QUANTUM COMPUTATION - EXERCISE 4

Due: Wednesday, January 24

1. Schmidt Decomposition

Find the Schmidt decompositions of the states

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}};\ \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2};\ \frac{|01\rangle + |10\rangle + |11\rangle}{\sqrt{3}}$$

2. Density matrices & Optimal Measurement

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

3. Bit Commitment

Write the proof that the protocol suggested in class for bit commitment is insecure to both players, that is, prove that each of the players can cheat.

4. quantum coin flipping: proof details

In class, we have provided a quantum coin flipping protocol, and claimed that it has bias at most 19/20. We have begun in class to prove this, but did not finish the calculation. Complete the details of this proof for the case of a cheating Alice to find an explicit upper bound.

Remark: We leave the case of a cheating Bob incomplete. In class, we have only shown that Bob cannot completely control the result of Alice. But we did not give any quantitative upper bound. This requires some more technical calculations, and we will save you the effort...

5. The No Quantum Majority Theorem

Let us consider the following hypothetical transformation. The input is a state of three qubits of the form $|\alpha\rangle \otimes |\beta\rangle \otimes |\gamma\rangle$. In case two or three of the states are equal (say, to alpha), the transformation outputs a first qubit in the state $|\alpha\rangle$, tensor with some (never mind which) two qubit state. In other words, the first qubit will contain the majority of the three states. Prove that such a majority transformation does not exist according to the laws of quantum mechanics.

6. Measurement in terms of Pauli matrices

Write an error of the type of a measurement (performed by the environment) in the $\{|+\rangle, |-\rangle\}$ basis, as a linear combination of the Pauli matrices, as was done in class. Do the same for a measurement in the computational basis.

7. Shor's code

Suppose some general one qubit superposition, encoded by Shor's code, went through an error of the type of a measurement in the computational basis, applied on the rightmost qubit. Suppose the result of the measurement was 0. Write the state before and after the error, and analyze what happens during the different steps in the error correction procedure, to show that this error is indeed corrected.

8. CSS codes: Linear classical Code And Its Dual

Prove that the Fourier transform of the uniform superposition over the words in some linear code C in Z_2^n is the uniform superposition over the dual code $C^{\perp}$. The more difficult part is to show that the coefficient in front of a string not in $C^{\perp}$ vanishes. Prove this fact directly, and not as was hinted in class, by calculating the coefficient directly (hint: fix a basis for C, and present any word in C as a sum of these basis elements.)