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 function"

Input $x$ is given via oracle

$1 \leq i \leq n$

$1 \leq i \leq \log_2 n$
Sometimes you might see a "phase oracle" \( \hat{O}_x \) defined by

\[
\hat{O}_x \left| i > 1 b > \right. = (-1)^{x_i b} \left| i > 1 b > \right.
\]

To implement \( O_x \) using \( \hat{O}_x \):

\[
(I \otimes H) \hat{O}_x (I \otimes H) \left| i > 1 b > \right.
\]

\[
= (I \otimes H) \hat{O}_x \left| i > 7 \left( \frac{107 + (-1)^b \left| 1 b > \right.}{\sqrt{2}} \right) \right.
\]

\[
= (I \otimes H) \left| i > 7 \left( \frac{1x_i \left| 7 + (-1)^b \left| 1 \right. \otimes x_i \left| 7 \right.}{\sqrt{2}} \right) \right.
\]

\[
= \left\{ \begin{array}{l}
\left| i > 1 b > \right., \quad x_i = 0 \\
-\left| i > 1 b > \right., \quad x_i = 1
\end{array} \right.
\]
14_L> = \mathbf{V}_{l+1} O_x \mathbf{V}_L \ldots O_x \mathbf{V}_2 O_x \mathbf{V}_1 10^m 7

followed by measurement.

define

Q_\varepsilon (f) = \min \# of quantum queries required to compute f in worst-case failure probability \leq \varepsilon.

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

D(f) = "deterministic classical alg."
Examples

\[ Q(OR_n) = O(\sqrt{n}) \quad \text{Grover} \]
\[ Q(OR_n) = \Omega(\sqrt{n}) \quad \text{HW} \]

\[ D(OR_n) = n \]
\[ R(OR_n) = \Theta(n) \]

2 Multivariable polynomials

Let \( f : \Sigma_0 \Sigma^n \rightarrow \Sigma_0 \Sigma^n \)

**Claim:** \( f \) has a unique representation as a multilinear polynomial in \( x_1, \ldots, x_n \) with real coefficients.

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

**Proof:** functions \( f : \Sigma_0 \Sigma^n \rightarrow \mathbb{R} \) 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.
**Expanded**

Let $z_i = 1 - 2x_i \in \{0, 1\}$

$$f(z_1, \ldots, z_n) = \sum_{s \in \{0, 1\}^n} \beta_s \ Z(s)$$

$$\beta_s = \frac{1}{2^n} \sum_{t \in \{0, 1\}^n} f(t) \ Z(s)$$

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

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

**Bottom line:** for any $f: \{0, 1\}^n \to \{0, 1\}$ we can define

$$\text{deg}(f) = \text{degree of multivariate polynomial representation of } f$$
Claim: Consider the state of an $L$-query quantum alg.

\[ 14_L > = V_{L+1} O_x V_L \ldots O_x V_1 10^{-7} \]

Then $<z|14_L>$ is a polynomial in $x_1, x_2, \ldots, x_n$ of degree at most $L$ for all $z \in \mathbb{F}_{0,1,2}^m$.

**Proof:** Induction on $L$

**Base case** $L = 0$ $<z|14_L> = <z|V_1 10^{-7}$ has no dependence on $x_1, x_2, \ldots, x_n$.

**Induction step:** $14_{L-1} > = V_L O_x \ldots O_x V_1 10^{-7}$

$O_x 14_{L-1} > = \sum_{x \in [i,b,y]} (-1)^b \rho^x_L (x) 127$ $= \sum_{z} \left( 1 - 2bx_i \right) \rho^x_{L-1} (x) 127$
Corollary: Suppose \( \text{alg.} \) outputs \( 1 \) with prob

\[
p_1 = \langle \mathcal{A}_1, M \rangle
\]

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

If \( \text{alg.} \) has worst case success prob \( \geq 1-\varepsilon \)

then \( p_1(x) \) satisfies

\[
\begin{align*}
|p_1(x) - f(x)| &\leq \varepsilon & \forall x \in \mathbb{F}_2^n \setminus \{y \}
\end{align*}
\]

An \( L \)-query \( \text{alg.} \) succeeds if degree \( \leq 2L \) polynomial \( p_1 \) satisfying (2).
Approximate degree

\[ \tilde{\deg}(f) = \min \{ \deg(p) : |p(x) - f(x)| \leq \epsilon \ \forall x \in \{0,1\}^n \} \]

\[ \tilde{\deg}(f) \overset{\text{def}}{=} \tilde{\deg}_\frac{1}{2}(f) \]

**Lower bounds on query complexity** \(Q(f)\)

**Follow from** \(LB\) on \(\tilde{\deg}(f)\)

 Aside: Symmetric functions

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

\[ f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) \]

\[ \forall \ \pi \in S_n \]

\[ \iff f(x) \text{ depends only on } |x| = \sum_{i=1}^{n} x_i \]

"Hamming weight"
Let \( F(K) = f \left( \frac{111 \cdots 100 \cdots 0}{K} \right) \) for \( 0 \leq K \leq n \).

Claim: \( F(K) \) is a polynomial of degree \( \leq \deg(f) \).

Proof:

\[
F(k) = \sum_{\substack{\text{1x}_1=k \\ \text{1x}_1=k}} \left[ \sum_{s \in [n]} \alpha_s \times (s) \right] \\
= \sum_{s \in [n]} \alpha_s \times \left[ \prod_{\substack{\text{1x}_1=k \\ \text{from}s}} \times_i \right] \\

\]

Choose some \( k - 1 \) elements of \( X \) to be \( +1 \) or \( x \) to be \( 0 \).

Choose \( s \) plus \( k - 1 \) of \( x \) to be \( +1 \).

\[
\sum = \binom{n-151}{k-151} = \frac{(n-151)!}{(k-151)!(n-k)!} + \frac{k! (n-k)!}{n!} \\

\]

only if \( s \leq k \) or \( 151 \) such that \( x \).