6.845 Problem Set 3: Quantum Algorithms and Lower Bounds

1. In the *Bernstein-Vazirani problem*, we are given oracle access to a Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$, and promised that there exists a string $s \in \{0,1\}^n$ such that $f(x) = s \cdot x \pmod 2$ for all x. The problem is to find s.

   (a) Give a deterministic algorithm that finds s using n queries to f.

   (b) Show that any classical algorithm (deterministic or randomized) needs $\Omega(n)$ queries to find s.

   (c) Give a quantum algorithm that finds s using only a single query to f. [*Hint:* Hadamards.]

2. Define *Simon's problem* as follows. We are given oracle access to a Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}^n$, and are promised that either (i) f is one-to-one, or (ii) f is *Simon*, meaning that there exists a "secret string" $s \neq 0^n$ such that $f(x) = f(y)$ if and only if $x = y \oplus s$ for all x, y.

   (a) In class, we handwaved that there exists a randomized algorithm that solves Simon's problem using $O\left(2^{n/2}\right)$ queries to f. Prove this.

   (b) In class, we handwaved that any randomized algorithm that solves Simon's problem needs $\Omega\left(2^{n/2}\right)$ queries to f. Prove this.

   (c) In class, we described a quantum algorithm that repeatedly samples a random string $z \in \{0,1\}^n$ such that $z \cdot s = 0 \pmod 2$. We handwaved that, with high probability, $O(n)$ such strings z are enough to uniquely determine s. Prove this.

3. **Oracle separations.**

   (a) Show that, if a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is Simon rather than one-to-one, then there is a polynomial-size classical *witness* proving that fact, which can be verified in deterministic polynomial time (i.e., in P).

   (b) Show by contrast that, if f is one-to-one rather than Simon, then there is no polynomial-size classical witness proving that fact, which can be verified in P.

   (c) *[Extra credit]* Using part b., show that there exists an oracle A such that $\mathsf{BQP}^A \not\subset \mathsf{NP}^A$.

   (d) *[Extra extra credit]* Extend your analysis to show that there exists an oracle A such that $\mathsf{BQP}^A \not\subset \mathsf{MA}^A$.

4. Recall from class that the "Almost-As-Good-As-New Lemma" says the following:

   Let M be a measurement with two possible outcomes ("accept" and "reject"), and suppose that M accepts a mixed state ρ with probability at least $1 - \varepsilon$. Then after applying M to ρ, it is possible to recover a state $\widetilde{\rho}$ such that $\|\widetilde{\rho} - \rho\|_{\text{tr}} \leq \sqrt{\varepsilon}$. Here $\| \|_{\text{tr}}$ denotes the usual trace distance metric.

   Prove the AAGANL. [For this problem, you can assume that M is a *projective measurement*: that is, a unitary transformation on ρ, followed by a measurement in the standard basis.]

5. Consider using Grover's algorithm to search a database of N items, of which $T \geq 1$ items are "marked." Assume T is known in advance.

   (a) Show that Grover's algorithm can be used to find a marked item with constant probability after $O\left(\sqrt{N/T}\right)$ queries. [*Note:* You do not need to worry about computation cost, just the number of queries. Also, there are two ways to solve this problem: you can either apply Grover's algorithm to the multi-item case directly, or you can reduce to the case of a single marked item and then run Grover's algorithm on that case.]

   (b) Show that any quantum algorithm needs $\Omega\left(\sqrt{N/T}\right)$ queries to find a marked item with constant probability.

6. Show that any quantum algorithm to search a list $x_1, \ldots, x_n$ for a marked item, which succeeds with *zero probability of error* regardless of the number of marked items, requires $\Omega(n)$ queries (i.e., does essentially no better than classical search). [*Hint:* Use the polynomial method.]

MIT OpenCourseWare
http://ocw.mit.edu

6.845 Quantum Complexity Theory
Fall 2010

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.