33-658, 758 Quantum Computation and Information Spring Semester, 2014
Assignment No. 13. Due Tuesday, April 22

READING:

MBQC = "Measurement-Based Quantum Computation" on course web page

QCQI = Nielsen and Chuang, Quantum Computation and Quantum Information

Communication complexity: H. Buhrman, R. Cleve, S. Massar, R. de Wolf, "Nonlocality and communication complexity", Rev. Mod. Phys. 82, pp. 665-698, Sec. III; specifically, subsections A, B, E, and G within section III.

Quantum cryptography: QCQI Secs. 12.6.1, 12.6.2, 12.6.3. (The discussion continues on in Secs. 12.6.4 and 12.6.5, but these are rather difficult.)

READING AHEAD:

Measurement-based quantum computation: MBQC; M. A. Nielsen, "Cluster-state quantum computation," Reports on Mathematical Physics 57 (2006) 141; arXiv:quant-ph/0504097v2; A. M. Childs, D. W. Leung and M. A. Nielsen, "Unifed deerivations of measurement-based schemes for quantum computation," Phys. Rev. A 71 (2005) 032318; arXiv:quant-ph/0404132.

Fault-tolerant quantum computation: QCQI Sec. 10.6; Preskill, Proc. R. Soc. London A **454** 385 (1998), or in *Introduction to Quantum Computation and Information*, edited by H-K Lo, S. Popescu, and T. Spiller (World Scientific, 1998), pp. 213-269. [The two items by Preskill are quite similar, though not identical.]

EXERCISES:

1. Turn in at most one page, and not less than half a page, indicating what you have read, examples or exercises (apart from those assigned below) that you worked out, difficulties you encountered, questions that came to mind, etc. You may include complaints about the course.

1b. Only for students enrolled in 33-758: Summarize in half a page to a page what you learned from the most recent seminar.

2. Consider the following variant of the hidden matching (Bar-Yossef) problem discussed in Buhrman et al., Rev. Mod. Phys. 82 (2010) 665, Sec. III.G. Let n be divisible by 3, and suppose that Alice receives a string $x \in \{0,1,2\}^n$, where $x_j = 0$, 1, or 2 indicates the color—red, white, or blue—of the j'th vertex of a graph of n vertices. The vertices are divided into sets of 3, so the graph consists of a collection of disjoint triangles, and the colors are such that for each triangle either (i) its vertices are all the same color, or (ii) no two of its vertices are of the same color (i.e., one is red, one white, and one blue). Alice is given the list of colors, but no indication of how the vertices are divided into sets of three to form triangles, while Bob is given the graph of triangles, but without the colors. The task is for Alice to send a message to Bob so that he can correctly state that for a particular triangle—he gets to choose which one—the vertices all have the same color, or else they all have different colors. (He does *not* have to specify the actual colors.)

a) Argue that it suffices for Alice to send a classical message to Bob containing the colors of the first $1+n/3$ vertices, thus a communication cost of $(1+n/3)\log 3$ bits, so that with this information Bob can accomplish the task as defined above, and even provide some additional information about the colors associated with the triangle.

b) Optional. Assume that Alice sends Bob the colors of m vertices chosen at random from a public list of random numbers (so that Bob knows to which vertex each of the colors belongs). Make an estimate of the minimum size of m so that with a probability of at least 2/3 Bob can identify a triangle which is either in category (i) or (ii).

c) Set up a deterministic quantum protocol which solves the problem by Alice making one use of a quantum channel of dimension n, thus $\log n$ qubits, to send information to Bob, using a generalization of the method discussed by Buhrman et al. for the hidden matching problem. Include enough details to show that you understand what you are doing.

3. Alice and Bob are using the BB84 protocol and Eve adopts the following eavesdropping strategy. She either (1) intercepts the qubit on its way from Alice to Bob, measures it in the Z basis, $|0\rangle$ or $|1\rangle$, and then transmits a qubit in measured state ($|0\rangle$ or $|1\rangle$) to Bob; (2) the same thing, but measuring and retransmitting using the X basis, $|+\rangle$ or $|-\rangle$; or (3) does nothing, i.e., sends the original qubit on to Bob. Suppose these three possibilities are carried out randomly with probabilities p_Z, p_X, and $1 - p_X - p_Z$. In answering the following questions, ignore all cases in which Alice transmits in one basis and Bob measures in a different basis, since those results are simply discarded.

a) Find the error rates ϵ_X and ϵ_Z which Alice and Bob will find for check bits transmitted (and received) in the X and in the Z basis, respectively, as functions of p_X and p_Z, and the overall error rate ϵ, assuming that eavesdropping is the sole source of noise in the channel. Here "error rate" is to be understood as the number of errors divided by the number of bits transmitted (and received).

b) At the end of the transmission but before efforts are carried out for information reconciliation and privacy amplification, how much information per bit does Eve possess about Alice's key? Work out separate values I_X and I_Z for bits which were transmitted in the X and Z bases, respectively, and also the value I for all of the bits, and express your answer in units of bits (of information, log to base 2) per bit (of raw key), so some number between 0 and 1.

c) For Eve's optimum strategy in the absence of collective attacks it is known that

$$I_X = \tfrac{1}{2}\phi[2\sqrt{\epsilon_Z(1-\epsilon_Z)}],$$

and the same with X and Z interchanged, where

$$\phi(x) = (1+x)\log(1+x) + (1-x)\log(1-x).$$

(See Phys. Rev. A 56 (1997) pp. 1163, 1173.) Compare your result in (b) with the optimum strategy for the cases (i) $p_X = 0.1, p_Z = 0.2$, (ii) $p_X = p_Z = 0.01$. Use numerical values with log to base 2.

4. The B92 quantum cryptography protocol is described in QCQI pp. 589 to 591. What follows is a modified version of their Exercise 12.28.

a) In order to understand how the B92 protocol works, construct a table which shows the joint probabilities of each of the eight possibilities for (a, a', b), assuming that $b = 0$ is the outcome corresponding to $|0\rangle$ or $|+\rangle$, and $b = 1$ to $|1\rangle$ or $|-\rangle$ (QCQI uses the opposite convention, but this seems to be a misprint.) Use this table to show that a and a' are perfectly correlated when $b = 1$.

b) One can use other nonorthogonal states in B92. Assume the protocol is the same, but that the angle between the points on the Bloch sphere corresponding to the two nonorthogonal states takes some value ω (ω is $\pi/2$ in the protocol as described in QCQI). Construct the same table of probabilities as in (a) for a general ω, and calculate the rate at which Alice and Bob can construct their key (bits in the key per qubits transmitted) as a function of ω. Show that it is possible to construct the key at a faster rate by using some ω which is different from $\pi/2$. What might be a disadvantage to constructing the key at a faster rate?