QUANTUM COMPUTATION - EXERCISE 5

Due: January 20 (submission in pairs).

1. Schmidt Decomposition

suppose you have a state such that its Schmidt decomposition has all vectors with the same weight:

$$|\phi\rangle = \sum_i \frac{1}{2^{n/2}} |\alpha_i\rangle |\beta_i\rangle .$$

Show that for any orthonormal basis $\{|\gamma_i\rangle\}$ of the space spanned by the $|\beta_i\rangle' s$, $|\phi\rangle$ has a Schmidt decomposition with the form:

$$\sum_i \frac{1}{2^{n/2}} |\delta_i\rangle |\gamma_i\rangle$$

(find $|\delta_i\rangle$ and show that they are mutually orthonormal).

2. Classical Cryptography

Explain why completely secure, and even 'somewhat' secure, classical bit commitment, classical coin flipping and classical key distribution are impossible, if we cannot assume any computational assumptions.

Make sure you deal with the most general case, i.e when the players can toss random bits (each in his/her own home) and these bits are unknown to the eavesdropper (if exists) nor to the other player (unless these bits have been sent on the channel).

3. Optimal Measurement

Repeat Question 3 of Exercise 1 of our course, in the language of density operators. Now prove that you found the optimal measurement, and analyze the probability of success.

4. Measurement Without Disturbance?

Bob prepares the system A in one of two *nonorthogonal* states, $|\phi\rangle_A$ or $|\psi\rangle_A$, and he challenges Alice to collect some information about which state he prepared *without in any way* disturbing the state. Alice has an idea about how to meet the challenge.

Alice intends to prepare a second "ancilliary" system B in the state $|\beta\rangle_B$, and then to apply to the composite system AB a unitary transformation U that acts according to

$$\begin{aligned} |\phi\rangle_A |\beta\rangle_B &\stackrel{U}{\to} |\phi\rangle_A |\beta_\phi\rangle_B \\ |\psi\rangle_A |\beta\rangle_B &\stackrel{U}{\to} |\psi\rangle_A |\beta_\psi\rangle_B , \end{aligned}$$

which does indeed leave the state of system A undisturbed. Then she plans to perform a measurement on system B that is designed to distinguish the states $|\beta_\phi\rangle$ and $|\beta_\psi\rangle$.

What do you think of Alice's idea? Prove.

5. Shor's Error Correcting Code

Give an exact analysis of what happens during an error of the type of a measurement (performed by the environment) in the $\{|+\rangle, |-\rangle\}$ basis of the second bit in Shor's 9-qubit code. What are the possible states after the error occurs, and what happens during the error correction procedure.