CS667/CO681/PH767/AM871 Quantum Information Processing (Fall 09)

Assignment 5

Due date: December 3, 2009

1. **Trace distance between pure states.**

   (a) Calculate an expression for the trace distance between $|0\rangle$ and $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ as a function of θ.

   (b) Calculate an expression for the Euclidean distance between the two points in the Bloch sphere that correspond to the pure states $|0\rangle$ and $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$.

2. **Amplitude amplification.** Consider a generalization of the search problem where, we are given a black box computing $f : \{0,1\}^n \to \{0,1\}$, and the goal is to find $x_0 \in \{0,1\}^n$ such that $f(x_0) = 1$ (for simplicity let us suppose here that x_0 is unique). Suppose that we are given another black box computing an n-qubit "guessing" unitary operation U_G that helps guess a satisfying assignment to f. The property of U_G is formally that $\langle x_0|U_G|0^n\rangle = \sqrt{p}$, for some number $p \in [0,1]$, which is interpreted as follows. Applying U_G to the initial state $|0^n\rangle$ and measuring in the computational basis results in x_0 with probability p. We would expect to repeat this process $O(1/p)$ times until x_0 is found, resulting in $O(1/p)$ queries to both the black box for f and the black box for U_G.

   (a) Show that the n-qubit Hadamard transform is always a guessing unitary with parameter $p = 1/2^n$.

   (b) There are cases where better guessing unitaries exist than the Hadamard, with $1/2^n \ll p \ll 1$. Show that $-U_G U_0 U_G^\dagger U_f$ applies a rotation by angle $2\sin^{-1}(\sqrt{p})$ in the two dimensional space spanned by $|x_0\rangle$ and $U_G|0^n\rangle$. Here, as in Grover's algorithm, U_f is the unitary that maps $|x\rangle$ to $(-1)^{f(x)}|x\rangle$, and U_0 is the unitary that maps $|x\rangle$ to
   $$\begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n. \end{cases} \tag{1}$$
   (Hint: use the property of two reflections being a rotation.)

   (c) Deduce from part (b) that x_0 can be found with probability at least $3/4$ (say) using only $O(\sqrt{1/p})$ queries to U_f, U_G, and $U_G^\dagger$.

3. **Two noisy channels.** Consider these two noise models for a one-qubit channel. The first channel performs
   $$\begin{cases} I & \text{with probability } 1-p \\ X & \text{with probability } p/3 \\ Y & \text{with probability } p/3 \\ Z & \text{with probability } p/3 \end{cases} \tag{2}$$
   and the second channel leaves its qubit intact with probability $1-q$ and replaces its qubit with one in state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ with probability q. Show that, for all $q \in [0,1]$, there is a value of $p \in [0,1]$ for which the first channel is equivalent to the second one.

4. **Sets of nearly orthogonal states.** Since a d-dimensional space can have at most d mutually orthogonal (non-zero) vectors, the number of qubits required to accommodate 2^n orthogonal states is n. What happens if we relax the orthogonality condition to one of ε-*nearly orthogonal*, meaning that the absolute value of the inner product between any two states is at most ε (rather than zero)? How many qubits are required to accommodate 2^n ε-nearly orthogonal states? We'll show that $O(\log(n/\varepsilon))$ qubits suffice (in other words, there are exponentially more ε-nearly orthogonal states than orthogonal states in any given finite dimension).

   Let $\varepsilon > 0$ be an arbitrarily small constant. Set q to any prime number between n/ε and $2n/\varepsilon$. First, for each $x \in \{0,1\}^n$, define the polynomial p_x as

$$p_x(t) = x_0 + x_1 t + x_2 t^2 + \cdots + x_{n-1} t^{n-1} \bmod p. \tag{3}$$

   Now, for each $x \in \{0,1\}^n$, define the state $|\psi_x\rangle$ as

$$|\psi_x\rangle = \frac{1}{\sqrt{q}} \sum_{t=0}^{q-1} |t\rangle |p_x(t)\rangle. \tag{4}$$

   (a) Explain why each $|\psi_x\rangle$ is a $2\log(2n/\varepsilon)$-qubit state.

   (b) Show that these 2^n states are pairwise ε-nearly orthogonal in the sense that, for all $x \neq y$, $|\langle \psi_x | \psi_y \rangle| \leq \varepsilon$.

5. **A nonlocal game.** Consider the following game. Alice and Bob receive $s, t \in \{0,1,2\}$ as input (s to Alice and t to Bob), at which point they are forbidden from communicating with each other. They each output a bit, a for Alice and b for Bob. The winning conditions are:

   - $a = b$ in the cases where $s = t$.
   - $a \neq b$ in the cases where $s \neq t$.

   (a) Show that any classical strategy that always succeeds in the $s = t$ cases can succeed with probability at most $2/3$ in the $s \neq t$ cases.

   (b) Give a quantum strategy (that is, one where Alice and Bob can base their outcomes on their measurement of an entangled state) that always succeeds in the $s = t$ cases and succeeds with probability $3/4$ in the $s \neq t$ cases. (Hint: try the entangled state $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$ and have Alice and Bob perform rotations depending on s and t respectively.)