Quantum algorithms (CO 781/CS 867/QIC 823) Winter 2013

ASSIGNMENT 3 due Tuesday 2 April (in class)

Problem 1 (*A limitation on quantum speedup for total functions*).

In this problem, you will show that quantum computers can obtain at most a polynomial speedup for the query complexity of total functions.

a. Given a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, a *certificate* for f on input $x \in \{0,1\}^n$ is a subset of the bits of x such that the value of $f(x)$ is determined by those bits alone. Let $C_x(f)$ denote the size of the smallest certificate for f on input x, and let $C(f) := \max_{x\in\{0,1\}^n} C_x(f)$ (this is called the *certificate complexity* of f). What is $C(\textsc{or})$?

b. Consider the following algorithm for computing $f(x)$:

Let $c \leftarrow \emptyset$
While c does not certify that $f(x) = 0$
  Choose $x' \in \{0,1\}^n$ such that $f(x') = 1$ and $x_i = x'_i$ for all $i \in c$
  Let c' be a minimal certificate for x'
  Query x_i for $i \in c'$
  Let $c \leftarrow c \cup c'$
  If c certifies that $f(x) = 1$ then return "1"
End while
Return "0"

Show that this algorithm uses at most $C(f)^2$ queries.

c. For $x \in \{0,1\}^n$ and $S \subseteq \{1,\ldots,n\}$, let $x^{(S)}$ denote x with x_i replaced by $\bar{x}_i$ for all $i \in S$. Call S a *sensitive block* of x if $f(x) \neq f(x^{(S)})$. Prove that if $S_1,\ldots,S_k$ is a maximal set of disjoint sensitive blocks of x (i.e., there is no other sensitive block that is disjoint from all of $S_1,\ldots,S_k$), then $S_1 \cup \cdots \cup S_k$ is a certificate for $f(x)$.

d. Let $\mathrm{bs}_x(f)$ denote the largest possible number of disjoint sensitive blocks of x, and let $\mathrm{bs}(f) := \max_{x\in\{0,1\}^n} \mathrm{bs}_x(f)$ (this is called the *block sensitivity* of f). Call a sensitive block S *minimal* if no subset of S is sensitive. Show that if S is a minimal sensitive block of some input, then $|S| \leq \mathrm{bs}(f)$.

e. Prove that $C(f) \leq \mathrm{bs}(f)^2$.

f. Let $x \in \{0,1\}^n$ have disjoint sensitive blocks $S_1,\ldots,S_{\mathrm{bs}(f)}$. For any $y \in \{0,1\}^{\mathrm{bs}(f)}$, let $x^{[y]}$ denote x with x_i replaced by $\bar{x}_i$ if $i \in S_j$ and $y_j = 1$ for some $j \in \{1,\ldots,\mathrm{bs}(f)\}$. Given a polynomial $p\colon \{0,1\}^n \to \mathbb{R}$, define a polynomial $p'\colon \{0,1\}^{\mathrm{bs}(f)} \to \mathbb{R}$ by $p'(y) := p(x^{[y]})$. Explain why $\deg(p') \leq \deg(p)$.

g. Prove that $\widetilde{\deg}(f) = \Omega(\sqrt{\mathrm{bs}(f)})$. (*Hint:* Generalize the proof that $\widetilde{\deg}(\textsc{or}) = \Omega(\sqrt{n})$, using p' in place of the original approximating polynomial p.)

h. Conclude that $Q(f) = \Omega(D(f)^{1/8})$, where $D(f)$ denotes the deterministic classical query complexity of f.

Problem 2 (*Combinatorial formulation of the adversary method*).

For a Boolean function $f\colon \{0,1\}^n \to S$, the adversary method says that $Q_\epsilon(f) \geq \frac{1-2\sqrt{\epsilon(1-\epsilon)}}{2}\operatorname{Adv}(f)$, where $\operatorname{Adv}(f) := \max_\Gamma \frac{\|\Gamma\|}{\|\Gamma_i\|}$, with the maximization is over all adversary matrices Γ for f.

Ambainis originally formulated the adversary method differently, as follows. Let $X, Y \subset \{0,1\}^n$ such that $f(x) \neq f(y)$ for all $x \in X, y \in Y$. For any relation $R \subset X \times Y$, define

$$m := \min_{x\in X} |\{y \in Y\colon (x,y) \in R\}| \qquad \ell := \max_{\substack{x\in X \\ i\in\{1,\ldots,n\}}} |\{y \in Y\colon (x,y) \in R \text{ and } x_i \neq y_i\}|$$

$$m' := \min_{y\in Y} |\{x \in X\colon (x,y) \in R\}| \qquad \ell' := \max_{\substack{y\in Y \\ i\in\{1,\ldots,n\}}} |\{x \in X\colon (x,y) \in R \text{ and } x_i \neq y_i\}|.$$

Then define $\operatorname{Amb}(f) := \max_{X,Y,R} \sqrt{\frac{mm'}{\ell\ell'}}$.

Prove that $\operatorname{Adv}(f) \geq \operatorname{Amb}(f)$, and hence that $Q_\epsilon(f) \geq \frac{1-2\sqrt{\epsilon(1-\epsilon)}}{2}\operatorname{Amb}(f)$.

Problem 3 (*Applying the adversary method*).

Use the adversary method to prove the following lower bounds. (You should apply the adversary method directly to the given function rather than giving a reduction from some other problem.)

a. (*Parity*) Define $\textsc{parity}\colon \{0,1\}^n \to \{0,1\}$ by $\textsc{parity}(x) = x_1 \oplus \cdots \oplus x_n$. Show that $Q(\textsc{parity}) = \Omega(n)$.

b. (*Graph connectivity*) With $x \in \{0,1\}^{\binom{n}{2}}$ specifying an n-vertex graph as in problem 5 from assignment 2, define $\textsc{con}\colon \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ by

$$\textsc{con}(x) = \begin{cases} 1 & \text{if the graph described by } x \text{ is connected} \\ 0 & \text{otherwise.} \end{cases}$$

Show that $Q(\textsc{con}) = \Omega(n^{3/2})$.

Problem 4 (*Quantum query complexity of formula evaluation*).

An AND-OR formula is a Boolean formula specified by a rooted tree in which every leaf represents an input bit, the root represents the output bit, and each internal vertex represents an AND or OR gate acting on its children. In this problem, you will use the adversary method and its dual to characterize the quantum query complexity of evaluating a Boolean formula on a black-box input.

a. Consider functions $g_i\colon \{0,1\}^{m_i} \to \{0,1\}$ for each $i \in \{1,\ldots,\ell\}$. Let $n := \sum_{i=1}^{\ell} m_i$. Define $f\colon \{0,1\}^n \to \{0,1\}$ by $f(x_1,\ldots,x_m) := \textsc{or}(g_1(x_1,\ldots,x_{m_1}),\ldots,g_\ell(x_{n-m_\ell+1},\ldots,x_n))$. Show that $\operatorname{Adv}^{\pm}(f) \geq \sqrt{\sum_{i=1}^{\ell} \operatorname{Adv}^{\pm}(g_i)^2}$. (*Hint:* Use optimal adversary matrices for $g_1,\ldots,g_\ell$ to construct an adversary matrix for f.)

b. Let the functions g_i and f be as in the previous part. Show that $\operatorname{Adv}^{\pm}(f) \leq \sqrt{\sum_{i=1}^{\ell} \operatorname{Adv}^{\pm}(g_i)^2}$. (*Hint:* Use optimal dual adversary solutions for $g_1,\ldots,g_\ell$ to construct a dual adversary solution for f.)

c. Show that part a also holds if OR is replaced by AND in the definition of f.

d. Show that part b also holds if OR is replaced by AND in the definition of f.

e. Prove that any n-input AND-OR formula has bounded-error quantum query complexity $\Theta(\sqrt{n})$.

Problem 5 (*Algorithms for st-connectivity and path detection*).

In the undirected *st*-connectivity problem, we are given a black box for the edges of an undirected graph G with vertex set $[n] := \{1, \ldots, n\}$. There are two distinguished vertices $s, t \in [n]$, and the goal is to determine whether there is a path joining s and t (i.e., whether $t \in C_s(G)$, where $C_s(G) \subseteq [n]$ denotes the component of G containing s). We consider this problem with the promise that if $t \in C_s(G)$, there is a path between s and t of length at most d.

a. A dual adversary solution consists of vectors $|v_{G,\{u,w\}}\rangle$ for each n-vertex graph G and each potential edge $\{u, w\}$ with $u, w \in [n]$. Suppose that for $t \notin C_s(G)$, we let

$$|v_{G,\{u,w\}}\rangle = \begin{cases} |u\rangle - |w\rangle & \text{if } u \in C_s(G) \text{ and } w \notin C_s(G) \\ 0 & \text{if } u, w \in C_s(G) \text{ or } u, w \notin C_s(G). \end{cases}$$

Give a dual adversary solution by choosing vectors $|v_{G,\{u,w\}}\rangle$ for the case where $t \in C_s(G)$. Prove that your choice indeed gives a dual adversary solution. (You can use the relaxed form of the dual adversary in which $\sum_{i:\, x_i \neq x'_i} \langle v_{x,i} | v_{x',i} \rangle$ is unconstrained for $f(x) = f(x')$.)

b. Compute the complexity of the solution as a function of n and d, and thereby give an upper bound on the quantum query complexity of *st*-connectivity.

c. Suppose each vertex from $[n]$ has a label from $[k+1]$ assigned to it. (These labels are fixed in advance and do not require any queries to learn.) We say that a graph with this labeled vertex set has a *sequential k-path* if it has a k-path in which the jth vertex has label j. Using the result of the previous part, show that for any fixed k, there is an algorithm for deciding whether a black-box graph has a sequential k-path using $O(n)$ quantum queries to the edges.

d. Consider the problem of deciding whether a graph contains a path of length k. Show that this problem also has quantum query complexity $O(n)$ for any fixed k.

e. *Research problem:* Consider the problem of *finding* (rather than simply detecting) a path of length k in a black-box graph. For what values of k is there an algorithm for finding a path of length k using $O(n)$ queries?