LECTURE 7 (February 7)

TODAY Quantum Lower Bounds via Polynomials

RECAP

- $\text{coSimon}^{O} = \{1^n \mid f_n \text{ is a 1-to-1 function}\}$ where O applies $f_n(x)$ for inputs of length n

  $\text{coSimon}^{O} \in \text{BQP}^{O}$

  By enumerating all NP-oracle machines $M_1, M_2, \ldots$ we can choose an f_{n_i} s.t. M_i fails on input 1^{n_i} $\Rightarrow \text{coSimon}^{O} \notin \text{NP}^{O}$

- Unstructured search problem: Given black-box access to $f : \{0,1\}^n \to \{0,1\}$ find if $f \equiv 0$ or $\exists\, x$ s.t. $f(x) = 1$

  Grover's algorithm $\Rightarrow$ Can decide this with $O(2^{n/2})$ quantum queries

  $\Rightarrow$ Is there a poly(n)-query quantum algorithm ?
  NO! Any quantum algorithm must make $\Omega(2^{n/2})$ queries

  $\Rightarrow \text{NP}^{O} \not\subseteq \text{BQP}^{O}$

We will introduce a general technique that can be used to prove lower bounds for quantum query algorithms for many kinds of problems

The polynomial method

Quantum query algorithm had access to a unitary $U_f : |y\rangle \to (-1)^{f(y)} |y\rangle$ for $y \in \{0,1\}^n$

To use the polynomial method, we will assume that the quantum algorithm has access to

$$O_x : |i\rangle \longrightarrow x_i |i\rangle \qquad \text{where } i \in [N]$$
$$x_i \in \{\pm 1\} \text{ and } N = 2^n$$

This is exactly the same as U_f where we view the string $x = x_1 \cdots x_N \in \{\pm 1\}^N$ the truth table of f (with ± 1 values instead of 0/1)

Let us consider the unstructured problem in this new notation

Previously $f \equiv 0$ or $\exists\, x$ s.t. $f(x) = 1$

Now $\underbrace{x = 1^N}_{\text{OR}(x_1,\ldots,x_N) = 0}$ or $\underbrace{\exists \text{ a bit } i \text{ s.t. } x_i = -1}_{\text{OR}(x_1,\ldots,x_N) = 1}$ if we view $1 = \text{False}$, $-1 = \text{True}$

Thus, our goal is to show that no quantum algorithm can compute the logical OR of N bits with less than $\sqrt{N}$ queries with error $\leq \frac{1}{3}$

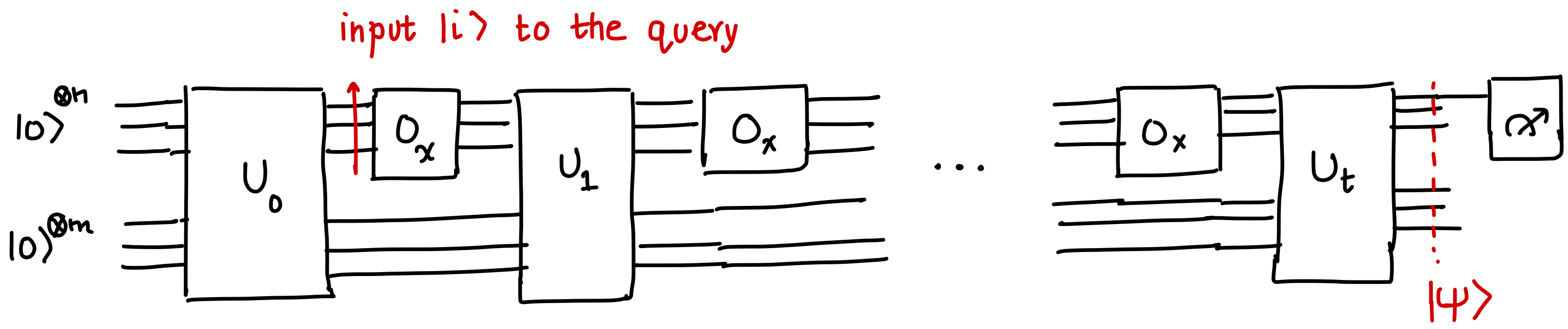
Quantum algorithm can query the bits of $x \in \{\pm 1\}^N$ in a superposition via

$$O_x : |i\rangle \longrightarrow x_i |i\rangle$$

The polynomial method is based on the following observation

Lemma The acceptance probability of any quantum algorithm that makes t queries can be expressed as a polynomial of degree $\leq 2t$ in the variables $x_1, \ldots, x_N$

Proof Consider an arbitrary quantum algorithm



The final state just before measurement is

$$|\psi\rangle = U_t (O_x \otimes I) U_{t-1} \cdots (O_x \otimes I) U_1 (O_x \otimes I) U_0 |0\rangle^{\otimes n+m}$$

Note that $O_x |i\rangle = x_i |i\rangle$ means that O_x is the diagonal $N \times N$ matrix with $x_1 \ldots x_N$ on the diagonal

$$O_x = \begin{array}{cc} \begin{bmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_N \end{bmatrix} & N \\ N & \end{array}$$

The amplitude of any basis state in $|\psi\rangle$ is a degree t polynomial in $x_1 \ldots x_N$ since it can pick one variable from each $O_x \otimes I$

$\Rightarrow$ Acceptance probability is a degree-$2t$ polynomial $\square$

Observations ① We may also assume that the polynomial has no variable with individual degree >1 ie. no x_i^2 or x_i^3 in any monomial since x_i only takes ± 1 values. Such polynomials are called multilinear and any such polynomial can be expressed as $\sum_{S \subseteq [N]} c_S \prod_{i \in S} x_i$

② polynomial only takes values between $[0,1]$ on any input $x \in \{\pm 1\}^N$

The takeaway If we can show that any polynomial that approximates OR of N-bits has degree $\Omega(\sqrt{N}) \Rightarrow$ Quantum queries needed is also $\Omega(\sqrt{N})$

Formally, for any polynomial p satisfying $|p(w) - OR_N(w)| < \frac{1}{3} \ \forall w$

we want to show that $\deg(p) = \Omega(\sqrt{N})$

This notion is called approximate degree

Approximate Degree of OR How do we bound the approximate degree ?

We use the following two observations $\Rightarrow$

① OR_N is a symmetric function of the bits i.e. if we permute the bits the output does not change

Let us define a symmetrized version of p

$$p_{sym}(x_1,\dots,x_N) = \frac{1}{N!} \sum_{\sigma \in S_N} p(x_{\sigma(1)},\dots,x_{\sigma(N)})$$

$\hookrightarrow$ still a polynomial of degree $\leq 2t$ Why ?

Claim If p was a approximating polynomial for OR_N, so is p_{sym}.

Proof If $x_1 \dots x_N = 1^N$, then $p(1,\dots 1) \in [0,\frac{1}{3}]$

and $p_{sym}(1,\dots 1) = \frac{1}{N!} N! \ p(1,\dots 1) \in [0,\frac{1}{3}]$

If $\exists$ a bit that is -1, then each permutation $x_{\sigma(1)} \dots x_{\sigma(N)}$ can also not be all 1's

Thus, $p(x_{\sigma(1)},\dots x_{\sigma(N)}) \in [\frac{2}{3},1]$ for each σ

So, $p_{sym}(x_1,\dots x_N) \in \frac{1}{\cancel{N!}} \cancel{N!} [\frac{2}{3},1]$ ∎

② For any input $x_1 \dots x_N \in \{\pm 1\}^N$

$p_{sym}(x_1,\dots x_N)$ only depends on the number of -1's in the input which we will call the Hamming weight of x & denote by $|x|$

$\Rightarrow$ We can define a univariate polynomial $p_{uni}(k)$ s.t. $p_{sym}(x_1 \dots x_N) = p_{uni}(|x|)$

Claim Define the univariate function

$$P_{uni}(k) = \mathbb{E}_{x \text{ s.t. } |x|=k}\left[p(x_1,\ldots x_N)\right]$$

This is a polynomial of degree $\leq 2t$.

Proof Write $p(x_1,\ldots x_N) = \sum_{S \subseteq [N]} \alpha_S \prod_{i \in S} x_i$ where $\alpha_S = 0$ if $|S| > 2t$ and $x \in \{\pm 1\}^N$

Let us do a variable substitution $x_i = 2z_i - 1$ where $z_i \in \{0,1\}$

We get a polynomial $q(z_1,\ldots z_N) = \sum_{S \subseteq [N]} \beta_S \prod_{i \in S} z_i$ where $z_1,\ldots z_N \in \{0,1\}$

where $\beta_S = 0$ if $|S| > 2t$

$$\mathbb{E}_{|x|=k}\Big[p(\underbrace{x_1,\ldots x_N}_{\pm 1})\Big] = \mathbb{E}_{|z|=k}\Big[q(\underbrace{z_1,\ldots z_N}_{0/1})\Big] \quad \text{where } |x| = \#\,-1\text{'s}, \; |z| = \#\,1\text{'s}$$

Thus,

$$P_{uni}(k) = \sum_{S \subseteq [N]} \beta_S \underbrace{\mathbb{E}_{|z|=k}\Big[\prod_{i \in S} z_i\Big]}$$

$$= \frac{\binom{n-|S|}{k-|S|}}{\binom{n}{k}} = \frac{(n-|S|)!}{(k-|S|)!\,\cancel{(n-k)!}} \cdot \frac{k!\,\cancel{(n-k)!}}{n!}$$

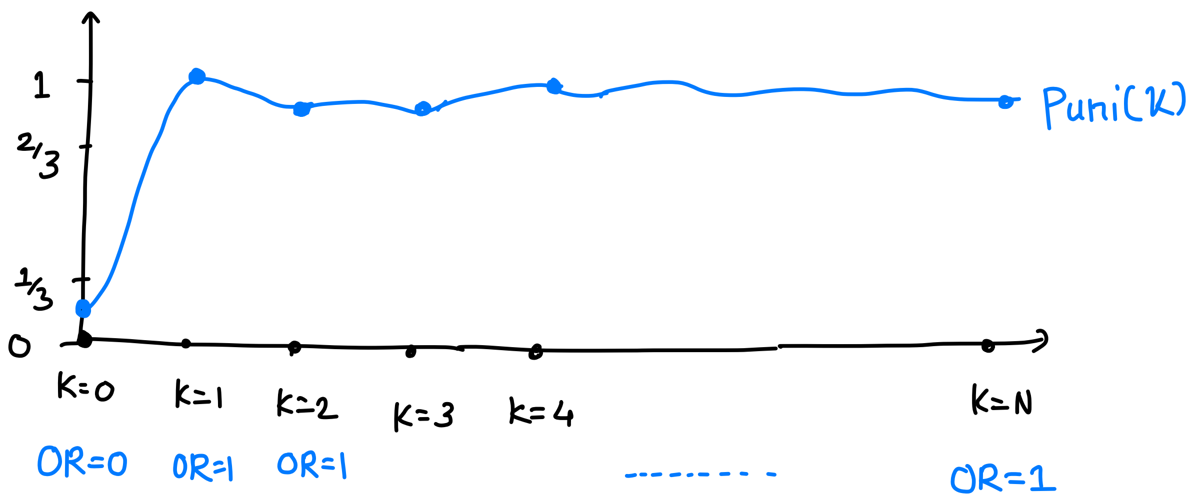
$$= \frac{(n-|S|)!}{n!}\, k(k-1)(k-2)\cdots(k-|S|+1)$$

$$= \sum_{S \subseteq [N]} \beta_S \frac{(n-|S|)!}{n!}\, k(k-1)\cdots(k-|S|+1)$$

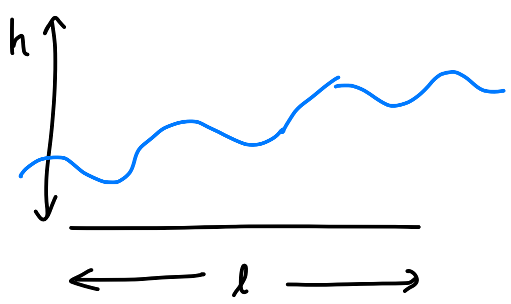
is a polynomial of degree $|S| \leq 2t$ since otherwise $\beta_S = 0$ ∎

So far, we have a univariate polynomial of degree $\leq 2t$ that approximates OR_N on all Hamming weights

$P_{uni}(k) =$



Lemma (Markov Brothers' Inequality 1890's) If p is a univariate polynomial that is bounded in some box of height h and length ℓ, then



$$|p'(z)| \leq \frac{h}{\ell} \deg(p)^2$$

for z in the box

Our polynomial p_{uni} is in $[0,1]$ on integer points $k = 0, 1, \ldots, N$

Let us suppose first that it was bounded in $[0,1]$ in the whole interval $k \in [0,N]$

Then, we have, $h = 1$, $\ell = N$ so maximum derivative $\leq \frac{\deg(p_{uni})^2}{N}$

but maximum derivative $\geq \frac{1}{3}$ [Why?]

$$\Rightarrow \deg(p_{uni}) \geq \Omega(\sqrt{N}) \quad \blacksquare$$

Now, since we only have that $p_{uni}(k) \in [0,1]$ for integer $k = 0, 1, 2, \ldots N$ how do we fix the argument?

Let $c = \max_{z \in [0,N]} |p'_{uni}(z)|$ be the maximum value of the derivative

Then, the following claim has a simple one line proof you can think about

Claim If $p_{uni}(k) \in [0,1]$ for $k = 0, 1, 2, \ldots N$ and c be as above.

Then $p_{uni}(k) \in \left[-\frac{c}{2}, 1 + \frac{c}{2}\right]$ for all $k \in [0,N]$ (including non-integer points)

Now, applying Markov's inequality with $h = 1 + c$, gives $c \leq \frac{(1+c)}{N} \deg(p_{uni})^2$

$$\Rightarrow \deg(p_{uni}) \geq \sqrt{\frac{Nc}{1+c}} \geq \Omega(\sqrt{N}) \quad \text{since } c \geq 1/3$$

The polynomial method is very powerful and can be used to prove lower bounds for many functions

There is another general purpose method called the adversary method that we will not cover here

NEXT TIME BQP vs PH