Lecture 13

1. Quantum query complexity
2. polynomials
3. polynomial method

Refs

[AMC] CH 20

[KLM] 9.5

[Beals et al '98]

---

1 Query Complexity

Task: given $x \in S \subseteq \{0,1\}^n$, compute $f(x)$

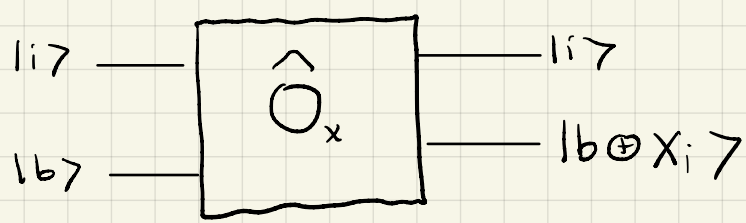
$S = \{0,1\}^n$: f is a "total function"

$S \neq \{0,1\}^n$: f is a "partial fcn"

Input x is given via oracle

$1 \le i \le n$

$b \in \{0,1\}$



Sometimes you might see a "phase oracle" O_x defined by

$$O_x |i\rangle|b\rangle = (-1)^{x_i b} |i\rangle|b\rangle$$

To implement O_x using $\hat{O}_x$:

$$(I \otimes H)\, \hat{O}_x\, (I \otimes H)\, |i\rangle|b\rangle$$

$$= (I \otimes H)\, \hat{O}_x\, |i\rangle \left(\frac{|0\rangle + (-1)^b |1\rangle}{\sqrt{2}} \right)$$

$$= (I \otimes H)\, |i\rangle \left(\frac{|x_i\rangle + (-1)^b |1 \oplus x_i\rangle}{\sqrt{2}} \right)$$

$$= \begin{cases} |i\rangle|b\rangle & , x_i = 0 \\ -|i\rangle|b\rangle & , x_i = 1 \end{cases}$$

L query quantum algorithm

3 registers $|i\rangle|b\rangle|y\rangle$ ← ancillas

$$|\psi_L\rangle = V_{L+1} O_x V_L \cdots O_x V_2 O_x V_1 \overbrace{|0^m\rangle}$$

followed by measurement.

define

$Q_\epsilon(f)$ = min # of quantum queries required to compute f w/ worst case failure probability $\leq \epsilon$.

$R_\epsilon(f)$ = min # of classical queries to f to compute f w/ failure prob $\leq \epsilon$
using a randomized alg.

$Q(f) \stackrel{\text{def}}{=} Q_{1/3}(f)$

$R(f) \stackrel{\text{def}}{=} R_{1/3}(f)$

$D(f)$ = " deterministic classical alg "

Examples

$$Q(OR_n) = O(\sqrt{n}) \qquad \text{Grover}$$

$$Q(OR_n) = \Omega(\sqrt{n}) \qquad \text{HW}$$

$$D(OR_n) = n$$

$$R(OR_n) = \Theta(n)$$

② Multivariate polynomials

Let $f: \{0,1\}^n \to \{0,1\}$

Claim: f has a unique representation as a multilinear polynomial in $x_1, \dots, x_n$ with real coefficients.

$$f(x_1, x_2, \dots, x_n) = \sum_{S \subseteq [n]} \alpha_S \, X(S)$$

$$\left\{ \begin{array}{l} \alpha_S \in \mathbb{R} \quad \forall S \\ X(S) \overset{\text{def}}{=} \prod_{i \in S} x_i \end{array} \right.$$

Pf: functions $f: \{0,1\}^n \to \mathbb{R}$ form a vector space of dim 2^n.
boolean functions are a subset.

monomials $X(S)$ independent for each $S \subseteq [n]$, form a basis for this vector space.

Expanded

let $z_i = 1 - 2x_i \in \{-1, 1\}$

$$f(z_1, \dots, z_n) = \sum_{S \subseteq [n]} \beta_S \, Z(S)$$

$$Z(S) = \prod_{i \in S} z_i$$

$$= \sum_{T \subseteq S} (-2)^T X(T)$$

$$\beta_S = \frac{1}{2^n} \sum_{z \in \{-1,1\}^n} f(z) \, Z(S)$$

<u>Bottom line</u>: for any $f : \{0,1\}^n \to \{0,1\}$ we can define

$$\boxed{\deg(f) = \text{degree of multivariate polynomial representation of } f}$$

③ Polynomial Method [Beals et al 98]

<u>Claim</u>: Consider the state of an L-query quantum alg.

$$|\psi_L\rangle = V_{L+1}\, O_x\, V_L \cdots O_x\, V_1\, |0^m\rangle$$

Then $\langle z|\psi_L\rangle$ is a polynomial in $x_1, x_2, \ldots, x_n$ of degree at most L for all $z \in \{0,1\}^m$.

<u>Pf</u>: Induction on L

Base case $L=0$ $\quad \langle z|\psi_L\rangle = \langle z|V_1|0^m\rangle$ has no dependence on $x_1, x_2, \ldots, x_n$ ✓

Induction step: $|\psi_{L-1}\rangle = V_L\, O_x \cdots O_x\, V_1\, |0^m\rangle$

$$= \sum_{\substack{z \in \{0,1\}^m \\ z=(i,b,y)}} p^z_{L-1}(x)\, |z\rangle$$

$L-1$ degree polynomial for each z.

$$O_x |\psi_{L-1}\rangle = \sum_{z=(i,b,y)} (-1)^{x_i b}\, p^z_{L-1}(x)\, |z\rangle = \sum_z \overbrace{(1-2bx_i)\, p^z_{L-1}(x)}^{\overset{\text{def}}{=} p^z_L(x)}\, |z\rangle$$

$(-1)^{x_i b} = 1 - 2x_i b$

//

<u>Corollary</u>: Suppose alg. outputs 1 with prob

$$p_1 = \langle \psi_L | M | \psi_L \rangle \qquad M = \text{Herm. op.}$$

Then p_1 is a polynomial $x_1, x_2, \ldots, x_n$ of deg. $\leq 2L$

If alg has worst case success prob $\geq 1-\epsilon$

then

$$p_1(x) \begin{cases} \geq 1-\epsilon & \text{if } f(x) = 1 \\ \leq \epsilon & \text{if } f(x) = 0 \end{cases}$$

$$(*) \quad \boxed{|p_1(x) - f(x)| \leq \epsilon \qquad \forall x \in \{0,1\}^n}$$

An L-query alg. succeeds w. failure prob $\leq \epsilon$ $\Longrightarrow$ $\exists$ degree $\leq 2L$ polynomial p_1 satisfying $(*)$.

Approximate degree

$$\widetilde{\deg}_\epsilon(f) = \min\{\deg(p) : |p(x) - f(x)| \le \epsilon \ \forall x \in \{0,1\}^n\}$$

$$\widetilde{\deg}(f) \overset{\text{def}}{=} \widetilde{\deg}_{1/3}(f)$$

LOWER BOUNDS ON QUERY COMPLEXITY $Q(f)$ FOLLOW FROM LB on $\widetilde{\deg}(f)$.

Aside: Symmetric functions

Suppose $f : \{0,1\}^n \to \{0,1\}$ is symmetric

$$\iff f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) \quad \forall \pi \in S_n$$

$\iff f(x)$ depends only on $|x| = \sum_{i=1}^n x_i$ "Hamming weight"

let $\quad F(k) = f(\underbrace{111\ldots1}_{k}\underbrace{00\ldots0}_{n-k}) \qquad 0 \le k \le n$

<u>Claim:</u> $F(k)$ is a polynomial of degree $\le \deg(f)$.

<u>Pf:</u>

$$F(k) = \mathbb{E}_{|x|=k}[f(x)]$$

$$= \mathbb{E}_{|x|=k}\left[\sum_{S\subseteq[n]} \alpha_S X(S)\right]$$

$$= \sum_{S\subseteq[n]} \alpha_S \mathbb{E}_{|x|=k}\left[\prod_{i\in S} x_i\right]$$

degree $\le \deg(f)$

$$\mathbb{E}_{|x|=k}\left(\prod_{i\in S} x_i\right) = \frac{1}{\binom{n}{k}}\binom{n-|S|}{k-|S|} = \frac{(n-|S|)!}{(k-|S|)!\,\cancel{(n-k)!}} \cdot \frac{k!\,\cancel{(n-k)!}}{n!}$$

$=1$ only if $S \subseteq$ k e/s of x that are 1

Choose S plus $k-|S|$ other bits of x to be $+1$.

$$= \underbrace{\frac{(n-|S|)!}{n!}}_{\text{doesn't depend on } k} \underbrace{k(k-1)\cdot(k-2)\ldots(k-|S|+1)}_{\text{degree } |S| \text{ polynomial}}$$