COL7160 : Quantum Computing

Lecture 23: Quantum Query Lower Bounds: The Adversary Method

Instructor: Rajendra Kumar **Scribe:** Payas Khurana

1 Query model and problem setup

Definition 1 (Promise decision problem)**.** A promise decision problem on N bits is specified by two disjoint sets $Y, Z \subseteq \{0,1\}^N$. The task is to output 1 on inputs in Y and 0 on inputs in Z. We write $Q(\varphi)$ for the bounded-error quantum query complexity of the problem $\varphi = (Y, Z)$, with error at most $1/3$.

Definition 2 (Quantum query algorithm)**.** A T-query quantum algorithm for input $x \in \{0,1\}^N$ has the form

$$|\psi_T^x\rangle = U_T O_x U_{T-1} O_x \cdots U_1 O_x U_0 |0\rangle ,$$

where the U_j are input-independent unitaries and O_x is the query oracle. For the analysis it is convenient to use the phase oracle

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

where $i \in [N]$ is the query register and w denotes all remaining workspace.

For each input x and each time step $t \in \{0, 1, \ldots, T-1\}$, let $|\psi_t^x\rangle$ be the state immediately before the $(t+1)$-st query. If we decompose

$$|\psi_t^x\rangle = \sum_{i=1}^{N} |i\rangle |\alpha_{t,i}^x\rangle ,$$

then we define

$$p_t^x(i) = \| |\alpha_{t,i}^x\rangle \|^2.$$

Thus $p_t^x(i)$ is the probability that the algorithm queries position i at time t on input x.

2 The progress measure

To prove a lower bound, we choose a relation $R \subseteq Y \times Z$ consisting of input pairs that should be hard to distinguish. For each pair $(y, z) \in R$, the algorithm must eventually give different outputs on y and z, even though these inputs are chosen to look very similar.

Definition 3 (Progress measure)**.** Fix a relation $R \subseteq Y \times Z$. For $t = 0, 1, \ldots, T$, define

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

The quantity S_t measures the total overlap between states corresponding to related yes/no instances. Initially all computations start from the same state, so every inner product equals 1.

Lemma 4 (Initial value)**.** *For the progress measure above,* $S_0 = |R|$.

Proof. Before any query, the algorithm has not seen the input, so $|\psi_0^y\rangle = |\psi_0^z\rangle$ for all y, z. Hence $|\langle \psi_0^y \mid \psi_0^z \rangle| = 1$ for every $(y, z) \in R$, and summing over all pairs gives $S_0 = |R|$. □

At the end of the computation, related yes- and no-instances must be distinguishable by the final measurement, so the corresponding final states cannot still have overlap close to 1.

Lemma 5 (Final value). *Suppose the algorithm solves φ with error at most $\varepsilon < 1/2$. Then there is a constant $c_\varepsilon < 1$ such that*

$$S_T \le c_\varepsilon |R|.$$

In particular, for the usual choice $\varepsilon = 1/3$, one may take $c_{1/3} = 2\sqrt{2}/3 < 1$.

Proof. For every $(y, z) \in R$, the final measurement accepts $y \in Y$ with probability at least $1 - \varepsilon$ and accepts $z \in Z$ with probability at most ε. Therefore the two measurement outcome distributions differ in total variation distance by at least $1 - 2\varepsilon$. By monotonicity of trace distance under measurements, the pure states $|\psi_T^y\rangle$ and $|\psi_T^z\rangle$ must satisfy

$$\sqrt{1 - |\langle \psi_T^y \mid \psi_T^z \rangle|^2} \ge 1 - 2\varepsilon.$$

Rearranging gives

$$|\langle \psi_T^y \mid \psi_T^z \rangle| \le 2\sqrt{\varepsilon(1-\varepsilon)} =: c_\varepsilon < 1.$$

Summing over all $(y, z) \in R$ proves the claim. □

So the only remaining question is: *how fast can one query reduce the progress measure?*

3 A one-query bound

From now on we restrict to the setting where every related pair differs in exactly one bit. For $(y, z) \in R$, let $i(y, z)$ denote the unique coordinate on which y and z differ.

Lemma 6 (Effect of one query). *For every related pair $(y, z) \in R$,*

$$\left| \langle \psi_{t+1}^y \mid \psi_{t+1}^z \rangle - \langle \psi_t^y \mid \psi_t^z \rangle \right| \le 2\sqrt{p_t^y(i(y,z))\, p_t^z(i(y,z))}.$$

Proof. Input-independent unitaries do not change inner products, so only the oracle call matters. Write

$$|\psi_t^x\rangle = \sum_{i=1}^{N} |i\rangle\, |\alpha_{t,i}^x\rangle\,.$$

Applying the phase oracle gives

$$O_x\, |\psi_t^x\rangle = \sum_{i=1}^{N} (-1)^{x_i}\, |i\rangle\, |\alpha_{t,i}^x\rangle\,.$$

If $(y, z) \in R$, then y and z differ only at the coordinate $i(y, z)$. Hence all terms in the inner product are unchanged except the one indexed by $i(y, z)$. Therefore

$$\begin{aligned} \left| \langle \psi_{t+1}^y \mid \psi_{t+1}^z \rangle - \langle \psi_t^y \mid \psi_t^z \rangle \right| &= 2 \left| \langle \alpha_{t,i(y,z)}^y \mid \alpha_{t,i(y,z)}^z \rangle \right| \\ &\le 2 \, \| \, |\alpha_{t,i(y,z)}^y\rangle \, \| \, \| \, |\alpha_{t,i(y,z)}^z\rangle \, \| \\ &= 2\sqrt{p_t^y(i(y,z))\, p_t^z(i(y,z))}, \end{aligned}$$

as claimed. □

The lemma says that a query only makes progress on a pair (y, z) if the algorithm places noticeable amplitude on the coordinate where those two inputs differ.

4 A simplified adversary theorem

Theorem 7 (Distance-1 adversary method)**.** *Let $\varphi = (Y, Z)$ be a promise decision problem. Suppose there is a relation $R \subseteq Y \times Z$ such that:*

1. *every $y \in Y$ is related to at least m strings $z \in Z$;*
2. *every $z \in Z$ is related to at least m' strings $y \in Y$;*
3. *every $(y, z) \in R$ satisfies $d_{\mathrm{H}}(y, z) = 1$.*

Then

$$Q(\varphi) = \Omega\Big(\sqrt{mm'}\Big).$$

Proof. For each $(y, z) \in R$, let $i(y, z)$ be the unique differing coordinate. Using the previous lemma and the triangle inequality,

$$\begin{aligned} S_t - S_{t+1} &\le \sum_{(y,z)\in R} \big|\langle \psi_{t+1}^y \mid \psi_{t+1}^z \rangle - \langle \psi_t^y \mid \psi_t^z \rangle\big| \\ &\le 2 \sum_{(y,z)\in R} \sqrt{p_t^y(i(y,z))\, p_t^z(i(y,z))}. \end{aligned}$$

Define

$$A_t := \sum_{(y,z)\in R} p_t^y(i(y,z)), \qquad B_t := \sum_{(y,z)\in R} p_t^z(i(y,z)).$$

By Cauchy–Schwarz,

$$S_t - S_{t+1} \le 2\sqrt{A_t B_t}.$$

We now bound A_t and B_t. Fix $y \in Y$. Since every related pair has Hamming distance 1, for a fixed index i there is at most one string z such that $(y, z) \in R$ and $i(y, z) = i$. Therefore

$$\sum_{z:(y,z)\in R} p_t^y(i(y,z)) \le \sum_{i=1}^{N} p_t^y(i) = 1.$$

Summing over all $y \in Y$ gives $A_t \le |Y|$. By the same argument, $B_t \le |Z|$. Hence

$$S_t - S_{t+1} \le 2\sqrt{|Y|\,|Z|}.$$

Next, the assumptions on m and m' imply

$$|R| \ge m|Y|, \qquad |R| \ge m'|Z|.$$

So

$$\sqrt{|Y|\,|Z|} \le \frac{|R|}{\sqrt{mm'}}.$$

Combining this with the previous inequality, we obtain

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

Summing over all $t = 0, 1, \ldots, T-1$ and using the bounds on S_0 and S_T,

$$(1 - c_{1/3})|R| \le S_0 - S_T = \sum_{t=0}^{T-1} (S_t - S_{t+1}) \le \frac{2T|R|}{\sqrt{mm'}}.$$

Therefore

$$T \ge \frac{1 - c_{1/3}}{2}\sqrt{mm'} = \Omega\Big(\sqrt{mm'}\Big),$$

which proves the theorem. □

Remark 8 (General adversary method). The theorem above is the special case of Ambainis's adversary bound [Amb02]. In the general version, related inputs may differ in more than one coordinate. One then introduces two additional parameters, usually denoted ℓ and ℓ', measuring how many related pairs can disagree on the same index from the yes and no sides, respectively. The lower bound becomes

$$Q(\varphi) = \Omega\left(\sqrt{\frac{mm'}{\ell\ell'}}\right).$$

The distance-1 case treated here corresponds to $\ell = \ell' = 1$.

5 Application: the decision version of OR_N

Consider the promise problem underlying the usual OR function on N bits:

$$\mathrm{OR}_N(x) = 1 \iff \exists i \in [N] \text{ such that } x_i = 1.$$

To apply the theorem, choose

$$Y = \{e_1, e_2, \ldots, e_N\}, \qquad Z = \{0^N\},$$

where e_i is the string with a single 1 in position i and zeros elsewhere. Let

$$R = \{(e_i, 0^N) : i \in [N]\} \subseteq Y \times Z.$$

Each related pair differs in exactly one bit, so condition (3) holds. Also:

- every yes-input e_i is related to exactly one no-input, so $m = 1$;
- the single no-input 0^N is related to all N yes-inputs, so $m' = N$.

Therefore the theorem yields

$$Q(\mathrm{OR}_N) = \Omega(\sqrt{N}).$$

This matches Grover's upper bound $Q(\mathrm{OR}_N) = O(\sqrt{N})$ [Gro96], and hence

$$Q(\mathrm{OR}_N) = \Theta(\sqrt{N}).$$

So Grover's search algorithm is optimal in the query model.

References

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

[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.