2.111/6.898/18.435/ESD.79J Practice Exam, December 16th, 2011

(1) Quantum Cryptography.

Quantum cryptography is a method for creating a shared, random secret key. The original protocal is called BB84 (Bennett-Brassard 1984). It works as follows.

Alice sends Bob a random sequence of qubit states chosen from the set $\{|\uparrow\rangle, |\downarrow\rangle, |\rightarrow\rangle, |\leftarrow\rangle\}$. Bob chooses at random to measure in either the z-basis or the x-basis. Afterwards, Alice and Bob call each other on the phone and determine which qubits Bob measured in the same basis as Alice sent them in. They then check a subset of those to see if Bob received the same state that Alice sent. If he received all qubits in the correct state, then Eve is not listening in, and Bob and Alice are assured that their remaining shared qubits are secret. If some fraction of the checked qubits differ from their proper values, then Alice and Bob can determine how much information Eve has obtained about their qubits.

(1a) Suppose that Eve measures each qubit in the z-basis then sends it on in the same state she measured. For what fraction of the qubits sent do Alice and Bob detect Eve's eavesdropping?

(1b) For what fraction of the qubits sent does Eve intercept the qubit sent without Alice and Bob detecting her evesdropping?

(1c) Suppose that Eve measures each qubit along an axis $\hat{j} = \cos\alpha\hat{z} + \sin\alpha\hat{x}$, and after measuring sends the qubit along in the same state she measured. What is the probability that Alice and Bob detect Eve? What α minimizes Eve's probability of being detected?

(2) Decoherence free subspace.

A collective error is one in which the same error occurs to each qubit. For example, if there are four qubits, a collective error could be of the form $U \otimes U \otimes U \otimes U$, where $U = e^{-i\theta\sigma/2}$ is a rotation by θ about an axis determined by σ. A four qubit quantum code to correct collective errors is defined as follows:

$$|0\rangle \rightarrow \frac{1}{2}(|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{12}}(2|1100\rangle + 2|0011\rangle - |1010\rangle - |0101\rangle - |0110\rangle - |1001\rangle).$$

(2a) Calculate the effect of an error $U \otimes U \otimes U \otimes U$ on the encoded version of the state $\alpha|0\rangle + \beta|1\rangle$, first for $U = \sigma_z$ and then for $U = e^{-i\theta\sigma_z/2}$. Show your work.

(2b) Calculate the effect of $U \otimes U \otimes U \otimes U$, where $U = e^{-i\theta\sigma_x/2}$.

(2c) Calculate the effect of $U \otimes U \otimes U \otimes U$, where $U = e^{-i\theta\sigma_y/2}$.

(2d) What is the effect of $U \otimes U \otimes U \otimes U$, for a generic $U = e^{-i\theta\sigma/2}$?

(3) Consider the operator

$$S = (1/2)(I \otimes I + \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z).$$

(3a) Show that $S^2 = 1$.

(3b) What is $S|\phi\rangle \otimes |\psi\rangle$? (Hint: S is called the 'swap' operator.)

(3c) What is $S|\Psi\rangle$, where $|\Psi\rangle = (1/\sqrt{2})(|0\rangle \times |1\rangle - |1\rangle \otimes |0\rangle)$ is the singlet state?

(3d) What is the effect of S on a triplet state?

(3e) Using S and $I \otimes I$, construct projection operators onto the singlet and triplet subspaces.