CS667/CO681/PH767 Quantum Information Processing (Fall 07)

Assignment 5

Due date: December 3, 2007 [1]

1. **Description of a simple operation in the Krauss form.** Consider the operation that takes one qubit as input, and produces that qubit combined with another qubit in the state $|0\rangle$ as output. More precisely, the operation maps any state ρ to the state $\rho \otimes |0\rangle\langle 0|$. Give a description of this operation in the Krauss form.

2. **A nonlocal game.** Consider the following scenario, which is similar to that arising in the CHSH game. Alice and Bob, who cannot communicate once the game starts, receive input bits s and t respectively, and produce output bits a and b respectively. Assume that their protocol is guaranteed to respect the following *validity* conditions (suppose that any violation leads to an enormous fine that they cannot afford to risk):

   - If their inputs are $st = 00$, at least one of them *must* output 0.
   - If their inputs are $st = 01$ and Alice outputs 0 then Bob *must* output 0.
   - If their inputs are $st = 10$ and Bob outputs 0 then Alice *must* output 0.

   (a) Show that, for any classical protocol that is valid, on input $st = 11$ the output *cannot* be $ab = 11$.

   (b) Suppose that Alice and Bob have the entangled state $|\psi\rangle_{AB} = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$. Show that, using this state, there is a valid protocol that, on input $st = 11$, outputs $ab = 11$ with probability at least $\frac{1}{12}$. (Hint: consider the Hadamard transform.)

3. **Alternate construction of nearly orthogonal states.** Let $\epsilon > 0$ be a given parameter. Set q to any prime number between n/ϵ and $2n/\epsilon$. First, for each $x \in \{0,1\}^n$, define the polynomial p_x as $p_x(t) = x_0 + x_1 t + x_2 t^2 + \cdots + x_{n-1} t^{n-1}$. Now, for each $x \in \{0,1\}^n$, define the $2\log(2n/\epsilon)$-qubit state $|\psi_x\rangle$ as

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

   Show that these 2^n states (on only $O(\log(n/\epsilon))$ qubits!) are pairwise nearly orthogonal in the sense that, for all $x \neq y$, $|\langle \psi_x | \psi_y \rangle| \leq \epsilon$.

4. **Secret key encryption.** Recall the classical one-time pad encryption scheme. The scenario is that Alice wants to send a string of bits of information to Bob over a channel that is possibly being monitored by Eve (an eavesdropper). We assume that Alice and Bob share a secret key, which was set up in advance. The secret key is a randomly chosen (uniformly distributed) $k \in \{0,1\}^n$, which is known by Alice and Bob, but—importantly—not by Eve. If Alice wants to send the string $m \in \{0,1\}^n$ to Bob then she

[1] Can be submitted through the CS main office, or slipped under the door of DC 2117.

computes $c = m \oplus k$ (bitwise) and sends c over the channel. When Bob receives c, he computes $m' = c \oplus k$. It is fairly straightforward to show that $m' = m$ and Eve acquires no information about m from looking at c.

We now consider a similar scenario, but where Alice wants to send n qubits to Bob over a quantum channel that is possibly being monitored by Eve. For simplicity, we'll set $n = 1$. How can this be accomplished so that if Eve performs operations (including measurements) on the data that goes through the channel, she cannot acquire any information about what Alice's qubit is?

(a) If Alice and Bob share a classical secret key bit $k \in \{0, 1\}$, and $|\psi\rangle$ is the message that Alice wants to send, then one approach is for Alice to send $X^k|\psi\rangle$ to Bob. This seems analogous to the classical protocol: Alice either flips or doesn't flip the (qu)bit according to a random key bit. Show that this is highly insecure by giving two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$ whose encryptions Eve can perfectly distinguish.

(b) Suppose that Alice and Bob have two (independently generated) key bits k_1, k_2, and Alice encrypts $|\psi\rangle$ as $Z^{k_1}X^{k_2}|\psi\rangle$. (Note that Bob can decrypt this since he has k_1 and k_2.) Show that this is perfectly secure in the sense that, for any two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$, Eve cannot distinguish *at all* between their encryptions.