Ph219a/CS219a

Solutions
Nov 8, 2013

Problem 1.1

(*a*) Since $p_a = \mathrm{Tr}(\rho E_a)$ and $\tilde{p}_a = \mathrm{Tr}(\tilde{\rho} E_a)$,

$$d(p, \tilde{p}) = \frac{1}{2} \sum_{a=1}^{N} |p_a - \tilde{p}_a| = \frac{1}{2} |\mathrm{Tr}((\rho - \tilde{\rho}) E_a)| \tag{1}$$

Writing $\rho - \tilde{\rho}$ in its eigen-basis, we have $\rho - \tilde{\rho} = \sum_i \lambda_i |i\rangle \langle i|$, so that

$$\begin{aligned} d(p, \tilde{p}) &= \sum_{a=1}^{N} |\mathrm{Tr}((\sum_i \lambda_i |i\rangle \langle i|) E_a)| \\ &= \frac{1}{2} \sum_{a=1}^{N} |\sum_i (\lambda_i \langle i| E_a |i\rangle)| \\ &\leq \frac{1}{2} \sum_i |\lambda_i| (\sum_{a=1}^{N} \langle i| E_a |i\rangle) \quad \text{(Triangle inequality!)} \\ &= \frac{1}{2} \sum_i |\lambda_i| \end{aligned} \tag{2}$$

using the fact that E_a are orthogonal projectors satisfying $\sum_a^N E_a = \mathcal{I}$.

(*b*) Construct one-dimensional projectors that project onto the basis in which $\rho - \tilde{\rho}$, ie. $E_i = |i\rangle \langle i|$. Notice that these are orthogonal projectors that sum to the identity, as desired. With this construction, the upper bound of equation (24) is saturated -

$$\begin{aligned} d(p, \tilde{p}) &= \sum_j |\sum_i (\lambda_i \langle i| E_j |i\rangle)| \\ &= \sum_j |\sum_i (\lambda_i \delta_{ij})| \\ &= \sum_j |\lambda_j| \end{aligned} \tag{3}$$

(c) Using the given definition, lets write down the L^1 norm of $\rho - \tilde{\rho}$:

$$\begin{aligned} \| \rho - \tilde{\rho} \|_1 &= \mathrm{Tr}(\sqrt{(\rho-\tilde{\rho})(\rho-\tilde{\rho})^\dagger}) \\ &= \mathrm{Tr}(\sqrt{(\rho-\tilde{\rho})^2}) \ \text{(since } \rho-\tilde{\rho} \text{ is Hermitian)} \\ &= \sum_i |\lambda_i| \\ &= 2d(p,\tilde{p}) \end{aligned} \tag{4}$$

Thus we have,

$$d(p,\tilde{p}) = \frac{1}{2} \| \rho - \tilde{\rho} \|_1 \tag{5}$$

(d) Using the given phase convention,

$$\rho - \tilde{\rho} = |\psi\rangle\langle\psi| - |\tilde{\psi}\rangle\langle\tilde{\psi}| = \begin{pmatrix} \cos\theta & 0 \\ 0 & -\cos\theta \end{pmatrix} \tag{6}$$

The eigenvalues are simply $\pm\cos\theta$ so that

$$d(p,\tilde{p}) = \frac{1}{2}(|\cos\theta| + |-\cos\theta|) = |\cos\theta| \tag{7}$$

(e) The Hilbert space norm of $(|\psi\rangle - |\tilde{\psi}\rangle)$ is given by

$$\begin{aligned} \| |\psi\rangle - |\tilde{\psi}\rangle \|^2 &= (\langle\psi| - \langle\tilde{\psi}|)(|\psi\rangle - |\tilde{\psi}\rangle) \\ &= \langle\psi|\psi\rangle - (\langle\tilde{\psi}|\psi\rangle + \langle\psi|\tilde{\psi}\rangle) + \langle\tilde{\psi}|\tilde{\psi}\rangle \\ &= 2(1-\sin\theta) \end{aligned} \tag{8}$$

Comparing this with the result of part (d),

$$\begin{aligned} (\, d(|\psi\rangle\langle\psi|, |\tilde{\psi}\rangle\langle\tilde{\psi}|)\,)^2 &= \cos^2\theta \\ &= 1 - \sin^2\theta = (1-\sin\theta)(1+\sin\theta) \\ &\leq 2(1-\sin\theta) \end{aligned} \tag{9}$$

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

(f) Consider for example, the states $|\psi\rangle$ and $|\tilde{\psi}\rangle$ for $\theta = \frac{3\pi}{2}$ so that $|\psi\rangle = -|\tilde{\psi}\rangle$. Since quantum states are really *rays*, vectors which differ only by an overall phase factor represent the same physical state. In other words, for $\theta = \frac{3\pi}{2}$, $|\psi\rangle$ and $|\tilde{\psi}\rangle$ should be indistinguishable. But computing the Hilbert space norm $\| |\psi\rangle - |\tilde{\psi}\rangle \|$, we find,

$$\| |\psi\rangle - |\tilde{\psi}\rangle \| = \| |\psi\rangle + |\psi\rangle \| = 2 \tag{10}$$

which would imply that $|\psi\rangle$ and $|\tilde{\psi}\rangle$ are maximally distinguishable! The norm $\| |\psi\rangle - |\tilde{\psi}\rangle \|$ is therefore not a good measure of distingushability.

On the other hand, distance measure d, also called the *Kolmogrov distance* between two states, gives:

$$d(|\psi\rangle\langle\psi|, |\tilde{\psi}\rangle\langle\tilde{\psi}|) = \frac{1}{2} \| |\psi\rangle\langle\psi| - |\tilde{\psi}\rangle\langle\tilde{\psi}| \|_1 = \frac{1}{2} \| |\psi\rangle\langle\psi| - |\psi\rangle\langle\psi| \|_1 = 0 \tag{11}$$

implying that the two states are indeed indistinguishable.

Problem 1.2

(a) The probability that Bob guesses wrong is

$$\begin{aligned} p_{error} &= \mathrm{Tr}[\, p_1\rho_1 E_2 + p_2\rho_2 E_1 \,] \\ &= \mathrm{Tr}[\, p_1\rho_1(\mathcal{I} - E_1) + p_2\rho_2 E_1 \,] \\ &= p_1 + \mathrm{Tr}[\, (p_2\rho_2 - p_1\rho_1)E_1 \,] \\ &= p_1 + \mathrm{Tr}\left[\sum_i (\lambda_i |i\rangle\langle i|) E_1\right] \\ &= p_1 + \sum_i \lambda_i \langle i| E_1 |i\rangle \end{aligned} \tag{12}$$

where $|i\rangle$ is the eigenstate of $(p_2\rho_2 - p_1\rho_1)$ corresponding to eigenvalue λ_i, as defined.

(b) Since E_1, E_2 are nonnegative and sum to identity ($E_1 + E_2 = \mathcal{I}$) their expectation values satisfy $0 \leq \langle i| E_1 |i\rangle \leq 1$. In order to minimize p_{error}, the coeffecient $\langle i| E_1 |i\rangle$ should be set to its minimum value(= 0) when $|i\rangle$ corresponds to a positive eigenvalue and maximum value(= 1) when $|i\rangle$ corresponds to a negative eigenvalue. In other words, Bob must choose E_1 to be the projector onto the subspace spanned by all eigenvectors of $(p_2\rho_2 - p_1\rho_1)$ corresponding to negative eigenvalues to obtain the optimal error probability

$$(p_{\text{error}})_{\text{optimal}} = p_1 + \sum_{\text{neg}} \lambda_i \tag{13}$$

(c)From the definition of the L^1 norm, we have,

$$\| p_2\rho_2 - p_1\rho_1 \|_1 = \sum_{i:\lambda_i \geq 0} \lambda_i - \sum_{i:\lambda_i < 0} \lambda_i \tag{14}$$

whereas

$$p_2 - p_1 = \mathrm{Tr}[\, p_2\rho_2 - p_1\rho_1 \,] = \sum_{i:\lambda_i \geq 0} \lambda_i + \sum_{i:\lambda_i < 0} \lambda_i \tag{15}$$

Combining equations (3) and (4), we have

$$\begin{aligned} \sum_{i:\lambda_i < 0} \lambda_i &= \frac{1}{2}(p_1 - p_2) - \frac{1}{2} \| p_2\rho_2 - p_1\rho_1 \|_1 \\ &= \frac{1}{2} - p_1 - \frac{1}{2} \| p_2\rho_2 - p_1\rho_1 \|_1 \end{aligned} \tag{16}$$

Therefore

$$(p_{\rm error})_{\rm optimal} = p_1 + \sum_{i:\lambda_i < 0} \lambda_i = \frac{1}{2} - \frac{1}{2} \parallel p_2\rho_2 - p_1\rho_1 \parallel_1 \tag{17}$$

When $\rho_1 = \rho_2$, equation(6) gives an optimal error probability of $(1 - |p_1 - p_2|)/2$. This makes sense, because when Bob is given identical states in both cases, his optimal strategy is to choose based on the *a priori* probabilities the state with the higher probability. Thus if $p_1 > p_2$, his probability of making an error is equal to the smaller probability p_2 and indeed, $(1 - |p_1 - p_2|)/2 = p_2$!

When ρ_1 and ρ_2 have support on orthogonal subspaces, then we expect that Bob should always be able to win by performing a POVM that distinguishes perfectly between the two states that Alice is sending. In terms of equation (6), this means that we can now diagonalize $(p_2\rho_2 - p_1\rho_1)$ by diagonalizing ρ_1 and ρ_2 separately so that $\parallel (p_2\rho_2 - p_1\rho_1) \parallel_1 = p_1 + p_2$. Therefore the optimal error probability is $\frac{1}{2}[1 - (p_1 + p_2)] = 0$ as expected!

(d) In this case,

$$p_2\rho_2 - p_1\rho_1 = \frac{1}{2} \begin{pmatrix} -\cos(2\alpha) & 0 \\ 0 & \cos(2\alpha) \end{pmatrix} \tag{18}$$

which has eigenvalues $\lambda_\pm = \pm\frac{1}{2}\cos(2\alpha)$. The eigenvector corresponding to the negative eigenvalue is $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ so that

$$E_1 = |0\rangle \langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{19}$$

which gives

$$(p_{\rm error})_{\rm optimal} = \frac{1}{2}(1 - \cos(2\alpha)) = \sin^2\alpha \tag{20}$$

(e) Bob's error probability is now given by

$$\begin{aligned} p_{\rm error} &= \sum_i p_i \, p_{\rm error}(i) \\ &= \sum_i p_i \left(\frac{1}{2} - \frac{1}{2} |p(2|i) - p(1|i)| \right) \\ &= \frac{1}{2} - \frac{1}{2} \sum_i |\, p_i p(2|i) - p_i p(1|i) \,| \\ &= \frac{1}{2} - \frac{1}{2} \sum_i |\, \mathrm{Tr}[\, (p_2\rho_2 - p_1\rho_1) E_i \,] \,| \end{aligned} \tag{21}$$

using the equalities $p_i p(2|i) = p_2 p(i|2) = p_2 \mathrm{Tr}[\rho_2 E_i]$ etc.

(f) Expanding $(p_2\rho_2 - p_1\rho_1)$ in its eigenbasis as $(p_2\rho_2 - p_1\rho_1) = \sum_j \lambda_j |j\rangle \langle j|$, we have,

$$\begin{aligned} p_{\text{error}} &= \frac{1}{2} - \frac{1}{2}\sum_i |\sum_j \lambda_j \langle j| E_i |j\rangle| \\ &\geq \frac{1}{2} - \frac{1}{2}\sum_i \sum_j |\lambda_j| \langle j| E_i |j\rangle \quad \text{(Triangle inequality!)} \\ &= \frac{1}{2} - \frac{1}{2}\sum_j |\lambda_j| \quad (\text{since } \sum_i E_i = \mathcal{I}) \\ &= \frac{1}{2} - \frac{1}{2} \parallel p_2\rho_2 - p_1\rho_1 \parallel_1 \end{aligned} \tag{22}$$

using the definition of the L^1 norm.

Problem 1.3

(a) Writing out the operator E_{DK} in the standard basis, we have,

$$E_{DK} = \begin{pmatrix} 1-A & A\sin(2\alpha) \\ A\sin(2\alpha) & 1-A \end{pmatrix} \tag{23}$$

which has eigenvalues $\lambda_\pm = (1-A) \pm A\sin(2\alpha)$. For E_{DK} to be positive, the smaller of the two eigenvalues must be positive, ie.

$$\lambda_- = 1 - A - A\sin(2\alpha) \geq 0 \;\; \Rightarrow A \leq \frac{1}{1+\sin(2\alpha)} \tag{24}$$

Thus the largest possible value of A that Bob can choose (so that E_{DK} is still positive) is $A = \frac{1}{1+\sin(2\alpha)}$.

The probability of outcome E_{DK} when Alice sends $|u\rangle$ and $|v\rangle$ are respectively,

$$\begin{aligned} p(E_{DK}|u) &= \langle u| E_{DK} |u\rangle = (1-2A) + A + A| < u|v > |^2 = 1 - A(1-\sin^2(2\alpha)) \\ p(E_{DK}|v) &= \langle v| E_{DK} |v\rangle = (1-2A) + A(\sin^2(2\alpha) + A = 1 - A(1-\sin^2(2\alpha)) \end{aligned} \tag{25}$$

Assuming Alice chooses between these two states equiprobably, the probability of outcome E_{DK} is $p(E_{DK}) = \frac{1}{2}(p(E_{DK}|u) + p(E_{DK}|u)) = 1 - A(1-\sin^2(2\alpha))$ which takes on the minimum value $(p(E_{DK}))_{\min} = \sin(2\alpha)$ when A takes on its maximum value $A = \frac{1}{1+\sin(2\alpha)}$.

(b) Lets denote the basis in which Eve is measuring as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. The probabilities of Eve's outcomes, conditioned on the state that Alice is sending are:

$$\begin{aligned} p(0|u) &= | < 0|u > |^2 = \cos^2\alpha \;,\; p(0|v) = | < 0|v > |^2 = \sin^2\alpha \\ p(1|u) &= | < 1|u > |^2 = \sin^2\alpha \;,\; p(1|v) = | < 1|v > |^2 = \cos^2\alpha \end{aligned} \tag{26}$$

(For example, $p(0|u)$ denotes the probability of Eve obtaining outcome $|0\rangle$ when Alice sends $|u\rangle$.)

Similarly, the probabilities of Bob's outcomes conditioned on the state he receives are:

$$\begin{aligned} p(E_{\neg v}|v) &= 0\ ,\ p(E_{\neg u}|v) = A(1 - |<u|v>|^2) = A(1-\sin^2(2\alpha)) \\ p(E_{\neg u}|u) &= 0\ ,\ p(E_{\neg v}|u) = A(1-\sin^2(2\alpha)) \end{aligned} \tag{27}$$

(We have already computed $p(E_{DK}|u)$ and $p(E_{DK}|v)$ in part(a).)
There are ways in which Bob could obtain a wrong, but conclusive outcome. Lets compute their probabilities, assuming that Alice is making her choice equiprobably -
(i) Alice sends $|u\rangle$, Eve obtains outcome $|1\rangle$ and sends $|v\rangle$ to Bob, who obtains the outcome $\neg u$. This occurs with probability

$$p(u \to 1 \to \neg u) = \frac{1}{2}p(1|u)p(E_{\neg u}|v) = \frac{1}{2}(\sin^2\alpha)(A\cos^2(2\alpha)) = \frac{A\sin^2\alpha\cos^2(2\alpha)}{2} \tag{28}$$

(ii) Alice sends $|v\rangle$, Eve obtains outcome $|0\rangle$ and sends $|u\rangle$ to Bob, who obtains the outcome $\neg v$. This occurs with probability

$$p(v \to 0 \to \neg v) = \frac{1}{2}p(0|v)p(E_{\neg v}|u) = \frac{A\sin^2\alpha\cos^2(2\alpha)}{2} \tag{29}$$

Thus the probability of Bob obtaining an error conclusively is given by,

$$p(\text{conclusive, error}) = A\sin^2\alpha\cos^2(2\alpha) = (\sin^2\alpha)(1-\sin(2\alpha)) \tag{30}$$

where we have used the largest possible value of A to minimize the probability.
This tells us what fraction of Alice's messages went wrong due to Eve's interference. Now lets look at it from the point of view of being able to detect Eve's presence. Given either $|u\rangle$ or $|v\rangle$, the probability that Bob obtains a conclusive outcome is simply

$$\begin{aligned} p(\text{conclusive}) &= 1 - p(E_{DK}) = 1 - \frac{1}{2}(p(E_{DK}|u) + p(E_{DK}|v)) \\ &= 1 - (1 - A\cos^2(2\alpha)) = 1 - \sin(2\alpha) \ \ \text{(using the max value of } A) \end{aligned} \tag{31}$$

Therefore the probability that Bob obtains an error, given that his outcome is conclusive is given by

$$\begin{aligned} p(\text{error}|\text{conclusive}) &= \frac{p(\text{conclusive, error})}{p(\text{conclusive})} \\ &= \frac{(\sin^2\alpha)(1-\sin(2\alpha))}{1-\sin(2\alpha)} = \sin^2\alpha \end{aligned} \tag{32}$$

which is also the probability of being able to detect Eve's presence.

Problem 1.4

(i) First we prove the converse -
From the GJHW theorem we know that two different realizations of a density operator ρ -

$$\begin{aligned} \rho &= \sum_i p_i \left|\alpha_i\right\rangle \left\langle\alpha_i\right| \\ &= \sum_\mu q_\mu \left|\phi_\mu\right\rangle \left\langle\phi_\mu\right| \end{aligned} \tag{33}$$

are related by

$$\sqrt{q_\mu}\,|\phi_\mu\rangle = \sum_i \sqrt{p_i} V_{\mu i}\,|\alpha_i\rangle \tag{34}$$

for some unitary V. Computing the norm on both sides of equation (10), we have

$$q_\mu = \sum_i p_i |V_{\mu i}|^2 = \sum_i p_i D_{\mu i} \tag{35}$$

The matrix D with elements $D_{\mu i} = |V_{\mu i}|^2$ is doubly stochastic (since V is unitary), thus proving that $q \prec p$.

(ii) The forward direction -
Given probability vectors q and p such that $q \prec p$, we know from Horn's lemma that there exists a unitary V such that

$$q_\mu = \sum_i p_i |V_{\mu i}|^2 \tag{36}$$

Consider the density operator ρ expressed in its diagonal form as $\rho = \sum_i p_i\,|\alpha_i\rangle\,\langle\alpha_i|$. Using the unitary V, we can construct pure states $|\phi_\mu\rangle$ as follows

$$\sqrt{q_\mu}\,|\phi_\mu\rangle = \sum_i \sqrt{p_i} V_{\mu i}\,|\alpha_i\rangle \tag{37}$$

Computing the norm on both sides, we find that the states $\{|\phi_\mu\rangle\}$ have unit norm -

$$\begin{aligned} q_\mu\,\langle\phi_\mu\rangle\,\phi_\mu &= \sum_i p_i |V_{\mu i}|^2 \\ \Rightarrow \langle\phi_\mu|\phi_\mu\rangle &= 1 \quad \text{(using equation (12))} \end{aligned} \tag{38}$$

Further,

$$\begin{aligned} \sum_\mu q_\mu\,|\phi_\mu\rangle\,\langle\phi_\mu| &= \sum_\mu \sum_{i,j} \sqrt{p_i p_j} V_{\mu i} V^*_{\mu j}\,|\alpha_i\rangle\,\langle\alpha_j| \\ &= \sum_i p_i\,|\alpha_i\rangle\,|\alpha_i\rangle \end{aligned} \tag{39}$$

since $\sum_\mu V_{\mu i} V^*_{\mu j} = \delta_{ij}$ when V is unitary. Thus we have shown that $\exists$ pure, normalized $\{|\phi_\mu\rangle\}$ such that $\rho = \sum_\mu q_\mu\,|\phi_\mu\rangle\,\langle\phi_\mu|$.