lower bound on the number of calls to the black box necessary to compute F

- This is a lower bound for the time complexity of the problem, but not necessarily tight (i.e. the unitaries for an optimal sequence of queries might be hard to implement).

Black-box quantum setting

We are interested in the following two quantities:

- $Q_E(F)$, the number of queries required by any quantum procedure to compute F with probability 1

- $Q_2(F)$, the number of queries required by any quantum procedure to compute F with probability 2/3

Main idea

Let X be an input with F(X)=1, and Y an input with F(Y)=0.

A procedure that computes F successfully must obtain final states $|\psi_X\rangle$ and $|\psi_Y\rangle$ that can be distinguished from each other.

State distinguishability

- This motivates the following problem:

Distinguishing Two Pure Quantum States With Minimum Error

Input: One of two known states $|\psi_X\rangle$ and $|\psi_Y\rangle$,with the property that $|\langle\psi_X|\psi_y\rangle| = \delta$

Output: A guess ‘X’ or ‘Y’

Problem: Maximize the probability that the guess is correct

State distinguishability

- The optimal procedure outputs a correct guess with probability

$$\frac{1}{2}+\frac{1}{2}\sqrt{1-\delta^2}$$

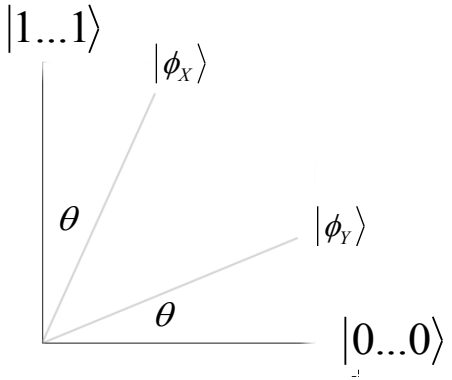
- Such an optimal procedure is the following
  - $|\psi_X\rangle$ goes to $\sin(\theta)|0...0\rangle+\cos(\theta)|1...1\rangle=|\phi_X\rangle$

    $|\psi_Y\rangle$ goes to $\cos(\theta)|0...0\rangle+\sin(\theta)|1...1\rangle=|\phi_X\rangle$

  - Unitarity implies $|\sin(2\theta)|=\delta$
  - $\sin(2\theta)$ takes every value between 0 and 1 one for θ between 0 and $\pi/4$
  - Therefore, we can make θ be in that range

State distinguishability

After the mapping we have:



- We measure the first qubit in the computational basis
- Output ‘X’ if we obtain $|1\rangle$
- Output ‘Y’ if we obtain $|0\rangle$
- Probability of success: $\cos^2(\theta) = \frac{1+\cos(2\theta)}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{1-\delta^2}$

State distinguishability

- Proof of optimality (sketch)
  - We can prove that wlog, a general measurement applies an unitary on state+ancilla and then measures the first qubit in the computational basis, with 0='X', 1='Y'
  - Wlog, the unitary sends

$$|\psi_X\rangle|0\ldots0\rangle \text{ to } \sqrt{1-\varepsilon_X}\,|0\rangle|\,junk(x,0)\rangle + \sqrt{\varepsilon_X}\,|1\rangle|\,junk(x,1)\rangle$$

$$|\psi_Y\rangle|0\ldots0\rangle \text{ to } \sqrt{\varepsilon_Y}\,|0\rangle|\,junk(y,0)\rangle + \sqrt{1-\varepsilon_Y}\,|1\rangle|\,junk(y,1)\rangle$$

  - Unitarity gives us a constraint for ε_X and ε_Y
  - Standard optimization/calculus gives us then that the best probability of a correct guess is $\frac{1}{2}+\frac{1}{2}\sqrt{1-\delta^2}$

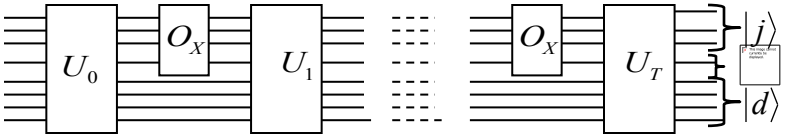
Hybrid method

- Originally used by Bennett, Bernstein, Brassard and Vazirani to prove optimality of Grover's search
- Indeed, easily proves that the restriction to the case where the number of marked items is at most one is also hard
- Considers the final state produced by an algorithm when the input is all zero. Bounds how different can the final state be for inputs with a one, as a function of the number of queries
- Finally, it uses the result for state distinguishability to relate the probability of success to the number of queries

Polynomial method

- Theorem(BBCMW) : A quantum algorithm making T queries to the black box O_X will produce a quantum state of the form

$$\sum_{\substack{j\in\{0,1\}^n \\ b\in\{0,1\} \\ d\in\{0,1\}^m}} \alpha_{j,b,d}(X)\left|j,b,d\right\rangle$$



Where the $\alpha_{j,b,d}(X)$ are multilinear polynomials of degree at most T in $X_0, X_1, \ldots, X_{n-1}$.

Polynomial method

Proof (by induction)

- For T=0, the amplitudes do not depend on the input, so it is true
- Suppose true for T=k-1. The state after T queries is then

$$\sum_{\substack{j\in\{0,1\}^n \\ b\in\{0,1\} \\ d\in\{0,1\}^m}} \alpha_{j,b,d}(X)\left|j,b,d\right\rangle$$

where the $\alpha_{j,b,d}(X)$ are multilinear polynomials of degree at most k-1 in $X_0,X_1,\ldots,X_{2^n-1}$.

Polynomial method

O_X maps

$$|j,b,d\rangle \xrightarrow{O_X} (1-X_j)|j,b,d\rangle + X_j|j,b\oplus 1,d\rangle$$

so

$$\sum_{\substack{j\in\{0,1\}^n \\ b\in\{0,1\} \\ d\in\{0,1\}^m}} \alpha_{j,b,d}(X)|j,b,d\rangle \xrightarrow{O_X} \sum_{\substack{j\in\{0,1\}^n \\ b\in\{0,1\} \\ d\in\{0,1\}^m}} \beta_{j,b,d}(X)|j,b,d\rangle$$

where the $\beta_{j,b,d}$ are polynomials of degree at most k in $X_0,X_1,\ldots,X_{2^n-1}$. As $x^2 = x$ for x in {0,1}, we can assume they are multilinear

Application to lower bounds

- Corollary: The probability of outputting 1 is a real multi-linear polynomial in the input variables of degree at most 2T.

- Intuitively, then a small number of queries can be used to compute only functions with a lot of structure

- More formally:

  - An N-variate polynomial p: $R^n \rightarrow R$ represents F if p(X)=F(X) for all X in $\{0,1\}^n$

  - An N-variate polynomial p: $R^n \rightarrow R$ approximates F if $|p(X)-F(X)| \leq 1/3$ for all X in $\{0,1\}^n$

Application to lower bounds

- Let the minimum degree of a real multi-linear polynomial polynomial p that represents F be deg(F)
- Let the minimum degree of a a real multi-linear polynomial p that approximates F be $\widetilde{deg}(F)$
- Using the corollary, we have:
  - $Q_E(F) \geq deg(F)/2$
  - $Q_2(F) \geq \widetilde{deg}(F)/2$

Application to lower bounds

- We have reduced obtaining lower bounds to studying representing/approximating a function with polynomials

- Polynomials and their use in approximating arbitrary functions have been studied for a very long time

- This gives us access to powerful mathematical tools that we can use to obtain quantum lower bounds

Easy example

- We can prove there exists exactly one multilinear polynomial of degree at most N representing a function on N inputs
- $1 - \prod_{j=1}^{N}(1 - X_j)$ represents the OR function on N inputs
- It has degree N
- We obtain then $Q_E(\mathrm{OR}) \geq N/2$

Some results

Some other results that can be obtained using the polynomial method are the following ones:

- $Q_2(\text{OR}) \in \Omega\left(\sqrt{N}\right)$
  This implies optimality for the number of queries to the oracle in Grover's algorithm
- $Q_2(\text{MAJORITY}) \in \Omega(N)$
- $Q_2(\text{PARITY}) \geq N/2$

Adversary method

The polynomial method and hybrid method have been very successfully been applied to find tight lower bounds on many important and interesting problems.

There exist problems where the polynomial method is known not to lead to the optimal lower bound.

Another approach to lower bounds (by Ambainis) is known as the “adversary method”.

Adversary method

Consider a t-query algorithm A trying to compute F(Z) and let $\left|\psi_j^Z\right\rangle$ denote the state of the quantum computer after j queries to the oracle for the string Z.

$$\mathcal{Y} = \left\{\left|\psi_t^Y\right\rangle : F(Y) = 1\right\}$$

$$\mathcal{X} = \left\{\left|\psi_t^X\right\rangle : F(X) = 0\right\}$$

Suppose that, for any input string Z, we want probability 1-Ɛ of guessing the correct value of F(Z).

Thus (theorem 9.2.1), we know that we must have, for any X,Y, with F(X)≠F(Y):

$$\left|\left\langle\psi_t^Y \middle| \psi_t^X\right\rangle\right| \leq 2\sqrt{\varepsilon(1-\varepsilon)}$$

Adversary method

$$\mathcal{Y} = \left\{ \left| \psi_t^Y \right\rangle : F(Y) = 1 \right\} \qquad \mathcal{X} = \left\{ \left| \psi_t^X \right\rangle : F(X) = 0 \right\}$$

$$\left| \left\langle \psi_t^Y \middle| \psi_t^X \right\rangle \right| \leq 2\sqrt{\varepsilon(1-\varepsilon)}$$

Let $R \subseteq \mathcal{X} \times \mathcal{Y}$

Then $$\sum_{(X,Y)\in R} \left| \left\langle \psi_t^Y \middle| \psi_t^X \right\rangle \right| = 2\sqrt{\varepsilon(1-\varepsilon)}|R|$$

Note that $$\sum_{(X,Y)\in R} \left| \left\langle \psi_0^Y \middle| \psi_0^X \right\rangle \right| = |R|$$

Adversary method

Let $$W^j = \sum_{(X,Y)\in R} \frac{1}{\sqrt{|X||Y|}} \left| \left\langle \psi_j^Y \middle| \psi_j^X \right\rangle \right|$$

Then $$W^t - W^0 \geq \frac{1-2\sqrt{\varepsilon(1-\varepsilon)}}{\sqrt{|X||Y|}} \in \Omega\left(\frac{|R|}{\sqrt{|X||Y|}} \right)$$

Adversary method

If we could show that for some value Δ>0, that

$$W^{k+1} - W^k \leq \Delta$$

…then

$$t \geq \frac{W^t - W^0}{\Delta}$$

Adversary method

Lemma 9.7.1

Let b and b' satisfy the following:

- For every X in $\mathcal{X}$ and i in {1,2,…, N}, there are at most b different Y in $\mathcal{Y}$ such that (X,Y) in R and $X_i \neq Y_i$
- For every Y in $\mathcal{Y}$ and i in {1,2,…, N}, there are at most b' different X in $\mathcal{X}$ such that (X,Y) in R and $X_i \neq Y_i$

Then:

$$W^k - W^{k-1} \leq \sqrt{bb'}$$

Adversary method

Consequently:

$$t \in \Omega\left(\frac{|R|}{\sqrt{|X||Y|}\sqrt{bb'}}\right)$$

Adversary method

Lemma 9.7.3

Let m and m' be any integers satisfying:

- For every X in $\mathcal{X}$ there are at least m different Y in $\mathcal{Y}$ such that (X,Y) in R
- For every Y in $\mathcal{Y}$ there are at least m' different X in $\mathcal{X}$ such that (X,Y) in R

Then

$$|R| \geq \sqrt{|\mathcal{X}||\mathcal{Y}|mm'}$$

Adversary method

$$t \in \Omega\left(\sqrt{\frac{mm'}{bb'}}\right)$$

Theorem 9.7.4

$$Q_2(F) \in \Omega\left(\sqrt{\frac{mm'}{bb'}}\right)$$

An example:

AND-OR trees

Partial functions

- So far, we assumed that F was defined for all inputs $\{0,1\}^n$. This is called a *total* function.
- It could be defined only for a subset of $\{0,1\}^n$. That is called a *partial* function.
- We can adapt the lower bound methods to this setting
  - For example, we can consider the polynomial that approximates a function over a certain domain

Relation with classical case

- Let D(F) be the number of queries required by any deterministic classical procedure evaluating F

- For total functions F, it is known that $D(F) = O(Q_2(F)^6)$