Ph 219a/CS 219a

Exercises
Due: Wednesday 12 November 2008

2.1 Which state did Alice make?

Consider a game in which Alice prepares one of two possible states: either ρ_1 with *a priori* probability p_1, or ρ_2 with *a priori* probability $p_2 = 1 - p_1$. Bob is to perform a measurement and on the basis of the outcome to guess which state Alice prepared. If Bob's guess is right, he wins; if he guesses wrong, Alice wins.

In this exercise you will find Bob's best strategy, and determine his optimal probability of error.

Let's suppose (for now) that Bob performs a POVM with two possible outcomes, corresponding to the two nonnegative Hermitian operators E_1 and $E_2 = I - E_1$. If Bob's outcome is E_1, he guesses that Alice's state was ρ_1, and if it is E_2, he guesses ρ_2. Then the probability that Bob guesses wrong is

$$p_{\text{error}} = p_1 \text{ tr } (\rho_1 E_2) + p_2 \text{ tr } (\rho_2 E_1) \ . \tag{1}$$

a) Show that

$$p_{\text{error}} = p_1 + \sum_i \lambda_i \langle i|E_1|i\rangle \ , \tag{2}$$

where $\{|i\rangle\}$ denotes the orthonormal basis of eigenstates of the Hermitian operator $p_2\rho_2 - p_1\rho_1$, and the λ_i's are the corresponding eigenvalues.

b) Bob's best strategy is to perform the two-outcome POVM that minimizes this error probability. Find the nonnegative operator E_1 that minimizes p_{error}, and show that error probability when Bob performs this optimal two-outcome POVM is

$$(p_{\text{error}})_{\text{optimal}} = p_1 + \sum_{\text{neg}} \lambda_i \ . \tag{3}$$

where $\sum_{\text{neg}}$ denotes the sum over all of the *negative* eigenvalues.

c) It is convenient to express this optimal error probability in terms of the L^1 norm of the operator $p_2\rho_2 - p_1\rho_1$,

$$\|p_2\rho_2 - p_1\rho_1\|_1 = \text{tr } |p_2\rho_2 - p_1\rho_1| = \sum_{\text{pos}} \lambda_i - \sum_{\text{neg}} \lambda_i \ , \tag{4}$$

the difference between the sum of positive eigenvalues and the sum of negative eigenvalues. Use the property tr $(p_2\rho_2 - p_1\rho_1) = p_2 - p_1$ to show that

$$(p_{\text{error}})_{\text{optimal}} = \frac{1}{2} - \frac{1}{2}\|p_2\rho_2 - p_1\rho_1\|_1 \ . \tag{5}$$

Check whether the answer makes sense in the case where $\rho_1 = \rho_2$ and in the case where ρ_1 and ρ_2 have support on orthogonal subspaces.

d) Now suppose that Alice decides at random (with $p_1 = p_2 = 1/2$) to prepare one of two pure states $|\psi_1\rangle$, $|\psi_2\rangle$ of a single qubit, with

$$|\langle\psi_1|\psi_2\rangle| = \sin(2\alpha) \ , \quad 0 \le \alpha \le \pi/4 \ . \tag{6}$$

With a suitable choice of basis, the two states can be expressed as

$$|\psi_1\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \ , \qquad |\psi_2\rangle = \begin{pmatrix} \sin\alpha \\ \cos\alpha \end{pmatrix} \ . \tag{7}$$

Find Bob's optimal two-outcome measurement, and compute the optimal error probability.

e) Bob wonders whether he can find a better strategy if his POVM $\{E_i\}$ has more than two possible outcomes. Let $p(a|i)$ denote the probability that state a was prepared, given that the measurement outcome was i; it can be computed using the relations

$$\begin{aligned} p_i p(1|i) &= p_1 p(i|1) = p_1 \text{ tr } \rho_1 E_i \ , \\ p_i p(2|i) &= p_2 p(i|2) = p_2 \text{ tr } \rho_2 E_i \ ; \end{aligned} \tag{8}$$

here $p(i|a)$ denotes the probability that Bob finds measurement outcome i if Alice prepared the state ρ_a, and p_i denotes the probability that Bob finds measurement outcome i, averaged over Alice's choice of state. For each outcome i, Bob will make his decision according to which of the two quantities

$$p(1|i) \ , \qquad p(2|i) \tag{9}$$

is the larger; the probability that he makes a mistake is the smaller of these two quantities. This probability of error, given that Bob obtains outcome i, can be written as

$$p_{\text{error}}(i) = \min\left(p(1|i), p(2|i)\right) = \frac{1}{2} - \frac{1}{2}\left|p(2|i) - p(1|i)\right| \ . \quad (10)$$

Show that the probability of error, averaged over the measurement outcomes, is

$$p_{\text{error}} = \sum_i p_i \ p_{\text{error}}(i) = \frac{1}{2} - \frac{1}{2}\sum_i \left|\text{tr}\left(p_2\rho_2 - p_1\rho_1\right) E_i\right| \ . \quad (11)$$

f) By expanding in terms of the basis of eigenstates of $p_2\rho_2 - p_1\rho_1$, show that

$$p_{\text{error}} \geq \frac{1}{2} - \frac{1}{2}\|p_2\rho_2 - p_1\rho_1\|_1 \ . \quad (12)$$

(**Hint**: Use the completeness property $\sum_i E_i = I$.) Since we have already shown that this bound can be saturated with a two-outcome POVM, the POVM with many outcomes is no better.

2.2 Fidelity

We saw in Exercise 1.4 that the L^1 norm $\|\rho - \tilde{\rho}\|_1$ provides a useful measure of the distinguishability of the states ρ and $\tilde{\rho}$. Another useful measure of distinguishability is the *fidelity* $F(\rho, \tilde{\rho})$, which is defined as

$$F(\rho, \tilde{\rho}) \equiv \| \ \tilde{\rho}^{\frac{1}{2}}\rho^{\frac{1}{2}} \ \|_1^2 = \left(\text{tr} \ \sqrt{\rho^{\frac{1}{2}}\tilde{\rho}\rho^{\frac{1}{2}}}\ \right)^2 \ . \quad (13)$$

(Some authors use the name "fidelity" for the square root of this quantity.) The fidelity is nonnegative, vanishes if ρ and $\tilde{\rho}$ have support on mutually orthogonal subspaces, and attains its maximum value 1 if and only if the two states are identical.

a) The fidelity $F(\rho, \tilde{\rho})$ is actually symmetric in its two arguments, although the symmetry is not manifest in eq. (13). To demonstrate the symmetry, show that for any Hermitian A and B, the L^1 norm obeys

$$\|AB\|_1 = \|BA\|_1 \ . \quad (14)$$

Hint: Show that $BAAB$ and $ABBA$ have the same eigenvalues.

The *overlap* of two probability distributions $\{p_i\}$ and $\{\tilde{p}_i\}$ is defined as

$$\text{Overlap}(\{p_i\},\{\tilde{p}_i\}) \equiv \sum_i \sqrt{p_i \cdot \tilde{p}_i}\ . \tag{15}$$

Suppose that we try to distinguish the two states ρ and $\tilde{\rho}$ by performing the POVM $\{E_i\}$. Then the two corresponding probability distributions have the overlap

$$\text{Overlap}(\rho,\tilde{\rho};\{E_i\}) \equiv \sum_i \sqrt{\text{tr } \rho E_i} \cdot \sqrt{\text{tr } \tilde{\rho} E_i}\ . \tag{16}$$

It turns out that the minimal overlap that can be achieved by any POVM is

$$\text{min}_{\{E_i\}}\left[\text{Overlap}(\rho,\tilde{\rho};\{E_i\})\right] = \|\tilde{\rho}^{\frac{1}{2}}\rho^{\frac{1}{2}}\|_1 = \sqrt{F(\rho,\tilde{\rho})}\ . \tag{17}$$

In this exercise, you will show that the square root of the fidelity bounds the overlap, but not that the bound can be saturated.

b) The space of linear operators acting on a Hilbert space is itself a Hilbert space, where the inner product (A,B) of two operators A and B is

$$(A,B) \equiv \text{tr}\left(A^\dagger B\right)\ . \tag{18}$$

For this inner product, the Schwarz inequality becomes

$$|\text{tr } A^\dagger B| \le \left(\text{tr } A^\dagger A\right)^{1/2}\left(\text{tr } B^\dagger B\right)^{1/2}\ , \tag{19}$$

Choosing $A = \rho^{\frac{1}{2}} E_i^{\frac{1}{2}}$ and $B = U\tilde{\rho}^{\frac{1}{2}} E_i^{\frac{1}{2}}$ (for an arbitrary unitary U), use this form of the Schwarz inequality to show that

$$\text{Overlap}(\rho,\tilde{\rho};\{E_i\}) \ge |\text{tr } \rho^{\frac{1}{2}} U \tilde{\rho}^{\frac{1}{2}}|\ . \tag{20}$$

c) Now use the polar decomposition

$$A = V\sqrt{A^\dagger A} \tag{21}$$

(where V is unitary) to write

$$\tilde{\rho}^{\frac{1}{2}}\rho^{\frac{1}{2}} = V\sqrt{\rho^{\frac{1}{2}}\tilde{\rho}\rho^{\frac{1}{2}}}\ , \tag{22}$$

and by choosing the unitary U in eq. (20) to be $U = V^{-1}$, show that

$$\text{Overlap}(\rho,\tilde{\rho};\{E_i\}) \ge \sqrt{F(\rho,\tilde{\rho})}\ . \tag{23}$$

d) We can obtain an explicit formula for the fidelity in the case of two states of a single qubit. Using the Bloch parametrization

$$\rho(\vec{P}) = \frac{1}{2}\left(I + \vec{\sigma}\cdot\vec{P}\right) \ , \tag{24}$$

show that the fidelity of two single-qubit states with polarization vectors $\vec{P}$ and $\vec{Q}$ is

$$F(\vec{P},\vec{Q}) = \frac{1}{2}\left(1 + \vec{P}\cdot\vec{Q} + \sqrt{(1-\vec{P}^2)(1-\vec{Q}^2)}\ \right) \ . \tag{25}$$

Hint: First note that the eigenvalues of a 2×2 matrix can be expressed in terms of the trace and determinant of the matrix. Then evaluate the determinant and trace of $\left(\rho^{\frac{1}{2}}\tilde{\rho}\rho^{\frac{1}{2}}\right)$, and calculate the fidelity using the corresponding expression for the eigenvalues.

2.3 Eavesdropping and disturbance

Alice wants to send a message to Bob. Alice is equipped to prepare either one of the two states $|u\rangle$ or $|v\rangle$. These two states, in a suitable basis, can be expressed as

$$|u\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \ , \quad |v\rangle = \begin{pmatrix} \sin\alpha \\ \cos\alpha \end{pmatrix} \ , \tag{26}$$

where $0 < \alpha < \pi/4$. Suppose that Alice decides at random to send either $|u\rangle$ or $|v\rangle$ to Bob, and Bob is to make a measurement to determine what she sent. Since the two states are not orthogonal, Bob cannot distinguish the states perfectly.

a) Bob realizes that he can't expect to be able to identify Alice's qubit every time, so he settles for a procedure that is successful only some of the time. He performs a POVM with three possible outcomes: $\neg u$, $\neg v$, or DON'T KNOW. If he obtains the result $\neg u$, he is certain that $|v\rangle$ was sent, and if he obtains $\neg v$, he is certain that $|u\rangle$ was sent. If the result is DON'T KNOW, then his measurement is inconclusive. This POVM is defined by the operators

$$\begin{aligned} E_{\neg u} = A(I - |u\rangle\langle u|) \ , \quad E_{\neg v} = A(I - |v\rangle\langle v|) \ , \\ E_{\mathrm{DK}} = (1-2A)I + A\left(|u\rangle\langle u| + |v\rangle\langle v|\right) \ , \end{aligned} \tag{27}$$

where A is a positive real number. How should Bob choose A to minimize the probability of the outcome DK, and what is this minimal DK probability (assuming that Alice chooses from $\{|u\rangle, |v\rangle\}$ equiprobably)? **Hint:** If A is too large, $E_{\rm DK}$ will have negative eigenvalues, and Eq.(27) will not be a POVM.

b) Eve also wants to know what Alice is sending to Bob. Hoping that Alice and Bob won't notice, she intercepts each qubit that Alice sends, by performing an orthogonal measurement that projects onto the basis $\left\{\binom{1}{0}, \binom{0}{1}\right\}$. If she obtains the outcome $\binom{1}{0}$, she sends the state $|u\rangle$ on to Bob, and if she obtains the outcome $\binom{0}{1}$, she sends $|v\rangle$ on to Bob. Therefore each time Bob's POVM has a conclusive outcome, Eve knows with certainty what that outcome is. But Eve's tampering causes detectable errors; sometimes Bob obtains a "conclusive" outcome that actually differs from what Alice sent. What is the probability of such an error, when Bob's outcome is conclusive?

2.4 The price of quantum state encryption

Alice and Bob are working on a top secret project. I can't tell you exactly what the project is, but I will reveal that Alice and Bob are connected by a perfect quantum channel, and that Alice uses the channel to send quantum states to Bob. Alice and Bob are worried that an eavesdropper (Eve) might intercept some of Alice's transmissions. By measuring the intercepted quantum state, Eve could learn something about what Alice is sending, and perhaps make an inference about the nature of the project.

To protect against eavesdropping, Alice and Bob decide to *encrypt* the quantum states that Alice sends. They share a *secret key*, a string of random bits about which the eavesdropper knows nothing. By consuming $2n$ bits of secret key, Alice can encrypt, and Bob can decrypt, an arbitrary n-qubit state ρ. For every possible state ρ, the encrypted state looks exactly the same to Eve, so she cannot find out anything about ρ.

Here is how the encryption procedure works: We may express the $2n$ bit string x as $x = x_1 x_2 \cdots x_n$, where $x_i \in \{0,1,2,3\}$, and denote a tensor product of n Pauli operators as

$$\sigma(x) = \sigma_{x_1} \otimes \sigma_{x_2} \otimes \cdots \otimes \sigma_{x_{n-1}} \otimes \sigma_{x_n} \tag{28}$$

(where $\sigma_0 = I$). Note that $\sigma(x)^2 = I^{\otimes n}$, the identity operator acting on n qubits. To encrypt, Alice consults her random string to determine x (which is chosen uniformly at random), and applies $\sigma(x)$ to the state, obtaining $\sigma(x)\rho\sigma(x)$. To decrypt, Bob, consults the same string and applies $\sigma(x)$ to recover ρ.

a) Since Eve does not know the secret key, to her the encrypted state is indistinguishable from

$$\mathcal{E}(\rho) = \frac{1}{2^{2n}} \sum_x \sigma(x)\rho\sigma(x) \; . \tag{29}$$

Show that, for any n-qubit state ρ

$$\mathcal{E}(\rho) = \frac{1}{2^n} I^{\otimes n} \; . \tag{30}$$

Since $\mathcal{E}(\rho)$ is independent of ρ, no information about ρ is accessible to Eve.

b) Alice wonders if it is possible to encrypt the state using a shorter key. Alice and Bob could use their shared randomness to sample an arbitrary probability distribution. That is, they could agree on a set of N unitary matrices $\{U_a, a = 1, 2, 3, \ldots, N\}$, and Alice could encrypt by applying U_a with probability p_a. Then Bob could decrypt by applying U_a^{-1}. To Eve, the encrypted state would then appear to be

$$\mathcal{E}'(\rho) = \sum_a p_a U_a \rho U_a^{-1} \; . \tag{31}$$

Show that, if $\mathcal{E}'(\rho) = I^{\otimes n}$, then $p_a \leq 2^{-2n}$ for each a.

Hint: Note that $\mathcal{E}$ has an operator sum representation with Kraus operators $\{\sigma(x)/2^n\}$ and that $\mathcal{E}'$ has an operator sum representation with Kraus operators $\{\sqrt{p_a}\, U_a\}$. Furthermore $\mathcal{E} = \mathcal{E}'$. Therefore, there exists an $M \times M$ unitary matrix V_{ax} (where $M = \text{Max}(N, 2^{2n})$ such that $\sqrt{p}_a U_a = \sum_x V_{ax}\sigma(x)/2^n$. Now express $p_a \text{tr}\left(U_a U_a^\dagger\right)$ in terms of V.

Remark: The result shows that encryption requires $N \geq 2^{2n}$, and that at least $2n$ bits of key are required to specify U_a. Thus the encryption scheme in which $\sigma(x)$ is applied is the most efficient possible scheme. (For encryption to be effective, it is enough for $\mathcal{E}(\rho)$ to be independent of ρ; it is not necessary that $\mathcal{E}(\rho) = I^{\otimes n}/2^n$. But the same result applies under the weaker assumption that $\mathcal{E}(\rho)$ is independent of ρ.)

2.5 Unital maps and majorization

Recall that the action of a trace-preserving completely positive (TPCP) map $\mathcal{E}$ can be expressed as

$$\mathcal{E}(\rho) = \sum_\mu M_\mu \rho M_\mu^\dagger \ , \tag{32}$$

where

$$\sum_\mu M_\mu^\dagger M_\mu = I \ . \tag{33}$$

A TPCP map is said to be *unital* if $\mathcal{E}(I) = I$, or equivalently if

$$\sum M_\mu M_\mu^\dagger = I \ . \tag{34}$$

If A is a nonnegative Hermitian operator with unit trace (tr $A = 1$), let $\lambda(A)$ denote the vector of eigenvalues of A, which can be regarded as a probability vector. If A and B are nonnegative Hermitian operators with unit trace, we say that $A \prec B$ ("A is majorized by B") if $\lambda(A) \prec \lambda(B)$. (Recall that for two probability vectors p and q, we say that $p \prec q$ if there is a doubly stochastic matrix D such that $p = Dq$.)

Show that if ρ is a density operator and $\mathcal{E}$ is a unital map, then

$$\mathcal{E}(\rho) \prec \rho \ . \tag{35}$$

Hint: Express $\rho = U\Delta U^\dagger$ where Δ is diagonal and U is unitary, and express $\rho' \equiv \mathcal{E}(\rho) = V\Delta' V^\dagger$, where Δ' is diagonal and V is unitary. Then try to show that the diagonal entries of Δ' can be expressed as a doubly stochastic matrix acting on the diagonal entries of Δ.

Remark: A unital map is the natural quantum generalization of a doubly stochastic map (a doubly stochastic map can be regarded as the special case of a unital map that preserves the basis in which ρ is diagonal). The result of the exercise shows that a unital map takes an input density operator to an output density operator that is no less random than the input.