CS395T Problem Set 2

Sep. 30, 2016

1. **Distinguishing two quantum states.**

   (a) Show that there exists a measurement that, given as input either $|\psi\rangle = a|0\rangle + b|1\rangle$ or $|\varphi\rangle = a|0\rangle - b|1\rangle$, for some real numbers a, b with $a^2 + b^2 = 1$, correctly identifies which state it was given with probability $\frac{1}{2}(a+b)^2$.

   (b) Given two pure quantum states $|\psi\rangle = \alpha_1 |1\rangle + \cdots + \alpha_N |N\rangle$ and $|\varphi\rangle = \beta_1 |1\rangle + \cdots + \beta_N |N\rangle$, recall that their inner product is defined to be

   $$\langle\psi|\varphi\rangle = \alpha_1^* \beta_1 + \cdots + \alpha_N^* \beta_N.$$

   Show that unitary transformations preserve inner product: that is, if $|\psi'\rangle = U|\psi\rangle$ and $|\varphi'\rangle = U|\varphi\rangle$, then $\langle\psi'|\varphi'\rangle = \langle\psi|\varphi\rangle$.

   (c) Show that there exists a measurement that, given as input either $|\psi\rangle$ or $|\varphi\rangle$, correctly identifies which state it was given with probability $\frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi|\varphi\rangle|^2}$. So in particular, if $\langle\psi|\varphi\rangle = 0$ (i.e., $|\psi\rangle$ and $|\varphi\rangle$ are *orthogonal*) then they can be distinguished perfectly. [*Hint:* Use symmetry to reduce to part a.]

2. Recall that a density matrix ρ is an $N \times N$ Hermitian positive semidefinite matrix with trace equal to 1. If a quantum system in state ρ is measured in the standard basis, the result is $|i\rangle$ with probability $(\rho)_{ii}$; if a unitary transformation U is applied to the system, then the density matrix of the transformed system is $U\rho U^{-1}$. Given two $N \times N$ density matrices ρ and σ, recall that their *trace distance* is defined to be

   $$\|\rho - \sigma\|_{\mathrm{tr}} = \frac{1}{2} \sup_U \operatorname{Tr} \left| U\rho U^{-1} - U\sigma U^{-1} \right|,$$

   where the supremum is over all $N \times N$ unitary matrices U. Trace distance is a measure of the distance between two quantum states.

   (a) Show that $0 \le \|\rho - \sigma\|_{\mathrm{tr}} \le 1$ for all quantum states ρ and σ.

   (b) Show that if a measurement accepts the state ρ with probability p, then it accepts the state σ with probability between $p - \|\rho - \sigma\|_{\mathrm{tr}}$ and $p + \|\rho - \sigma\|_{\mathrm{tr}}$.

   (c) Show that for pure states, trace distance is related to inner product via the following formula: $\| |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \|_{\mathrm{tr}} = \sqrt{1 - |\langle\psi|\varphi\rangle|^2}$.

   (d) Combining b. and c., show that the measurement you designed in problem 1 was the optimal one. That is, *any* measurement either mistakes $|\psi\rangle$ for $|\varphi\rangle$ or vice versa with probability at least $\frac{1}{2} - \frac{1}{2}\sqrt{1 - |\langle\psi|\varphi\rangle|^2}$.

3. Recall the definition of BQP, as the class of languages $L \subseteq \{0,1\}^*$ decidable with bounded probability of error by a uniform family $\{C_n\}_{n \ge 1}$ of polynomial-size quantum circuits. Here uniform means there exists a deterministic (classical) algorithm that, given n as input, outputs a description of C_n in time polynomial in n. Show that we get the same complexity class, if we instead allow a quantum algorithm to output C_n (or more precisely, a probability distribution over C_n's). Here, in the preceding sentence, "quantum algorithm" means one defined using the original definition of BQP.

4. Say a problem B is *complete* for the complexity class $\mathcal{C}$ if (i) B is in $\mathcal{C}$, and (ii) every problem in $\mathcal{C}$ can be reduced to B in deterministic polynomial time (i.e., $\mathcal{C} \subseteq \mathsf{P}^B$).

   (a) Let $\mathsf{PromiseBQP}$ be the class of *promise problems* efficiently solvable by a quantum computer: that is, the set of all ordered pairs $\Pi_{YES} \subseteq \{0,1\}^*$, $\Pi_{NO} \subseteq \{0,1\}^*$ such that

   - $\Pi_{YES} \cap \Pi_{NO} = \varnothing$, and
   - there exists a uniform family of polynomial-size quantum circuits that decides, given an input x, whether $x \in \Pi_{YES}$ or $x \in \Pi_{NO}$ with bounded probability of error, promised that one of these is the case.

   Give an example of a promise problem that's complete for $\mathsf{PromiseBQP}$. [*Hint:* This problem just requires understanding the definitions; it does not require cleverness.]

   (b) Explain the basic difficulty in finding a language $L \subseteq \{0,1\}^*$ that's complete for BQP.

5. Recall Simon's problem: given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$, and promised there exists a secret string $s \neq 0$ such that $f(x) = f(y)$ if and only if $x = y \oplus s$, find s. Simon's algorithm works by repeatedly finding a uniform random $z \in \{0,1\}^n$ such that $s \cdot z = 0 \,(\mathrm{mod}\, 2)$. Assuming this, show that s is uniquely determined after $O(n)$ steps, with all but exponentially small probability.

6. In class, we discussed how to use Simon's problem to construct an oracle A such that $\mathsf{BPP}^A \neq \mathsf{BQP}^A$.

   (a) Consider the variant of Simon's problem where we're promised that *either* f is a one-to-one function (in which case the answer is YES), or else f satisfies the usual Simon promise (in which case the answer is NO). Show that this variant is not even solvable in NP: that is, YES answers have no polynomial-size certificates that can be verified in polynomial time.

   (b) *[Extra credit]* MA (Merlin-Arthur) is a probabilistic version of NP. Formally, MA is the class of languages $L \subseteq \{0,1\}^*$ for which there exists a probabilistic polynomial-time Turing machine M such that for all inputs x:

   - If $x \in L$, then there exists a polynomial-size witness w such that $M(x,w)$ accepts with probability 1.
   - If $x \notin L$, then $M(x,w)$ accepts with probability at most $1/2$ regardless of the witness w.

   Using the same variant of Simon's problem from part a., show that there exists an oracle A such that $\mathsf{BQP}^A \not\subset \mathsf{MA}^A$.

7. 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.