Ph 219b/CS 219b

Exercises
Due: Wednesday 18 January 2006

4.1 Entanglement-assisted classical capacity of a quantum channel

The resource inequality for entanglement-assisted classical communication

$$\langle \mathcal{N}^{A\to B} : \rho^A \rangle + H(R)[qq] \geq I(R;B)[c \to c] \tag{1}$$

follows from the father protocol. As usual, the inequality expresses an asymptotically achievable communication rate. For a given input density operator ρ^A, we consider its purification ϕ^{RA}, where R is a "reference system." The noisy quantum channel $\mathcal{N}^{A\to B}$ mapping system A to system B takes ϕ^{RA} to a density operator σ^{RB}. In eq. (1), $H(A)$ is the von Neumann entropy of ρ^A, and $I(R;B)$ is the quantum mutual information of R and B in the state σ^{RB}. The inequality means that by using the channel many times, classical information can be transmitted from A to B with negligible error probability at a rate of $I(R;B)$ bits per "letter" (we say that n letters are sent when the channel is used n times), while consuming $H(R)$ ebits per letter of pre-existing entanglement shared by A and B before the protocol begins.

The supremum of achievable rates is the entanglement assisted classical capacity C_E of the quantum channel $\mathcal{N}$, which can be expressed as the "single-letter formula"

$$C_E(\mathcal{N}) \equiv \max_{\rho^A} \; I(R;B) \; . \tag{2}$$

Recall that, due to the superadditivity of coherent information, there is no known single-letter formula for the quantum capacity $Q(\mathcal{N})$, and that a proposed single-letter formula for the classical capacity $C(\mathcal{N})$ has not been rigorously established, since the conjectured additivity of the Holevo χ quantity has not been proven. In contrast, the theory of the $C_E(\mathcal{N})$ is in better shape — an upper bound on C_E that matches the lower bound expressed in eq. (1) can be proven. The purpose of this problem is to prove the matching upper bound.

In the general protocol for entanglement-assisted classical communication, Alice and Bob share an entangled pure state ϕ^{RA} at the beginning of the protocol, where Alice has system A and Bob has system R. To send message x, Alice records the message x in her register (system X), applies quantum operation $\mathcal{E}_x$ to her half of the entangled state, and then sends her half of the state through the noisy channel $\mathcal{N}^{A\to B}$. If message x is chosen with *a priori* probability $p(x)$, then after Bob receives Alice's transmission, Alice and Bob share the quantum state

$$\sigma^{XRB} = \sum_x p(x)\, (|x\rangle\langle x|)^X \otimes (I \otimes \mathcal{N})\left(\phi_x^{RA}\right) \ , \tag{3}$$

where Alice has X and Bob has RB. Here $\phi_x^{RA} = (I \otimes \mathcal{E}_x)\left(\phi^{RA}\right)$. Now Bob performs a decoding POVM $\mathcal{D}$ producing output y. Bob's information gain about Alice's message is $I(X;Y)$, where the random variable X is Alice's input message, and the random variable Y is the outcome of Bob's measurement.

a) Show that the quantum mutual information satisfies the identity

$$I(X;RB) = I(X;R) + I(XR;B) - I(R;B) \ . \tag{4}$$

b) Show that

$$I(X;Y) \le I(XR;B)_\sigma \ , \tag{5}$$

where $I(XR;B)_\sigma$ denotes the quantum mutual information evaluated in the state σ^{XRB}. **Hint**: The Holevo bound on accessible information relates $I(X;Y)$ to $I(X;RB)$. Then use eq. (4), noting that $I(X;R) = 0$ (why?) and $I(R;B) \ge 0$.

c) Show that

$$I(XR;B)_\sigma \le I(\tilde{R};B)_{\tilde{\sigma}} \ ; \tag{6}$$

here $\tilde{R}$ is a reference system such that $\phi^{\tilde{R}A}$ is a pure state of $\tilde{R}A$, $\tilde{\sigma}^{\tilde{R}B}$ is the output produced by the action of $\mathcal{N}^{A\to B}$ on $\phi^{\tilde{R}A}$, and $I_{\tilde{\sigma}}$ denotes the quantum mutual information evaluated in the state $\tilde{\sigma}^{\tilde{R}B}$. **Hint**: Recall the *monotonicity* of quantum mutual information — a quantum channel $\mathcal{E}^{A\to A'}$ cannot increase the quantum mutual information of A and B: $I(A;B)_{\text{before}} \ge I(A';B)_{\text{after}}$ (where "before" and "after" refer to the joint quantum state before and after the action of the channel). Therefore, it suffices to observe that there is a channel $\mathcal{E}^{\tilde{R}\to XR}$ that maps $\tilde{\sigma}^{\tilde{R}B}$ to σ^{XRB}.

d) Quantum conditional entropy is defined by $H(A|B) = H(AB) - H(B)$, and the quantum mutual entropy can be expressed as $I(A;B) = H(A) - H(A|B)$. Show that the strong subadditivity inequality $I(A;BC) \geq I(A;B)$ implies

$$H(A|BC) \leq H(A|B) \ , \tag{7}$$
$$H(AB|C) \leq H(A|C) + H(B|C) \ , \tag{8}$$
$$H(AB|CD) \leq H(A|C) + H(B|D) \ . \tag{9}$$

e) Parts (*b*) and (*c*) together provide an upper bound on Bob's accessible information about Alice's chosen operation. To turn this into an upper bound on C_E, we need an additivity property of the quantum mutual information. Consider two channels acting independently, $\mathcal{N}_1^{A_1\to B_1}$ and $\mathcal{N}_2^{A_2\to B_2}$. Let $\rho^{A_1A_2}$ be a joint state of the composite system A_1A_2, and let $\phi^{RA_1A_2}$ be a purification of $\rho^{A_1A_2}$, where R is a reference system. (Note that there is a single reference system R that purifies the joint state of A_1A_2.) The tensor product channel $\mathcal{N}_1 \otimes \mathcal{N}_2$ maps the pure state $\phi^{RA_1A_2}$ to the state $\sigma^{RB_1B_2}$. Show that

$$I(R;B_1B_2) \leq I(RA_2;B_1) + I(RA_1;B_2) \ . \tag{10}$$

(Note that, as far as $\mathcal{N}_1$ is concerned, RA_2 can be regarded as a reference system that purifies A_1, and as far as $\mathcal{N}_2$ is concerned, RA_1 can be regarded as a reference system that purifies A_2; therefore, eq. (10) is the natural notion of additivity for two independent channels.) **Hint**: The channels can be realized by isometries $U_1^{A_1\to B_1E_1}$ and $U_2^{A_2\to B_2E_2}$, where E_1 and E_2 are "environment" systems. Notice that if U_1 acts before U_2, then its the output state on $RA_2B_1E_1$ is pure, and that if U_2 acts before U_1, then its the output state on $RA_1B_2E_2$ is pure (why?); then use eq. (9) and subadditivity of von Neumann entropy.

f) Now, consider $\mathcal{N}^{\otimes n}$ (n independent uses of the channel $\mathcal{N}$), mapping $A^{\otimes n}$ to $B^{\otimes n}$. If the rate M is achievable, then we may consider a probability distribution on X^n that is uniform on Alice's 2^{nM} possible messages, and since Bob can decode with arbitrarily small error probability, $I(X;Y)$ is arbitrarily close to nM for n sufficiently large. Show that the upper bound

$$M \leq C_E(\mathcal{N}) \equiv \max_{\rho^A} \ I(R;B) \tag{11}$$

then follows.

4.2 Mother protocol for the GHZ state

The *mother* resource inequality

$$\langle \phi^{ABE} \rangle + \frac{1}{2} I(A;E)[q \to q] \geq \frac{1}{2} I(A;B)[qq] + \langle \phi'^{\tilde{B}E} \rangle \qquad (12)$$

expresses an asymptotic resource conversion that can be achieved if Alice, Bob, and Eve share n copies of the pure state ϕ^{ABE}, where $I(A;E)$ and $I(A;B)$ denote quantum mutual informations evaluated in the state ϕ^{ABE}. Initially Alice and Bob share the purification of Eve's state. The inequality says that, by sending $\frac{n}{2} I(A;E)$ qubits to Bob, Alice can destroy the correlations of her state with Eve's state, so that Bob alone holds the purification of Eve's state. Furthermore, at the end of the protocol, Alice and Bob share $\frac{n}{2} I(A;B)$ ebits of entanglement. The fidelity of this conversion is arbitrarily good for n sufficiently large.

Normally, the resource conversion can be realized with perfect fidelity only in the limit $n \to \infty$. But in this problem we will see that the conversion can be perfect if Alice, Bob and Eve share only $n = 2$ copies of the three-qubit GHZ state

$$|\phi\rangle^{ABE} = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle \right) . \qquad (13)$$

a) Show that in the GHZ state $|\phi\rangle^{ABE}$, $I(A;E) = I(A;B) = 1$. Thus, for this state, the mother inequality becomes

$$2\langle \phi^{ABE} \rangle + [q \to q]^{AB} \geq [qq]^{AB} + 2\langle \phi'^{\tilde{B}E} \rangle . \qquad (14)$$

b) Suppose that in the GHZ state Alice measures the Pauli operator X, gets the outcome $+1$ and broadcasts her outcome to Bob and Eve. What state do Bob and Eve then share? What if Alice gets the outcome -1 instead?

c) Suppose that Alice, Bob, and Eve share just one copy of the GHZ state ϕ^{ABE}. Find a protocol such that, after one unit of *coherent classical communication* from Alice to Bob, the shared state becomes $|\phi^+\rangle_{AB} \otimes |\phi^+\rangle_{BE}$, where $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is a maximally entangled Bell pair.

d) Now suppose that Alice, Bob, and Eve start out with two copies of the GHZ state, and suppose that Alice and Bob can borrow an ebit of entanglement, which will be repaid later, to catalyze the resource conversion. Use coherent superdense coding to construct a protocol that achieves the (catalytic) conversion eq. (14) *perfectly*.

4.3 Coherent information and entanglement fidelity

A criterion for the reversibility of the effect of a quantum channel $\mathcal{N}^{A\to B}$ on the input state ρ^A can be formulated in terms of the coherent information I_c. Let ϕ^{RA} be a purification of ρ^A, where R is a reference system; the channel maps ϕ^{RA} to the output σ^{RB}, which has purification ψ^{RBE}. Here system E can be regarded as the environment, where the channel $\mathcal{N}$ is realized as an isometry $U^{A\to BE}$. There is a decoding map $\mathcal{D}^{B\to C}$ that restores the purity of the state on RC if and only if

$$I_c(R\,\rangle B) \equiv H(B) - H(RB) = H(R)\ , \tag{15}$$

or equivalently

$$H(RE) = H(R) + H(E)\ , \tag{16}$$

where the entropy is evaluated in the output state ψ^{RBE}. That is, the effect of $\mathcal{N}^{A\to B}$ on input ρ^A is perfectly reversible if and only if the output state of the environment is uncorrelated with the reference system. That makes sense — there will be irreversible decoherence if and only if information about the input state leaks to the environment.

Naturally, we expect that if the effect of the channel is *nearly* reversible, then the criterion eq. (15) is *nearly* satisfied. The purpose of this problem is to make this observation more precise.

a) Show that

$$H(R) - I_c(R\,\rangle B) \leq 2H(RC)\ . \tag{17}$$

Therefore, if the decoder's output (the state of RC) is almost pure, then the coherent information of the channel $\mathcal{N}$ comes close to matching the input entropy. **Hint**: Use the data processing inequality

$$I_c(R\,\rangle C) \leq I_c(R\,\rangle B)\ , \tag{18}$$

and the subadditivity of von Neumann entropy. It is convenient to consider the pure joint state of the reference system, output, and environment. Do *not* assume (because it is not true) that the environment E used in the realization of the noisy channel $\mathcal{N}$ is uncorrelated with the environment E' used in the realization the decoder $\mathcal{D}$.

b) In a d-dimensional system, suppose that the state ρ has fidelity $F = 1 - \varepsilon$ with the pure state $|\psi\rangle$:

$$F = \langle\psi|\rho|\psi\rangle = 1 - \varepsilon \ . \tag{19}$$

Show that

$$H(\rho) \le H_2(\varepsilon) + \varepsilon \log_2(d-1) \ , \tag{20}$$

where $H_2(\varepsilon) = -\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log_2(1-\varepsilon)$ is the binary Shannon entropy. **Hint**: Recall that if the random variable X describes the outcome of a complete orthogonal measurement performed on the state ρ, then $H(\rho) \le H(X)$, where $H(X)$ is the Shannon entropy of X.

c) The *entanglement fidelity* F_e provides a useful way to quantity how much the quantum channel $\mathcal{N}^{A\to B}$ deviates from the identity channel. Channel input ρ^A has purification ϕ^{RA}, which is mapped by $\mathcal{N}$ to σ^{RB}. The entanglement fidelity, defined as

$$F_e(\rho^A, \mathcal{N}) \equiv \mathrm{tr}\left(\phi^{RB}\sigma^{RB}\right) \ , \tag{21}$$

does not depend on how the purification is chosen. $F_e = 1$ if the channel preserves its input, and F_e is close to 1 if the output is close to the input. Suppose that

$$F_e(\rho^A, \mathcal{D}\circ\mathcal{N}) = 1 - \varepsilon \ , \tag{22}$$

where $\mathcal{N}^{A\to B}$ is a noisy channel and $\mathcal{D}^{B\to C}$ is the decoding map. Show that

$$H(R) - I_c(R\,\rangle B) \le 2H_2(\varepsilon) + 2\varepsilon \log_2(d^2-1) \ , \tag{23}$$

where $d = \dim\, R = \dim\, C$.

d) To define the quantum capacity $Q(\mathcal{N})$ of a noisy channel $\mathcal{N}^{A\to B}$, we can use entanglement fidelity rather than fidelity as the criterion for asymptotically successful quantum communication. The rate M may be said to be achievable if, by using the channel n times, nM qubits can be transmitted from A to B such that, after decoding, the entanglement fidelity is arbitrarily close to 1 for n sufficiently large. The quantum capacity $Q(\mathcal{N})$ is the supremum of achievable rates. This definition of the capacity $Q(\mathcal{N})$ is equivalent to the definition where the fidelity rather than the entanglement fidelity is required to approach 1 as $n \to \infty$ (you are not asked to prove this equivalence). For n independent uses of the channel, let $R^{(n)}$ denote a reference system that purifies the input state on $\rho^{A^{\otimes n}}$. Show that

$$Q(\mathcal{N}) \leq \lim_{n\to\infty} \max_{\rho^{A^{\otimes n}}} \left(\frac{1}{n} I_c \left(R^{(n)} \rangle B^{\otimes n} \right) \right) \ . \tag{24}$$

Hint: Consider an input density operator to $\mathcal{N}^{\otimes n}$ that is uniform on the subspace of dimension 2^{nM} that can be transmitted reliably.

Remark: The resource inequality

$$\langle \mathcal{N}^{A\to B} : \rho^A \rangle \geq I_c(R\,\rangle B)[q \to q] \ , \tag{25}$$

descended from the father protocol, shows that the inequality eq. (24) is actually an equality. But unfortunately, because of the superadditivity of coherent information, this result does not yield a single-letter formula for the quantum capacity $Q(\mathcal{N})$.