6.845 Problem Set 2: Basic Training for the BQP Army

Do any 7 of the 10 problems—the remaining 3 are extra credit.

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

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

   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 $|\varphi\rangle$ each with probability $\frac{1}{2}$, correctly identifies which state it was given with probability $\frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi|\varphi\rangle|^2}$. [*Hint:* Use symmetry to reduce to part (a.).]

2. **Trace distance.** Recall the formalism of *density matrices* from pset1. 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, 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 and the absolute value of a matrix is taken entrywise. Trace distance is a measure of the distance between two quantum states.

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

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

   (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. **Density matrices and quantum algorithms.** Let $f : \{1, \ldots, N\} \to \{0, 1\}$ be a Boolean function. Consider a quantum algorithm that first prepares an equal superposition over all inputs $x \in \{1, \ldots, N\}$, then computes f in superposition, then runs the f algorithm backwards to uncompute garbage. This algorithm proceeds through the following three states:

$$\frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle \to \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle |\text{garbage}_x\rangle |f(x)\rangle \to \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle |f(x)\rangle.$$

Describe the *density matrix of the* $|x\rangle$ *register only* for each of these three states. [Here you can assume the map $x \to \text{garbage}_x$ is injective. You can also fix a particular f for definiteness: for example, $f(x) = 1$ if $x \geq N/2$ and $f(x) = 0$ otherwise.]

4. **Errors in a quantum computation build up linearly rather than exponentially.**

   (a) Show that trace distance (defined in problem 2) satisfies the triangle inequality:

   $$\|\rho - \xi\|_{\text{tr}} \leq \|\rho - \sigma\|_{\text{tr}} + \|\sigma - \xi\|_{\text{tr}}$$

   (b) Let $U_1, \ldots, U_T$ be "ideal" unitary matrices, and let V_t be a noisy approximation to U_t that our quantum computer actually implements. Suppose $\left\| U_t \rho U_t^\dagger - V_t \rho V_t^\dagger \right\|_{\text{tr}} \leq \varepsilon$ for all mixed states ρ and all t. Show that for all ρ,

   $$\left\| U_T \cdots U_1 \rho U_1^\dagger \cdots U_T^\dagger - V_T \cdots V_1 \rho V_1^\dagger \cdots V_T^\dagger \right\|_{\text{tr}} \leq \varepsilon T.$$

   [*Hint:* This doesn't follow *directly* from part (a.) – do you see why not? – though you'll certainly want to use part (a.)]

5. **Uniformity.** Recall the definition of BQP as the class of languages $L \subseteq \{0, 1\}^*$ decidable with bounded probability of error by a uniform family $\{C_n\}_{n \geq 1}$ 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 BQP algorithm to output C_n (or more precisely, a probability distribution over C_n's).

6. **Complete problems.** For our purposes, 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 is complete for BQP.

7. **Improved upper bound on BQP.** Probabilistic Polynomial-Time, or PP, is defined as the class of languages $L \subseteq \{0,1\}^*$ for which there exists a probabilistic Turing machine M such that for all inputs x:

   - If $x \in L$ then $M(x)$ accepts with probability $\geq 1/2$.
   - If $x \notin L$ then $M(x)$ accepts with probability $< 1/2$.

   It is clear that $\mathsf{BPP} \subseteq \mathsf{PP} \subseteq \mathsf{P}^{\#\mathsf{P}}$. Show that $\mathsf{BQP} \subseteq \mathsf{PP}$, thereby improving the result from class that $\mathsf{BQP} \subseteq \mathsf{P}^{\#\mathsf{P}}$. [*Hint:* First show how to write the acceptance probability p_C of a quantum circuit C as the sum of exponentially many complex numbers, each computable in polynomial time. Then show how this implies the existence of a PP machine to decide whether $p_C \geq 1/2$.]

8. **Equivalence of two types of quantum queries.** In class, we saw two types of quantum queries. Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, a *phase query* maps each basis state $|x,a,z\rangle$ to $(-1)^{a \cdot f(x)}|x,a,z\rangle$, where a is a "control qubit" that is set to 1 if and only if the query should happen. A *XOR query* maps each basis state $|x,a,z\rangle$ to $|x, a \oplus f(x), z\rangle$, where a is a 1-qubit "answer register".

   (a) Show how to simulate a phase query to f using a single XOR query. [*Hint:* What happens when you Hadamard a before querying?]

   (b) Show how to simulate a XOR query to f using a single phase query.

9. **Reals vs. complex amplitudes.** Show that any quantum computation involving complex amplitudes, can be polynomially simulated by another quantum computation involving real amplitudes only. [*Hint:* Double the number of basis states.]

10. **Number of quantum states.** Let H_N be the set of pure quantum states over the basis $|1\rangle, \ldots, |N\rangle$ (in other words, unit vectors in $\mathbb{C}^N$). Also, fix a constant $c > 0$.

    (a) Show that one can find $T = 2^{\Omega(N)}$ states $|\psi_1\rangle, \ldots, |\psi_T\rangle$ in H_N, such that $|\langle\psi_i|\psi_j\rangle| \leq c$ for all $i \neq j$. [*Hint:* It suffices to restrict attention to states of the form $\frac{1}{\sqrt{N}} \sum_{i=1}^{N} (-1)^{x_i} |i\rangle$. Do you see a connection to error-correcting codes?]

    (b) Let G be a finite, universal set of quantum gates. Using part (a.), show that there exist quantum states $|\psi\rangle$ of n qubits that require $2^{\Omega(n))}$ gates from G to prepare even approximately. In other words, the exponential dependence on n in the Solovay-Kitaev Theorem is necessary.

    (c) *[Extra credit]* Show that when c is close to 1, the bound from part a. can be sharpened to $T \geq \left(\frac{1}{1-c}\right)^{\Omega(N)}$.

6.845 Quantum Complexity Theory
Fall 2010