MASSACHUSETTS INSTITUE OF TECHNOLOGY

Media Laboratory

MAS.961 Quantum Information Science November 8, 2001

Problem Set #5

(due in class, 27-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 (11/08, 11/13, 11/15, 11/20): entanglement, quantum cryptography

Recommended Reading: Nielsen and Chuang, Chapters 11-12; Preskill, Chapters 5 & 7

Exercises:

E1: (**Concavity of entropy exchange**) Show that the entropy exchange is concave in the quantum operation $\mathcal{E}$.

E2: (**Convexity of majorized set**) Show that $x \prec y$ if and only if for all real t, $\sum_{j=1}^{d} \max(x_j - t, 0) \leq \sum_{j=1}^{d} \max(y_j - t, 0)$, and $\sum_{j=1}^{d} x_j = \sum_{j=1}^{d} y_j$. Use this result to show that the set of x such that $x \prec y$ is convex.

E3: (**Entanglement conversion without communication**) Suppose Alice and Bob are trying to convert a pure state $|\psi\rangle$ into a pure state $|\phi\rangle$ using local operations only – no classical communication. Show that this is possible if and only if $\lambda_\psi \cong \lambda_\phi \otimes x$, where x is some real vector with non-negative entries summing to 1, and '$\cong$' means that the vectors on the left and the right have identical non-zero entries.

E4: (**Affine cryptosystems**) Alice holds a triplet of integers (n, m, s), and Bob $(n, m^{-1}, -m^{-1}s)$, which satisfy $\gcd(m, n) = 1$. Alice encodes by applying the transformation $x \to mx + s (\bmod\ n)$ to her original message x (an integer less than n), and Bob decodes by applying $x' \to (m^{-1}x' - m^{-1}s)(\bmod\ n)$ to the encoded message x' he receives from Alice.

(a) Give the conditions for this private key *affine cryptosystem* to be secure.

(b) Prove that there are $n\phi(n)$ distinct invertible affine encryption schemes on n letters.

E5: (**Statistics of measurement results**) Let $\{M_1, M_2, \ldots, M_n\}$ be a set of measurement observables which produce respective results X_i when an input state ρ is measured. Argue that the random variables X_i obey classical probability arguments if $[M_i, M_j] = 0$, that is, they commute with each other.

E6: (**CSS codes basis**) Show that the states $|\xi_{v_k,z,x}\rangle$ defined as

$$|\xi_{v_k,z,x}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z \cdot w} |v_k + w + x\rangle \tag{1}$$

form an orthonormal basis for a 2^n-dimensional Hilbert space, that is,

$$\sum_{v_k,z,x} |\xi_{v_k,z,x}\rangle\langle\xi_{v_k,z,x}| = I\,. \tag{2}$$

Hint: for C_1 an $[n,k_1]$ code, C_2 an $[n,k_2]$ code, and $m = k_1 - k_2$, note that there are 2^m distinct values of v_k, 2^{n-k_1} distinct x, and 2^{k_2} distinct z.

Problems:

P1: (**Properties of the Schmidt number**) Suppose $|\psi\rangle$ is a pure state of a composite system with components A and B.

(a) Prove that the Schmidt number of $|\psi\rangle$ is equal to the rank of the reduced density matrix $\rho_A \equiv \mathrm{tr}_B(|\psi\rangle\langle\psi|)$. (Note that the rank of a Hermitian operator is equal to the dimension of its support.)

(b) Suppose $|\psi\rangle = \sum_j |\alpha_j\rangle|\beta_j\rangle$ is a representation for $|\psi\rangle$, where $|\alpha_j\rangle$ and $|\beta_j\rangle$ are (un-normalized) states for systems A and B, respectively. Prove that the number of terms in such a decomposition is greater than or equal to the Schmidt number of $|\psi\rangle$, $\mathrm{Sch}(\psi)$.

(c) Suppose $|\psi\rangle = \alpha|\phi\rangle + \beta|\gamma\rangle$. Prove that

$$\mathrm{Sch}(\psi) \geq |\mathrm{Sch}(\phi) - \mathrm{Sch}(\gamma)|\,. \tag{3}$$

(d) Recall that the Schmidt number of a bi-partite pure state is the number of non-zero Schmidt components. Prove that the Schmidt number of a pure quantum state cannot be increased by local operations and classical communication. Use this result to argue that the number of Bell states shared between Alice and Bob cannot be increased by local operations and classical communication.

P2: (**Entanglement catalysis**) Suppose Alice and Bob share a pair of four level systems in the state $|\psi\rangle = \sqrt{0.4}|00\rangle + \sqrt{0.4}|11\rangle + \sqrt{0.1}|22\rangle + \sqrt{0.1}|33\rangle$. Show that it is not possible for them to convert this state by LOCC to the state $|\phi\rangle = \sqrt{0.5}|00\rangle + \sqrt{0.25}|11\rangle + \sqrt{0.25}|22\rangle$. Imagine, however, that a friendly bank is willing to offer them the loan of a *catalyst*, an entangled pair of qubits in the state $|c\rangle = \sqrt{0.6}|00\rangle + \sqrt{0.4}|11\rangle$. Show that it is possible for Alice and Bob to convert the state $|\psi\rangle|c\rangle$ to $|\phi\rangle|c\rangle$ by local operations and classical communication, returning the catalyst $|c\rangle$ to the bank after the transformation is complete.

P3: (**Entanglement and communication complexity**) Alice is in Amsterdam and Bob is in Boston, and they share an EPR pair in the state $|Q_AQ_B\rangle = |00\rangle - |11\rangle$ (suppressing normalization). Alice chooses some uniformly random bit x and independently, Bob chooses y. Define the rotation operator

$$R(\alpha) = \left(\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}\right) \tag{4}$$

If $x = 1$ Alice applies $R(\pi/8)$ to her qubit Q_A; otherwise she does nothing. If $y = 1$, Bob applies $R(-3\pi/16)$ to his qubit Q_B; otherwise he does nothing. Both Alice and Bob then measure their qubits in the computational basis, obtaining bits a and b, respectively.

(a) Show that prob$[a \oplus b = x \wedge y] = \cos^2(\pi/8) \approx 0.853$, where $\oplus$ denotes addition modulo two, and $\wedge$ is the logical AND operation. The probability distribution is taken over all values of a, b, x and y.

(b) Now suppose that Alice has a two bit number $x = x_1x_0$ and Bob has $y = y_1y_0$, and let $z = z_2z_1z_0 = x + y$ be their sum. Alice and Bob desire to obtain the middle bit of the sum, z_1, with high probability. Give a protocol using one EPR pair and only two bits of classical communication between Alice and Bob which allows them to obtain z_1 with probability better than 0.853. By "two bits of communication," we mean, both here and in the next part, that only two bits may be transmitted total: Alice and Bob can each send one bit to each other, or one party can send two bits to the other one.

(c) Show that classically, the best probability achievable with two bits of communication (and no EPR pairs) is 0.75.

P4: (**Random sampling tests**) The random test of n of $2n$ check bits allows Alice and Bob to place an upper bound on the number of errors in their untested bits, with high probability. Specifically, for any $\delta > 0$, the probability of obtaining less than δn errors on the check bits, and more than $(\delta + \epsilon)n$ errors on the remaining n bits is asymptotically less than $\exp[-O(\epsilon^2 n)]$, for large n. We prove this claim here.

(a) Without loss of generality, you may assume that there are μn errors in the $2n$ bits, where $0 \leq \mu \leq 2$. Now, if there are δn errors on the check bits, and $(\delta + \epsilon)n$ errors on the rest, then $\delta = (\mu - \epsilon)/2$. The two conditional statements in the claim thus imply the following:

$$\begin{aligned} < \delta n \text{ errors on check bits} \quad &\Rightarrow \quad < \delta n \text{ errors on check bits} && (5)\\ > (\delta + \epsilon)n \text{ errors on rest} \quad &\Rightarrow \quad > (\mu - \delta)n \text{ errors on rest}\,, && (6)\end{aligned}$$

and in fact, the top claim on the right implies the bottom one on the right. Using this, show that the probability p which we would like to bound satisfies

$$p < \binom{2n}{n}^{-1} \binom{\mu n}{\delta n} \binom{(2-\mu)n}{(1-\delta)n} \delta n\,. \tag{7}$$

(b) Show that for large n, you can bound

$$\frac{1}{an+1} 2^{anH(b/a)} \leq \binom{an}{bn} \leq 2^{anH(b/a)}\,, \tag{8}$$

where $H(\cdot)$ is the binary entropy function. Apply this to the above bound for p.

(c) Apply the bound $H(x) < 1 - 2(x - 1/2)^2$ to obtain the final result, $p < \exp[-O(\epsilon^2 n)]$. You may replace μ by a constant which expresses the worst possible case.

(d) *(optional, 5 bonus points)* Compare the result with the Chernoff bound, Box 3.4 on p. 154 in Nielsen and Chuang. Can you come up with a different way to derive an upper bound on p?

P5: (**6-state quantum key distribution**) Give a protocol using six states, the eigenstates of X, Y, and Z, and argue why it is also secure. Discuss the sensitivity of this protocol to noise and eavesdropping, in comparison with that of BB84 and B92.