MASSACHUSETTS INSTITUE OF TECHNOLOGY

Media Laboratory

MAS.961 Quantum Information Science October 25, 2001

Problem Set #4

(due in class, 08-Nov-01)

Instructions: You will be graded only on the *problems* (second section, below). The *exercises* are for your own enlightenment and practice.

Lecture Topics (10/30, 11/01, 11/06): quantum information theory, distributed QC

Recommended Reading: Nielsen and Chuang, Chapters 11-12

Exercises:

E1: (**Simple calculations of entropy**) What is the entropy associated with the toss of a fair coin? With the roll of a fair die? How would the entropy behave if the coin or die were unfair?

E2: Prove that the binary entropy $H_{\rm bin}(p)$ attains its maximum value of one at $p = 1/2$.

E3: (**Example calculations of entropy**) Calculate $S(\rho)$ for

$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{1}$$

$$\rho = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \tag{2}$$

$$\rho = \frac{1}{3}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}. \tag{3}$$

E4: (**Comparison of quantum and classical entropies**) Suppose $\rho = p|0\rangle\langle 0| + (1-p)\frac{(|0\rangle+|1\rangle)(\langle 0|+\langle 1|)}{2}$. Evaluate $S(\rho)$. Compare the value of $S(\rho)$ to $H(p, 1-p)$.

E5: (**Holevo to Shannon**) Use the Holevo bound to argue that n qubits can not be used to transmit more than n bits of classical information.

E6: (**Data compression circuit**) Outline the construction of a circuit to reliably compress a qubit source with $\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ into nR qubits for any $R > S(\rho) = H(p)$.

E7: The *erasure channel* has two inputs, 0 and 1, and three outputs, $0, 1$ and e. With probability $1-p$ the input is left alone. With probability p the input is 'erased', and replaced by e.

(a) Show that the capacity of the erasure channel is $1-p$.

(b) Prove that the capacity of the erasure channel is greater than the capacity of the binary symmetric channel. Why is this result intuitively plausible?

Problems:

P1: (**Holevo's Theorem**) Suppose Alice sends Bob an equal mixture of the four pure states

$$|X_1\rangle = |0\rangle \tag{4}$$

$$|X_2\rangle = \sqrt{\frac{1}{3}}\left[|0\rangle + \sqrt{2}|1\rangle\right] \tag{5}$$

$$|X_3\rangle = \sqrt{\frac{1}{3}}\left[|0\rangle + \sqrt{2}e^{2\pi i/3}|1\rangle\right] \tag{6}$$

$$|X_4\rangle = \sqrt{\frac{1}{3}}\left[|0\rangle + \sqrt{2}e^{4\pi i/3}|1\rangle\right] . \tag{7}$$

(a) Compute the maximum mutual information between Bob's measurement and Alice's transmission; this is less than one bit.

(b) (*optional, for 5 bonus points*) A POVM which achieves ≈ 0.415 bits is known. Construct this.

(c) (*optional, for 15 bonus points*) Construct a POVM which achieves the Holevo bound.

P2: (**Teleporting a Fredkin gate**) Fault-tolerant constructions for the Toffoli and $\pi/8$ gates were shown in class. These constructions used a certain ancilla state $|\chi\rangle$, together with Bell basis measurement and single qubit Pauli operations. Using these resources alone, you can perform Toffoli and $\pi/8$ gates.

(a) What ancilla state $|\chi\rangle$ do you need in order to be able to teleport a quantum Fredkin gate, which performs the unitary transform

$$U_F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} , \tag{8}$$

that is, $|0xy\rangle \to |0xy\rangle$ and $|1xy\rangle \to |1yx\rangle$?

(b) Assume you have, in addition to the Bell basis measurements and single qubit Pauli operations, the ability to perform controlled-NOT gates. That is, you can perform any Clifford group operation. Describe the protocol that is performed to implement U_F using your $|\chi\rangle$ state.

P3: (**Entanglement and Werner states**) The Werner state with parameter p is defined as

$$W_p = p|\beta_{11}\rangle\langle\beta_{11}| + \frac{1-p}{3}\left[|\beta_{00}\rangle\langle\beta_{00}| + |\beta_{01}\rangle\langle\beta_{01}| + |\beta_{10}\rangle\langle\beta_{10}|\right] \tag{9}$$

$$= p|\Psi^-\rangle\langle\Psi^-| + \frac{1-p}{3}\left[|\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Phi^+\rangle\langle\Phi^+|\right] , \tag{10}$$

where $|\beta_{xy}\rangle = \left[|0y\rangle + (-1)^x|1\bar{y}\rangle\right]/\sqrt{2}$ are the usual Bell states.

(a) Re-express W_p as an ensemble of eight pure states,

$$|\psi_{\pm\pm\pm}\rangle = \sqrt{p_0}|\beta_{00}\rangle \pm \sqrt{p_1}|\beta_{01}\rangle \pm \sqrt{p_2}|\beta_{10}\rangle \pm \sqrt{p_3}|\beta_{11}\rangle\,, \tag{11}$$

each occuring with probability 1/8, that is

$$W_p = \frac{1}{8}\sum_k |\psi_k\rangle\langle\psi_k|\,. \tag{12}$$

Give values for p_i in terms of p.

(b) Now suppose that none of the p_i are larger than 1/2. Find ϕ_i such that an ensemble of eight pure states

$$|\psi'_{\pm\pm\pm}\rangle = \sqrt{p_0}e^{i\phi_0}|\beta_{00}\rangle \pm \sqrt{p_1}e^{i\phi_1}|\beta_{01}\rangle \pm \sqrt{p_2}e^{i\phi_2}|\beta_{10}\rangle \pm \sqrt{p_3}e^{i\phi_3}|\beta_{11}\rangle\,, \tag{13}$$

each occuring with probability 1/8 also gives W_p, and furthermore each of the $|\psi'_{\pm\pm\pm}\rangle$ are *unentangled*. Conclude that W_p can be prepared with only local operations and classical communication for $p < 1/2$.

P4: (**Twirling**) (*optional, for 10 bonus points*) Protocols for creating pure entanglement from mixed states often assume that Alice and Bob begin by sharing Werner states, or at least mixed states that are diagonal in the Bell basis. If Alice and Bob share an arbitrary joint two-qubit mixed state ρ, then how can they use classical communication and local quantum operations to project ρ onto the space of Werner states?

P5: (**Entanglement distillation by quantum error correction**) Codewords of an $[n, m]$ qubit stabilizer code can be constructed by measuring its generators $g_1, \ldots, g_{n-m}$ on an *arbitrary* n qubit quantum state, then applying Pauli operations to change the result to be a simultaneous $+1$ eigenstate of the generators. This idea can be used to perform entanglement distillation, as follows.

(a) Consider the $n = 5$ qubit perfect code, which has the stabilizer generators g_k and the normalizer operators $\bar{Z}$ and $\bar{X}$ given by

Name	Operator				
g_1	X	Z	Z	X	I
g_2	I	X	Z	Z	X
g_3	X	I	X	Z	Z
g_4	Z	X	I	X	Z
$\bar{Z}$	Z	Z	Z	Z	Z
$\bar{X}$	X	X	X	X	X

. (14)

Let us start out with n EPR pairs in the state $(|00\rangle + |11\rangle)/\sqrt{2}$, where Alice and Bob have one qubit of each pair. Show that if Alice and Bob each measure g_1 through g_4 then using the results they can perform normalizer operations which leave them with the encoded Bell pair state $(|0_L0_L\rangle + |1_L1_L\rangle)/\sqrt{2}$, where $|0_L\rangle$ and $|1_L\rangle$ are the 5-qubit code codewords.

(b) Show that if any single qubit error occurs to either Alice's or Bob's qubits, then Alice and Bob still obtain $(|0_L0_L\rangle + |1_L1_L\rangle)/\sqrt{2}$ using the same procedure.