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 1

Basics of query complexity & The hybrid method

Problem 1 (Miscellaneous)

Question 1. Define $R_\epsilon(f)$ (resp. $Q_\epsilon(f)$) to be the smallest number of queries that a randomized (resp. quantum) algorithm has to do to be correct with probability at least $1-\epsilon$ on all inputs. Show that $R_\epsilon(f) \leq O(R(f)\log(1/\epsilon))$ and $Q_\epsilon(f) \leq O(Q(f)\log(1/\epsilon))$.

Question 2. Propose a way of extending the quantum query model to inputs $x \in \{0,\ldots,m-1\}^n$ over a larger alphabet of size $m > 2$.

Problem 2 (Parity)

This problem studies the quantum query complexity of the PARITY function. One may use the Hadamard transform H defined as $H|b\rangle = \frac{|0\rangle+(-1)^b|1\rangle}{\sqrt{2}}$ for $b \in \{0,1\}$.

Question 1. Define the *phase query* operator as the unitary $O_x^\pm$ such that $O_x^\pm|i,b\rangle = (-1)^{b\cdot x_i}|i,b\rangle$ for all $1 \leq i \leq n$ and $b \in \{0,1\}$. Let $Q^\pm(f)$ denote the corresponding query complexity of a function f, where O_x has been replaced with $O_x^\pm$ in the model. Show that $Q^\pm(f) = Q(f)$.

Question 2. Construct a quantum algorithm that compute the 2-bit function $f(x_1,x_2) = x_1 \oplus x_2$ with 1 query. Conclude that $Q(\text{PARITY}) \leq n/2$.

> We will see later in the course that $Q(\text{PARITY}) = \Omega(n)$. Currently, the hybrid method would only give $Q(\text{PARITY}) = \Omega(\sqrt{n})$.

Problem 3 (Block sensitivity)

The *block sensitivity* $\mathrm{bs}(f)$ of a function $f : \{0,1\}^n \to \{0,1\}$ is the largest number k such that there exists an input $x \in \{0,1\}^n$ and k disjoint subsets $B_1,\ldots,B_k \subseteq \{1,\ldots,n\}$ satisfying $f(x^{B_j}) \neq f(x)$ for all $1 \leq j \leq n$, where $x^{B_j} \in \{0,1\}^n$ is defined by $x_i^{B_j} = 1 - x_i$ when $i \in B_j$ and $x_i^{B_j} = x_i$ otherwise.

Question 1. Compute $\mathrm{bs}(f)$ for the OR, AND, PARITY and MAJORITY functions.

Question 2. Show the lower bound $R(f) = \Omega(\mathrm{bs}(f))$ on the randomized query complexity.

Question 3. Use the hybrid method to show that $Q(f) = \Omega(\sqrt{\mathrm{bs}(f)})$.

The goal of the next questions is to upper bound the deterministic query complexity $D(f)$ in terms of the block sensitivity.

Question 4.1. We say that $B \subseteq \{1, \ldots, n\}$ is a *minimal sensitive block* for $x \in \{0,1\}^n$ if $f(x^B) \neq f(x)$ and $f(x^{B'}) = f(x)$ for all proper subsets $B' \subsetneq B$. Show that any minimal sensitive block B for x must satisfy $f(x^B) \neq f(x^{B \setminus \{i\}})$ for all $i \in B$ and conclude that $|B| \leq \mathrm{bs}(f)$.

Question 4.2. We say that $C \subseteq \{1, \ldots, n\}$ is a *certificate* for $x \in \{0,1\}^n$ if for all $y \in \{0,1\}^n$ that agrees with x on C (i.e. $x_i = y_i$ for all $i \in C$) we have $f(x) = f(y)$. Show that for each x there exists some certificate C_x of size at most $|C_x| \leq \mathrm{bs}(f)^2$.

Question 4.3. Let $C^{(0)} = \{C_y : y \in \{0,1\}^n, f(y) = 0\}$ and $C^{(1)} = \{C_y : y \in \{0,1\}^n, f(y) = 1\}$. Consider the following algorithm:

```
repeat until C^(0) = ∅ or C^(1) = ∅:
  choose any C_y ← C^(0)
  query x_i for all i ∈ C_y
  remove from C^(0) and C^(1) all the sets C_z where z_i ≠ x_i for some i ∈ C_y
if C^(0) = ∅ then output 1 else output 0
```

Show that the algorithm outputs $f(x)$ and terminates after at most $\mathrm{bs}(f)^2$ repetitions.

Question 4.4. Conclude that $D(f) = O(\mathrm{bs}(f)^4)$ and $Q(f) \leq D(f) = O(Q(f)^8)$ for any function $f : \{0,1\}^n \to \{0,1\}$.

> One can improve the above arguments to show that[1,2] $D(f) = O(\mathrm{bs}(f)^3)$ and $D(f) = O(Q(f)^4)$. It is a major open problem to show whether $D(f) = O(\mathrm{bs}(f)^2)$.
>
> These results do not hold for *partial* functions $f : D \to \{0,1\}$ whose domain is a proper subset $D \subsetneq \{0,1\}^n$. In that case, the gap between $D(f)$ and $Q(f)$ can be exponential[3].

[1] "Quantum Lower Bounds by Polynomials". R. Beals, H. Buhrman, R. Cleve, M. Mosca, R. de Wolf. *J. ACM*, 2001.

[2] "Degree vs. Approximate Degree and Quantum Implications of Huang's Sensitivity Theorem". S. Aaronson, S. Ben-David, R. Kothari, S. Rao, A. Tal. *Proc. of STOC*, 2021.

[3] "Forrelation: A Problem that Optimally Separates Quantum from Classical Computing". S. Aaronson, A. Ambainis. *SICOMP*, 2018.