Quantum Query Complexity
PCMI Graduate Summer School 2023
Instructor: Yassine Hamoudi. Teaching assistant: Angelos Pelecanos.
Course page: `https://yassine-hamoudi.github.io/pcmi2023/`

Problem Session 3

The recording and adversary methods

Problem 1 (Recording method & Final condition)

Recall the SEARCH problem that asks to find a value i such that $x_i = 1$ using queries to a *uniformly random* input $x \in \{0, \ldots, n-1\}^n$. The progress measure Δ_t was defined as the probability that the record contains a solution $x_i = 1$ after t queries. The goal of the next questions is to show that the progress must be large for an algorithm to succeed.

Question 1. For any integer T, show that no *randomized* algorithm can succeed (i.e. output i such that $x_i = 1$) with probability larger than $\Delta_T + 1/n$ after T queries. Deduce a lower bound on the randomized query complexity of SEARCH.

Define Π_{rec} to be the operator that projects onto $\mathrm{span}\big\{|x_1, \ldots, x_n\rangle \otimes |i, b\rangle : 1 \in \{x_1, \ldots, x_n\}\big\}$ and Π_{succeed} to be the operator that projects onto $\mathrm{span}\big\{|x_1, \ldots, x_n\rangle \otimes |i, b\rangle : x_i = 1\big\}$. Recall that the quantum progress after T queries is $\Delta_T = \|\Pi_{\mathrm{rec}}|\psi^T_{\mathrm{rec}}\rangle\|^2$ and the probability to succeed is $\|\Pi_{\mathrm{succeed}}|\psi^T\rangle\|^2$.

Question 2.1. Compute the norm $\|\Pi_{\mathrm{succeed}}(S^{\otimes n}|x_1, \ldots, x_n\rangle) \otimes |i, b\rangle\|$ when $x_i = \varnothing$, $x_i = 1$ and $x_i \in \{0, \ldots, n-1\} \setminus \{1\}$.

Question 2.2. Using the relation $|\psi^T\rangle = (S^{\otimes n} \otimes \mathrm{Id})|\psi^T_{\mathrm{rec}}\rangle$, show that $\|\Pi_{\mathrm{succeed}}|\psi^T\rangle\| \leq \sqrt{\Delta_T} + O(1/\sqrt{n})$.

Question 2.3. Deduce a lower bound on the quantum query complexity of SEARCH.

Problem 2 (Recording method & Collision finding)

The COLLISION problem asks to find a pair of values $i \neq j$ such that $x_i = x_j$ using queries to a *uniformly random* input $x \in \{0, \ldots, n-1\}^n$.

Question 1. Give a classical algorithm showing that the randomized query complexity of COLLISION is at most $O(\sqrt{n})$.

Consider the progress measure Δ_t defined as the probability that the record contains a collision after t queries.

Question 2. Use the classical recording method to show that $\Delta_t = O(t^2/n)$ after t classical queries. Conclude that the randomized query complexity of COLLISION is at least $\Omega(\sqrt{n})$.

Question 3. Show that after t quantum queries, the state $|\psi^t_{\text{rec}}\rangle$ (defined in the recording query model) is always supported onto basis states $|x\rangle \otimes |i, b\rangle$ such that $|\{j : x_j \neq \varnothing\}| \leq t$.

Question 4. Use the quantum recording method to show that $\Delta_t = O(t^3/n)$ after t quantum queries, where Δ_t is the probability that the record register in $|\psi^t_{\text{rec}}\rangle$ contains a collision.

> The quantum query complexity of the COLLISION problem was first established[1] using a rather complex polynomial symmetrization method.

Problem 3 (Combinatorial view on the adversary method)

Given a function $f : \{0,1\}^n \to \{0,1\}$, choose two sets $V_0 \subseteq \{x : f(x) = 0\}$, $V_1 \subseteq \{x : f(x) = 1\}$ and a bipartite graph G over (V_0, V_1). For each $1 \leq i \leq n$, define G_i to be the subgraph of G obtained by keeping the edges (x, y) for which $x_i \neq y_i$. Let m_0, m_1, ℓ_0, ℓ_1 be four integers such that each left (resp. right) vertex in G has degree at least m_0 (resp. m_1) and each left (resp. right) vertex in G_i has degree at most ℓ_0 (resp. ℓ_1) for all i.

Question 1. Let E (resp. E_i) be the set of edges in G (resp. G_i). Show that the deterministic query complexity of f is at least $D(f) \geq \frac{|E|}{\max_i |E_i|}$. Deduce that $D(f) \geq \max\left\{\frac{m_0}{\ell_0}, \frac{m_1}{\ell_1}\right\}$.

Question 2. Use the quantum adversary method to show that $Q(f) = \Omega\left(\sqrt{\frac{m_0 m_1}{\ell_0 \ell_1}}\right)$.

Question 3. Consider the k-THRESHOLD(x) function that evaluates to 1 if and only the Hamming weight of $x \in \{0,1\}^n$ is at least $|x| \geq k$. Use the above method to show that $D(f) = \Omega(\max\{n - k + 1, k\})$ and $Q(f) = \Omega(\sqrt{(n - k + 1)k})$.

Question 4. Consider the CONNECTIVITY function that takes as input the adjacency matrix $x \in \{0,1\}^{\binom{n}{2}}$ of an undirected n-vertex graph and that outputs 1 if it is connected. Use the above method to show that $D(\text{CONNECTIVITY}) = \Omega(n^2)$ and $Q(\text{CONNECTIVITY}) = \Omega(n^{3/2})$.

Hint: You can take $V_1 = \{x \in \{0,1\}^{\binom{n}{2}} : x \text{ represents a cycle graph}\}$.

[1] "Quantum Lower Bounds for the Collision and the Element Distinctness Problems". S. Aaronson and Y. Shi. *J. ACM*, 2004.