ANNOUNCEMENT: No classes on Monday and Wednesday, March 24 and 26 (CMU Spring Break)

RECOMMENDED READING (CQT = Griffiths, Consistent Quantum Theory; QCQI = Nielsen and Chuang, Quantum Computation and Quantum Information)

A. Entanglement. QCQI Sec. 12.5.2. Griffiths' lecture notes Sec. 12. If you are ambitious, Bennett et al. Phys. Rev. A 54, 3824-3851 (1996); Preskill's Lecture Notes, Ch. 4.

Quantum Cryptography. QCQI Sec. 12.6. Concentrate on 12.6.1 and 12.6.3, and glance at the other stuff. Griffiths lecture notes Sec. 13, if available.

B. Decoherence. CQT Ch. 26. QCQI Sec. 7.1.

Quantum Channels. QCQI Secs. 8.1, 11.3.0, 11.3.2, Ch. 12, part preceding 12.1.1.

EXERCISES:

Items marked with an asterisk * are to be turned in; the others are recommended, but should not be turned in.

*1. If you did not turn this in on March 19, please turn it in on Monday, March 31! Prepare a one-page description of your term paper. Include the title, some description of the contents, and an indication of the resources you plan to use. E.g., you have located some interesting papers, or you plan to use some of the material in Nielsen and Chuang, or you will be employing their bibliography, or you will be getting advice from Prof. X, etc. If necessary you can change the plan later, but for any significant change, please discuss it with whichever instructor has approved the topic. We will contact you promptly if it looks as if the topic is not suitable for the course, or if we see any other problems associated with it.

Problems below due on Wednesday, April 2

*2. Reading: part A. You should turn in at most 1 page indicating what you read, exercises you worked out, difficulties you encountered, questions that came to mind, etc.

*3. a) Alice and Bob share $10^4$ entangled pairs of qubits in the state

$$|\psi_1\rangle = 0.6|01\rangle + 0.8|10\rangle,$$

and they want to convert these to a smaller number $N_0$ of entangled pairs in the state $|B_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ using local operations and classical communication. Estimate the maximum possible value of $N_0$.  

b) Repeat with $|\psi_1\rangle$ replaced with

$$|\psi_2\rangle = 0.48|01\rangle + 0.60|10\rangle + 0.64i|11\rangle.$$  

[Hint: What is the reduced density operator of Alice's qubit?]

*4. The circuit

$$|a\rangle \xrightarrow{H} |\rangle$$

$$|b\rangle$$

with $|a\rangle = |0\rangle$ or $|1\rangle$ and $|b\rangle = |0\rangle$ or $|1\rangle$ results in four fully-entangled Bell states.
a) Show that there are two mutually orthogonal states \(|b_0\rangle\) and \(|b_1\rangle\) such that the circuit maps \(|a\rangle \otimes |b_j\rangle\) to a product state for any choice of \(|a\rangle\). [Hint: \(\sum_{jk} c_{jk} |j\rangle |k\rangle\) is a product state if and only if \(c_{00}c_{11} = c_{01}c_{10}\).]

b) Show that by replacing \(H\) in this circuit by a suitable single qubit gate \(U(p)\) depending on a parameter \(p\), the circuit will map the four states \(|a\rangle = |0\rangle\) or \(|1\rangle\), \(|b\rangle = |0\rangle\) or \(|1\rangle\) onto four states each of which has an entanglement given by \(h(p)\), where

\[h(p) = -p \log p - (1 - p) \log (1 - p).\]

Write \(U(p)\) as a 2 \(\times\) 2 matrix in the standard basis. (The answer is not unique; just find one that works.) [Hint: Suppose that \(|b\rangle = |0\rangle\), and that after passing through \(U(p)\) the \(a\) qubit is in the state \(a|0\rangle + \beta|1\rangle\). How entangled is the two-qubit state after the controlled-not gate has acted?]

*5. 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 \(\epsilon_X\) and \(\epsilon_Z\) 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 \(\epsilon\), assuming that eavesdropping is the sole source of noise in the channel.

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 (some number between 0 and 1).

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

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

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 in bits.)

6. First part of Exercise 12.29 in QCQI, p. 591. (The second part is a research project!)

*7. a) (Modified version of Exercise 12.28 in QCQI, p. 591.) 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 \(|-\rangle\) (Nielsen and Chuang use 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 \(\omega\) (\(\omega\) is \(\pi/2\) in the protocol as described in Nielsen and Chuang). Construct the same table of probabilities as in (a) for a general \(\omega\), and calculate the rate at which Alice and Bob can construct their key (bits in the key per qubits transmitted) as a function of \(\omega\). Show that it is possible to construct the key at a faster rate by using some \(\omega\) which is different from \(\pi/2\). What might be a disadvantage to constructing the key at a faster rate?