Ph 219a/CS 219a

Exercises
Due: Thursday 26 October 2018

1.1 How far apart are two quantum states?

Consider two quantum states described by density operators ρ and $\tilde{\rho}$ in an N-dimensional Hilbert space, and consider the complete orthogonal measurement $\{E_a, a = 1, 2, 3, \ldots N\}$, where the E_a's are one-dimensional projectors satisfying

$$\sum_{a=1}^{N} E_a = I \ . \tag{1}$$

When the measurement is performed, outcome a occurs with probability $p_a = \text{tr}\ \rho E_a$ if the state is ρ and with probability $\tilde{p}_a = \text{tr}\ \tilde{\rho} E_a$ if the state is $\tilde{\rho}$.

The L^1 *distance* between the two probability distributions is defined as

$$d(p, \tilde{p}) \equiv \|p - \tilde{p}\|_1 \equiv \frac{1}{2} \sum_{a=1}^{N} |p_a - \tilde{p}_a| \ ; \tag{2}$$

this distance is zero if the two distributions are identical, and attains its maximum value one if the two distributions have support on disjoint sets.

a) Show that

$$d(p, \tilde{p}) \leq \frac{1}{2} \sum_{i=1}^{N} |\lambda_i| \tag{3}$$

where the λ_i's are the eigenvalues of the Hermitian operator $\rho - \tilde{\rho}$. **Hint**: Working in the basis in which $\rho - \tilde{\rho}$ is diagonal, find an expression for $|p_a - \tilde{p}_a|$, and then find an upper bound on $|p_a - \tilde{p}_a|$. Finally, use the completeness property eq. (1) to bound $d(p, \tilde{p})$.

b) Find a choice for the orthogonal projector $\{E_a\}$ that saturates the upper bound eq. (3).

Define a distance $d(\rho,\tilde{\rho})$ between density operators as the maximal L^1 distance between the corresponding probability distributions that can be achieved by any orthogonal measurement. From the results of (a) and (b), we have found that

$$d(\rho,\tilde{\rho}) = \frac{1}{2}\sum_{i=1}^{N} |\lambda_i| \ . \tag{4}$$

$c)$ The L^1 *norm* $\|A\|_1$ of an operator A is defined as

$$\|A\|_1 \equiv \mathrm{tr}\left[(AA^\dagger)^{1/2}\right] \ . \tag{5}$$

How can the distance $d(\rho,\tilde{\rho})$ be expressed as the L^1 norm of an operator?

Now suppose that the states ρ and $\tilde{\rho}$ are pure states $\rho = |\psi\rangle\langle\psi|$ and $\tilde{\rho} = |\tilde{\psi}\rangle\langle\tilde{\psi}|$. If we adopt a suitable basis in the space spanned by the two vectors, and appropriate phase conventions, then these vectors can be expressed as

$$|\psi\rangle = \begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix} \ , \quad |\tilde{\psi}\rangle = \begin{pmatrix} \sin\theta/2 \\ \cos\theta/2 \end{pmatrix} \ , \tag{6}$$

where $\langle\psi|\tilde{\psi}\rangle = \sin\theta$.

$d)$ Express the distance $d(\rho,\tilde{\rho})$ in terms of the angle θ.

$e)$ Express $\|\ |\psi\rangle - |\tilde{\psi}\rangle\|^2$ (where $\|\cdot\|$ denotes the Hilbert space norm) in terms of θ, and by comparing with the result of (d), derive the bound

$$d(|\psi\rangle\langle\psi|, |\tilde{\psi}\rangle\langle\tilde{\psi}|) \leq \|\ |\psi\rangle - |\tilde{\psi}\rangle\| \ . \tag{7}$$

$f)$ Bob thinks that the norm $\|\ |\psi\rangle - |\tilde{\psi}\rangle\|$ should be a good measure of the distinguishability of the pure quantum states ρ and $\tilde{\rho}$. Explain why Bob is wrong. **Hint**: Remember that quantum states are *rays*.

1.2 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

$$p_{\text{error}} = p_1 \text{ tr } (\rho_1 E_2) + p_2 \text{ tr } (\rho_2 E_1) \ . \tag{8}$$

a) Show that

$$p_{\text{error}} = p_1 + \sum_i \lambda_i \langle i|E_1|i\rangle \ , \tag{9}$$

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

$$(p_{\text{error}})_{\text{optimal}} = p_1 + \sum_{\text{neg}} \lambda_i \ . \tag{10}$$

where $\sum_{\text{neg}}$ denotes the sum over all of the *negative* eigenvalues of $p_2\rho_2 - p_1\rho_1$.

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

$$\|p_2\rho_2 - p_1\rho_1\|_1 = \text{tr } |p_2\rho_2 - p_1\rho_1| = \sum_{\text{pos}} \lambda_i - \sum_{\text{neg}} \lambda_i \ , \tag{11}$$

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

$$(p_{\text{error}})_{\text{optimal}} = \frac{1}{2} - \frac{1}{2}\|p_2\rho_2 - p_1\rho_1\|_1 \ . \tag{12}$$

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

$$|\langle\psi_1|\psi_2\rangle| = \sin(2\alpha) \ , \quad 0 \leq \alpha \leq \pi/4 \ . \tag{13}$$

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

$$|\psi_1\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \ , \qquad |\psi_2\rangle = \begin{pmatrix} \sin\alpha \\ \cos\alpha \end{pmatrix} \ . \tag{14}$$

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

$$\begin{aligned} p_i p(1|i) &= p_1 p(i|1) = p_1 \ \mathrm{tr}\ \rho_1 E_i \ , \\ p_i p(2|i) &= p_2 p(i|2) = p_2 \ \mathrm{tr}\ \rho_2 E_i \ ; \end{aligned} \tag{15}$$

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

$$p(1|i) \ , \qquad p(2|i) \tag{16}$$

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

$$p_{\text{error}}(i) = \min\left(p(1|i), p(2|i)\right) = \frac{1}{2} - \frac{1}{2}\left|p(2|i) - p(1|i)\right| \ . \tag{17}$$

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

$$p_{\text{error}} = \sum_i p_i \ p_{\text{error}}(i) = \frac{1}{2} - \frac{1}{2}\sum_i \left|\mathrm{tr}\left(p_2\rho_2 - p_1\rho_1\right) E_i\right| \ . \tag{18}$$

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

$$p_{\text{error}} \geq \frac{1}{2} - \frac{1}{2}\|p_2\rho_2 - p_1\rho_1\|_1 \ . \tag{19}$$

(**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.

1.3 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

$$|u\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \ , \quad |v\rangle = \begin{pmatrix} \sin\alpha \\ \cos\alpha \end{pmatrix} \ , \tag{20}$$

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

$$\begin{aligned} E_{\neg u} = A(I - |u\rangle\langle u|) \ , \quad E_{\neg v} = A(I - |v\rangle\langle v|) \ , \\ E_{\text{DK}} = (1-2A)I + A\left(|u\rangle\langle u| + |v\rangle\langle v|\right) \ , \end{aligned} \tag{21}$$

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_{DK} will have negative eigenvalues, and Eq.(21) 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?

1.4 What probability distributions are consistent with a mixed state?

A density operator ρ, expressed in the orthonormal basis $\{|\alpha_i\rangle\}$ that diagonalizes it, is

$$\rho = \sum_i p_i |\alpha_i\rangle\langle\alpha_i| \ . \tag{22}$$

We would like to realize this density operator as an ensemble of pure states $\{|\varphi_\mu\rangle\}$, where $|\varphi_\mu\rangle$ is prepared with a specified probability q_μ. This preparation is possible if the $|\varphi_\mu\rangle$'s can be chosen so that

$$\rho = \sum_\mu q_\mu |\varphi_\mu\rangle\langle\varphi_\mu| \ . \tag{23}$$

We say that a probability vector q (a vector whose components are nonnegative real numbers that sum to 1) is *majorized* by a probability vector p (denoted $q \prec p$), if there exists a *doubly stochastic* matrix D such that

$$q_\mu = \sum_i D_{\mu i} \ p_i \ . \tag{24}$$

A matrix is doubly stochastic if its entries are nonnegative real numbers such that $\sum_\mu D_{\mu i} = \sum_i D_{\mu i} = 1$. That the columns sum to one assures that D maps probability vectors to probability vectors (*i.e.*, is *stochastic*). That the rows sum to one assures that D maps the uniform distribution to itself. Applied repeatedly, D takes any input distribution closer and closer to the uniform distribution (unless D is a permutation, with one nonzero entry in each row and column). Thus we can view majorization as a partial order on probability vectors such that $q \prec p$ means that q is more nearly uniform than p (or equally close to uniform, in the case where D is a permutation).

Show that normalized pure states $\{|\varphi_\mu\rangle\}$ exist such that eq. (23) is satisfied if and only if $q \prec p$, where p is the vector of eigenvalues of ρ.

Hint: Recall that, according to the *Hughston-Jozsa-Wootters Theorem*, if eq. (22) and eq. (23) are both satisfied then there is a unitary matrix $V_{\mu i}$ such that

$$\sqrt{q_\mu}\ |\varphi_\mu\rangle = \sum_i \sqrt{p_i}\ V_{\mu i}|\alpha_i\rangle\ . \tag{25}$$

You may also use (but need not prove) *Horn's Lemma*: if $q \prec p$, then there exists a unitary (in fact, orthogonal) matrix $U_{\mu i}$ such that $q = Dp$ and $D_{\mu i} = |U_{\mu i}|^2$.