CO 781 / QIC 823 / CS 867 Quantum Algorithms
University of Waterloo, Winter 2017
Instructor: Ashwin Nayak

Assignment 2, Mar. 13, 2017
Due: by noon, Mar. 27, 2017

Question 1. Let $f : \{0,1\}^n \to \{0,1\}$. Let $R \subseteq X \times Y$ be a relation such that

1. X contains only 0-inputs, Y contains only 1-inputs, and both are non-empty.
2. For each $x \in X$, there are at least m inputs $y \in Y$ such that $(x, y) \in R$.
3. For each $y \in Y$, there are at least m' inputs $x \in X$ such that $(x, y) \in R$.
4. For each $x \in X$ and $i \in [n]$, there are at most ℓ_{xi} inputs $y \in Y$ such that $(x, y) \in R$ and $y_i \neq x_i$.
5. For each $y \in Y$ and $i \in [n]$, there are at most ℓ_{yi} inputs $x \in X$ such that $(x, y) \in R$ and $x_i \neq y_i$.

Let $L = \max_{x,y,i} \; \ell_{xi}\ell_{yi}$. Prove that the adversary bound for f is at least $\sqrt{mm'/L}$.

Question 2. Use the adversary method to prove the following query bounds, given the input via an oracle.

(a) The parity function $f : \{0,1\}^n \to n$ is defined as $f(x) = \bigoplus_{i=1}^n x_i$. Prove a lower bound of $\Omega(n)$ for computing f.

(b) Let $G = (V, E)$ be an undirected graph on n vertices, which is described by an oracle for its adjacency matrix. Prove that the query complexity of determining whether the input graph is connected is $\Omega(n^{3/2})$.

Question 3. Let G be a finite abelian group, and let $\hat{G}$ denote the set of its irreps. Define a binary operation '$\circ$' on $\hat{G}$ as $(\sigma \circ \tau)(x) = \sigma(x)\,\tau(x)$ for all $x \in G$.

(a) Verify that $\hat{G}$ endowed with this operation is an abelian group of the same order as G.

(b) For any $x \in G$, define $\chi_x : \hat{G} \to \mathbb{C}$ as $\chi_x(\sigma) = \sigma(x)$. Verify that χ_x is an irrep of $\hat{G}$.

(c) Prove that $x \mapsto \chi_x$ is an isomorphism between G and $\hat{\hat{G}}$. (Note that $\hat{\hat{G}}$ is the group of irreps of $\hat{G}$.)

(In answering this question, use only elementary group theory and the properties of linear representations we learnt in class.)

Question 4. Consider the multiplicative group $\mathbb{Z}_p^*$, where p is a prime. Let the element g be a generator of the group. In the Discrete Logarithm problem, the input is an element $x \in \mathbb{Z}_p^*$, and the task is to determine $k \pmod{p-1}$ such that $g^k = x$.

(a) Consider the following superposition over group elements:

$$|\psi_j\rangle \quad = \quad \frac{1}{\sqrt{p-1}} \sum_{i=0}^{p-2} \omega^{ij} |g^i\rangle,$$

where ω is a primitive $(p-1)$-th root of unity. Show that this is an eigenvector of the operator

$$U_a : |y\rangle \mapsto |ay\rangle$$

for any $a \in \mathbb{Z}_p^*$. Find the corresponding eigenvalue.

(b) With the group element $x = g^k$ and the superposition $|\psi_j\rangle$ as input, and using part (a) above, show how you can construct the superposition

$$\frac{1}{\sqrt{p-1}} \sum_{i=0}^{p-2} \omega^{-ik} |i\rangle.$$

State any assumptions you need to make.

(c) Describe an algorithm based on parts (a) and (b) to compute Discrete Logarithms. State its time and space complexity.