Quantum Computing Exercises # 13

Ronald de Wolf

May 3, 2011

(to be handed in before or at the start of the lecture on May 10)

1. Here we will consider in more detail the information-disturbance tradeoff for measuring a qubit in one of the four BB84 states (each of which occurs with probability 25%).

   (a) Suppose Eve measures the qubit in the orthonormal basis given by $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ and $-\sin(\theta)|0\rangle + \cos(\theta)|1\rangle$, for some parameter $\theta \in [0, \pi]$. For each of the four possible BB84 states, give the probabilities of outcome 0 and outcome 1 (so the answer consists of 8 numbers, each of which is a function of θ).

   (b) What is the average probability that Eve's measurement outcome equals the encoded bit a_i, as function of θ? (average taken both over the uniform distribution over the four BB84 states, and over the probabilities calculated in part (a))

   (c) What is the average absolute value of the angle by which the state is changed if Eve's outcome is the encoded bit a_i? Again, the answer should be a function of θ.

2. (a) What is the Schmidt rank of the state $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$?

   (b) Suppose Alice and Bob share k EPR-pairs. What is the Schmidt rank of their joint state?

   (c) Prove that a pure state $|\phi\rangle$ is entangled if, and only if, its Schmidt rank is greater than 1.

3. Prove that Alice cannot give information to Bob by doing a unitary operation on her part of an entangled pure state. *Hint: Show that a unitary on Alice's side of the state won't change Bob's local density matrix ρ_B.*

4. Suppose Alice sends *two* n-bit messages M_1 and M_2 with the one-time pad scheme, reusing the *same* n-bit key K. Show that Eve can now get some information about M_1, M_2 from tapping the classical channel.