COL7160 : Quantum Computing

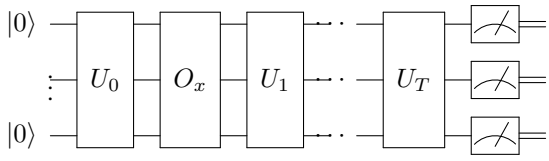
Lecture 23 : Quantum Query Lower Bound: Adversary Method

Instructor: Rajendra Kumar **Scribe:** Vivswan Savyasachi

1 Quantum Query Lower Bound

1.1 Adversary Method

Consider an input string $x \in \{0,1\}^N$ for a decision problem. We evaluate the problem using a standard quantum query model.



Let the state after U_0 but before the first oracle call be $|\psi_0\rangle$. Depending on the input x, the state evolves to $|\psi_t^{(x)}\rangle$ after t queries. The final states before measurement are $|\psi_T^{(y)}\rangle$ and $|\psi_T^{(z)}\rangle$ for inputs y and z respectively.
For the algorithm to successfully distinguish a "yes" instance y from a "no" instance z with high probability, the final states must be sufficiently distinguishable. We require:

$$|\langle\psi_T^{(y)}|\psi_T^{(z)}\rangle| \leq 0.9$$

The adversary method bounds the rate at which the inner product between states for YES and NO instances can diverge with each oracle application [dW23].

Theorem 1 (Unweighted Adversary Bound [Amb02])**.** *For a boolean function f, let $Y \subseteq f^{-1}(1)$ and $Z \subseteq f^{-1}(0)$ be subsets of YES and NO instances. Suppose there exists a relation $R \subseteq Y \times Z$ such that:*

- *For every $(y,z) \in R$, the Hamming distance is dist$(y,z) = 1$.*
- *For each $y \in Y$, there are at least m strings $z \in Z$ such that $(y,z) \in R$.*
- *For each $z \in Z$, there are at least m' strings $y \in Y$ such that $(y,z) \in R$.*

Then the bounded-error quantum query complexity of f is bounded by:

$$Q(f) = \Omega\left(\sqrt{m \cdot m'}\right)$$

1.2 Application: The OR Problem

We apply the adversary bound to the N-bit OR function, $f(x) = \bigvee_{i=1}^{N} x_i$.
Define the sets as follows:

$$Z = \{0^N\}$$
$$Y = \{y \in \{0,1\}^N : \text{Hamming weight } |y| = 1\}$$

We define the relation $(y,z) \in R \iff \text{dist}(y,z) = 1$.

- For a given $y \in Y$ (which contains exactly one '1'), there is exactly $m = 1$ string in Z at distance 1, namely 0^N.
- For the given $z \in Z$ (0^N), there are exactly $m' = N$ strings in Y at distance 1, corresponding to flipping each of the N bits.

Applying the theorem:

$$Q(\text{OR}) \geq c\sqrt{m \cdot m'} = c\sqrt{1 \cdot N} = c\sqrt{N}$$

Thus, any quantum algorithm requires $\Omega(\sqrt{N})$ queries to compute the OR function, demonstrating that Grover's algorithm is optimal [Gro96].

Remark 2. Point to Ponder: While the unweighted method easily captures the $\Omega(\sqrt{N})$ bound for the OR function, consider what happens for functions where YES and NO instances have highly asymmetric distances, or where the "neighborhood" sizes vary drastically. The restriction that $\text{dist}(y, z) = 1$ becomes a severe bottleneck for bounding the complexity of more complex algorithms, such as those solving the Collision Problem.

2 Proof of the Adversary Bound

Let the relation set be $R = \{(y, z) \in Y \times Z : \text{dist}(y, z) = 1\}$. Define a progress measure S_t as the sum of the inner products over all related pairs at step t:

$$S_t = \sum_{(y,z)\in R} |\langle \psi_t^{(y)} | \psi_t^{(z)} \rangle|$$

At $t = 0$, before any oracle calls, the states are identical and independent of the input ($|\psi_0^{(y)}\rangle = |\psi_0^{(z)}\rangle = |\psi_0\rangle$). Since unitary operations preserve the inner product:

$$S_0 = \sum_{(y,z)\in R} 1 = |R|$$

To successfully distinguish the instances, a necessary condition at the final step T is:

$$S_T \leq 0.9|R|$$

Proposition 3. *The change in the progress measure S_t after a single oracle query is bounded by:*

$$S_t - S_{t+1} \leq \frac{2}{\sqrt{mm'}} \cdot |R|$$

Proof. Consider the state representation. For a given pair $(y, z) \in R$, we can write the state $|\psi_t\rangle$ in the computational basis where the oracle acts:

$$|\psi_t^{(y)}\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle |\varphi_i\rangle \quad \text{and} \quad |\psi_t^{(z)}\rangle = \sum_{i=1}^{N} \beta_i |i\rangle |\theta_i\rangle$$

where $|\varphi_i\rangle$ and $|\theta_i\rangle$ are unit vectors in the workspace register, and $\sum_i |\alpha_i|^2 = \sum_i |\beta_i|^2 = 1$. Note that α_i and β_i depend implicitly on y and z respectively.
The oracle application maps $|i\rangle \to (-1)^{x_i} |i\rangle$. Therefore:

$$|\psi_{t+1}^{(y)}\rangle = \sum_{i=1}^{N} (-1)^{y_i} \alpha_i |i\rangle |\varphi_i\rangle$$

$$|\psi_{t+1}^{(z)}\rangle = \sum_{i=1}^{N} (-1)^{z_i} \beta_i |i\rangle |\theta_i\rangle$$

Let $S'_t = \langle \psi_t^{(y)} | \psi_t^{(z)} \rangle$ and $S'_{t+1} = \langle \psi_{t+1}^{(y)} | \psi_{t+1}^{(z)} \rangle$.

$$S'_t = \sum_{i=1}^{N} \alpha_i^* \beta_i \langle \varphi_i | \theta_i \rangle$$

$$S'_{t+1} = \sum_{i=1}^{N} (-1)^{y_i + z_i} \alpha_i^* \beta_i \langle \varphi_i | \theta_i \rangle$$

Since $(y, z) \in R$, we know $\text{dist}(y, z) = 1$. Let j^* be the unique index where $y_{j^*} \neq z_{j^*}$. For all $i \neq j^*$, $y_i = z_i$, so $(-1)^{y_i+z_i} = 1$. For $i = j^*$, $y_{j^*} + z_{j^*} = 1$, so $(-1)^{y_{j^*}+z_{j^*}} = -1$.
The difference in the inner product is isolated to the single index j^*:

$$S'_t - S'_{t+1} = 2\alpha^*_{j^*}\beta_{j^*} \langle \varphi_{j^*} | \theta_{j^*} \rangle$$

Using the triangle inequality and the fact that workspace states are unit vectors ($| \langle \varphi | \theta \rangle | \leq 1$):

$$| \langle \psi^{(y)}_t | \psi^{(z)}_t \rangle | - | \langle \psi^{(y)}_{t+1} | \psi^{(z)}_{t+1} \rangle | \leq 2|\alpha_{j^*}| \cdot |\beta_{j^*}|$$

Applying the AM-GM inequality in the form $2ab \leq ca^2 + \frac{1}{c}b^2$ with $c = \sqrt{m/m'}$:

$$2|\alpha_{j^*}| \cdot |\beta_{j^*}| \leq \sqrt{\frac{m}{m'}}|\alpha_{j^*}(y)|^2 + \sqrt{\frac{m'}{m}}|\beta_{j^*}(z)|^2$$

Now, we sum this difference over all pairs in R:

$$S_t - S_{t+1} \leq \sqrt{\frac{m}{m'}} \sum_{(y,z)\in R} |\alpha_{j^*(y,z)}(y)|^2 + \sqrt{\frac{m'}{m}} \sum_{(y,z)\in R} |\beta_{j^*(y,z)}(z)|^2$$

Let us analyze the first sum: $\sum_{(y,z)\in R} |\alpha_{j^*}(y)|^2$. We can rewrite this by fixing $y \in Y$ and summing over valid $z \in Z$:

$$\sum_{y\in Y} \left(\sum_{z:(y,z)\in R} |\alpha_{j^*(y,z)}(y)|^2 \right)$$

Because y is fixed, each z that is at distance 1 from y must differ from y at a distinct index j^*. Thus, as we sum over z, the index j^* takes on unique values. This implies the inner sum is bounded by the total norm of the state:

$$\sum_{z:(y,z)\in R} |\alpha_{j^*(y,z)}(y)|^2 \leq \sum_{i=1}^{N} |\alpha_i(y)|^2 = 1$$

Summing this bound over all $y \in Y$ yields:

$$\sum_{(y,z)\in R} |\alpha_{j^*}(y)|^2 \leq |Y|$$

By an identical symmetric argument for fixed z, the second sum is bounded by $|Z|$. Substituting these back gives:

$$S_t - S_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$$

By the degree constraints of our bipartite relation graph R: $|R| \geq m|Y|$ and $|R| \geq m'|Z|$. Therefore:

$$\frac{|R|}{\sqrt{mm'}} \geq \sqrt{\frac{m}{m'}}|Y| \quad \text{and} \quad \frac{|R|}{\sqrt{mm'}} \geq \sqrt{\frac{m'}{m}}|Z|$$

Summing these two inequalities gives:

$$\frac{2|R|}{\sqrt{mm'}} \geq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$$

Which proves our proposition. □

Conclusion of Theorem: The total drop in the progress measure after T queries is bounded by T times the maximum drop per query:

$$S_0 - S_T \leq T \cdot \frac{2|R|}{\sqrt{mm'}}$$

We require $S_0 - S_T \geq |R| - 0.9|R| = 0.1|R|$ for successful distinction. Thus:

$$0.1|R| \leq T \cdot \frac{2|R|}{\sqrt{mm'}} \implies T \geq 0.05\sqrt{mm'}$$

This concludes the proof that $Q(f) = \Omega(\sqrt{mm'})$.

Remark 4. Point to Ponder: Is this lower bound always tight? The unweighted version presented here is not tight for all functions. It was later demonstrated that by assigning an arbitrary real weight matrix Γ to the pairs (y, z) (the Negative-Weight Adversary Method), the bound becomes perfectly tight, characterizing the exact quantum query complexity for any boolean function.

Next Topic → Quantum Money.

References

[Amb02] Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

[dW23] Ronald de Wolf. Quantum computing: Lecture notes, 2023.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. Association for Computing Machinery.