Quantum Information Basics: Patrick Hayden

Problems

1. *Partial transposition and entanglement.*

A density operator ρ^{AB} on a bipartite system $A \otimes B$ is *separable* if it can be written as a convex combination of product states: $\rho^{AB} = \sum_i p_i \, \sigma_i^A \otimes \omega_i^B$, where $\sum_i p_i = 1$, $p_i \geq 0$ and all the σ_i^A and ω_i^B are density operators. Density operators that are not separable are said to be *entangled*. In this problem, you will study one way of distinguishing entangled states from separable states. Because of the ensemble ambiguity of the density operator, it isn't obvious how to determine whether a state is entangled; if there exists a single ensemble which is a mixture of product states then the state is separable so how can we ever be sure without checking all possible ensembles?

a) Show that the transpose map $T(X) = Y$ where $Y_{ij} = X_{ji}$ is positive but not completely positive. That is, T always takes positive semidefinite operators to positive semidefinite operators, but $I \otimes T$ does not. *Hint:* Let T act on half of a maximally entangled pair of qubits.

b) Show that $(\mathrm{id} \otimes T)(\rho_{AB})$ is positive semidefinite for any separable density operator ρ_{AB}. ($\mathrm{id} \otimes T$ is called the *partial transpose* just as $\mathrm{id} \otimes \mathrm{Tr}$ is the partial trace.)

You have therefore demonstrated that the partial transpose can be used to test for the presence of entanglement. The test isn't conclusive, though. If the partial transpose of ρ is not positive semidefinite then ρ must be entangled, but sometimes states that are entangled will nonetheless have positive semidefinite partial transposes. (The test *is* conclusive for pairs of qubits, though.)

Solution:

a) To show that the partial transpose is *positive*, suppose $X \geq 0$ is a positive semi-definite operator. Then by definition, all the eigenvalues of X satisfy $\lambda_i \geq 0$, and they solve the characteristic equation

$$\det[X - \lambda_i I] = 0. \tag{1}$$

Now consider $T(X) = X^\top$. This has the characteristic equation

$$\begin{aligned} \det[X^\top - \alpha_i I] &= 0 \\ \det[X^\top - \alpha_i I^\top] &= 0 \\ \det[(X - \alpha_i I)^\top] &= 0 \\ \det[(X - \alpha_i I)] &= 0 \end{aligned} \tag{2}$$

where in the last line we've used the property of determinants that $\det[A^\top] = \det[A]$ for all matrices A.

But we already know the roots of this characteristic equation: λ_i. Therefore, (up to shuffling of indices) we have that

$$\alpha_i = \lambda_i. \tag{3}$$

In other words, $T(X)$ has the same eigenvalues as X. But all $\lambda_i \geq 0$. Therefore

$$T(X) \geq 0 \tag{4}$$

and we see that $T(X)$ is positive semidefinite. Therefore, the transpose is a positive operation.

However, the transpose is not *completely positive*. We show this using an explicit example. Consider the maximally entangled state $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

$$\rho = |\Phi\rangle\langle\Phi| = \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right). \tag{5}$$

We can rewrite this state (as we did in the discussion section) as

$$\rho = \frac{1}{2}\left(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\right). \tag{6}$$

We now act on this state with the map $\mathrm{id} \otimes T$:

$$\begin{aligned}(\mathrm{id} \otimes T)(\rho) &= \frac{1}{2}\left(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\right) \\ &= \frac{1}{2}\left(|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|\right). \end{aligned} \tag{7}$$

How can we tell if this matrix is positive semi-definite? One trick to use is to calculate the determinant. If we find that it is negative, we know that we must have at least one negative eigenvalue (an odd number, actually). Sparing the simple algebra, we find that the determinant is $-1/16$. Therefore, we know we must have negative eigenvalues, so this matrix is *not* positive semi-definite. Therefore $\mathrm{id} \otimes T$ is not completely positive.

Another (sure-fire) way to arrive at the result is to calculate the eigenvalues of the matrix. In the standard basis $(\mathrm{id} \otimes T)[\rho]$ has the matrix representation

$$(\mathrm{id} \otimes T)[\rho] \mapsto \begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 0 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{bmatrix}. \tag{8}$$

The eigenvalues of this matrix are $\{1/2, 1/2, 1/2, -1/2\}$, verifying the above results that the transpose is positive but not completely positive.

b) Suppose ρ_{AB} is separable. Any separable operator can be written as a convex combination of pure product states. In particular, we can write (WLOG)

$$\rho_{AB} = \sum_i p_i \psi_A^i \otimes \phi_B^i \tag{9}$$

for some pure states ψ_A^i and ϕ_B^i on A and B, respectively. Since $\mathrm{id} \otimes T$ is a *linear* operator, it sufices to demonstrate its action on a single product state $\psi_A \otimes \phi_B$. The result will then extend to the full state ρ_{AB} by linearity.

Consider

$$(\mathrm{id} \otimes T)[\psi_A \otimes \phi_B] = \psi_A \otimes T[\phi_B]. \tag{10}$$

Now, from part (a) we know that the transpose map is positive. Since $\phi_B \geq 0$ (because it is a density operator), $\chi_B := T[\phi_B] \geq 0$ is also a positive semi-definite operator. Therefore

$$\psi_A \otimes \chi_B \geq 0 \tag{11}$$

and we can conclude that

$$(\mathrm{id} \otimes T)[\psi_A \otimes \phi_B] \geq 0 \tag{12}$$

Taking a convex combination leaves the result positive semi-definite (since $p_i \geq 0$ for all i). Therefore $(\mathrm{id} \otimes T)[\rho_{AB}]$ is positive semi-definite when ρ_{AB} is separable. ■

2. *Bit commitment.*

Alice and Bob don't trust each other but would like to jointly execute a computation. One of the basic primitives from which they can build up the ability to perform complicated secure two-party computations is *bit commitment*. The idea is to mimic the functionality of a safe: Alice locks a bit in the safe and then transfers the safe to Bob. At some time in the future, Alice tells Bob the combination so that he can look inside the safe and determine the value of Alice's bit.

We will restrict our attention to protocols of the following form:

- **Commitment phase:** Alice selects a bit $b \in \{0, 1\}$. She then prepares a state $|\psi^{(b)}\rangle_{AB_1B_2}$ and sends the B_1 system to Bob.
- **Reveal phase:** Alice sends the B_2 system to Bob. He performs a POVM measurement $\{M_0, M_1\}$ on B_1B_2 and announces j as the value of the bit when M_j occurs.

An ideal bit commitment protocol has the following properties:

- **Hiding**: When Alice follows the protocol, the density operator $\psi_{B_1}^{(b)} = \mathrm{Tr}_{AB_2} |\psi^{(b)}\rangle\langle\psi^{(b)}|_{AB_1B_2}$ is independent of b. Bob therefore can't learn anything about b before the reveal phase.
- **Binding:** A dishonest Alice cannot change her mind after the commitment phase. In other words, it is impossible for Alice to change $|\psi^{(b)}\rangle$ into $|\psi^{(\neg b)}\rangle$ after the completion of the commitment phase.

a) Argue that if $|\varphi\rangle_{AB}$ and $|\psi\rangle_{AB}$ satisfy $\varphi_A = \psi_A$ then there exists a unitary transformation U acting on B such that $(I \otimes U)|\varphi\rangle_{AB} = |\psi\rangle_{AB}$. *Hint:* Schmidt decomposition.

b) Show that ideal bit commitment is impossible.

There is a highly cited paper from the nineties purporting to show that quantum mechanics makes it possible to implement secure bit commitment. It was wrong, as you've demonstrated. (The full argument is actually a bit more subtle because it must take into account fancier kinds of protocols including classical and bidirectional communication, but the spirit is the same.)

Solution:

For easier transition from part (a) to part (b), we interchange the roles of A and B in part (a), and we concatenate the subsystems in part (b) as AB_2B_1 rather than AB_1B_2.

a) Using a Schmidt decomposition, we can write

$$|\varphi\rangle_{AB} = \sum_j \sqrt{p_j}|e_j^A\rangle|e_j^B\rangle \tag{13}$$

where $\sum_j p_j = 1$, and $|e_j^A\rangle$ and $|e_j^B\rangle$ are sets of orthonormal vectors in A and B respectively. But rather than[1] also doing a Schmidt decomposition on the state $|\psi\rangle_{AB}$, we expand it in the basis $|e_j^B\rangle$:

$$|\psi\rangle_{AB} = \sum_j |\tilde{f}_j^A\rangle|e_j^B\rangle, \tag{14}$$

where the $|\tilde{f}_j^A\rangle$ are not necessarily orthonormal (hence the tilde).

Taking the partial trace over A for the first state, we get

$$\varphi_B = \sum_{j,k} \sqrt{p_j p_k}\,\mathrm{tr}\left(|e_j^A\rangle\langle e_k^A|\right)|e_j^B\rangle\langle e_k^B| = \sum_{j,k}\sqrt{p_j p_k}\delta_{jk}|e_j^B\rangle\langle e_k^B|. \tag{15}$$

Similarly, taking the partial trace over A for the second state,

$$\psi_B = \sum_{j,k}\mathrm{tr}\left(|\tilde{f}_j^A\rangle\langle\tilde{f}_k^A|\right)|e_j^B\rangle\langle e_k^B| = \sum_{j,k}\langle\tilde{f}_k^A|\tilde{f}_j^A\rangle|e_j^B\rangle\langle e_k^B|. \tag{16}$$

Now, we must have $\varphi_B = \psi_B$, so this implies that for all j and k,

$$\sqrt{p_j p_k}\delta_{jk} = \langle\tilde{f}_k^A|\tilde{f}_j^A\rangle \quad \Rightarrow \quad |\tilde{f}_j^A\rangle = \sqrt{p_j}|f_j^A\rangle, \tag{17}$$

where the $|f_j^A\rangle$ are proper orthonormal states in A. Hence,

$$|\psi\rangle_{AB} = \sum_j \sqrt{p_j}|f_j^A\rangle|e_j^B\rangle, \tag{18}$$

and we conclude that $(U_A \otimes \mathrm{id}_B)|\varphi\rangle_{AB} = |\psi\rangle_{AB}$, where U_A is a unitary acting only on A, taking the states $|e_j^A\rangle$ to $|f_j^A\rangle$.

b) Suppose that Alice selects $b = 0$ in the commitment phase. So she prepares the state $|\psi^{(0)}\rangle_{AB_2B_1}$, and sends the B_1 system to Bob. Since Bob cannot learn anything about b before the reveal phase, the hiding property requires $\psi_{B_1}^{(0)} = \psi_{B_1}^{(1)}$. But now, by the result of part (a), there exists a unitary U_{AB_2} on the AB_2 subsystem alone such that

$$(U_{AB_2} \otimes \mathrm{id}_{B_1})\,|\psi^{(0)}\rangle_{AB_2B_1} = |\psi^{(1)}\rangle_{AB_2B_1}\,. \tag{19}$$

Since this operation is one which Alice can perform after the commitment phase (and before the reveal phase) without the help of Bob, Alice can change the overall state to $|\psi^{(1)}\rangle_{AB_2B_1}$, allowing her to change her mind after having committed. Hence ideal bit commitment is not possible: the binding property is incompatible with the hiding property.

[1]The advantage here is that we adapt the expansion of $|\psi\rangle_{AB}$ to whatever Schmidt decomposition we use for $|\varphi\rangle_{AB}$. This is helpful because in the case where the reduced density matrix has degenerate subspaces, the excessive freedom in two simultaneous Schmidt decompositions makes the choice of unitary difficult, as we can no longer appeal to the uniqueness of the spectral decomposition to conclude that $p_j = r_j$ and $|e_j^A\rangle = |f_j^A\rangle$. See for example, the argument presented at `https://marozols.wordpress.com/tag/schmidt-decomposition/`, from which this presentation is adapted.

3. *Quantum Pinsker's inequality.*

The goal of this problem is to prove an inequality between the relative entropy and the trace distance. You'll then derive a widely used consequence, which is a bound on correlators in terms of mutual information.

a) The trace distance between two density operators ρ and σ can be expressed in terms of the outcome probabilities of the optimal measurement for distinguishing them, known as the Helstrom measurement. The POVM operators of the Helstrom measurement are orthogonal projectors Π_+ and Π_- onto the positive (technically, nonnegative) and negative eigenspaces of $\rho - \sigma$. Let $r_\pm = \operatorname{tr} \Pi_\pm \rho$ and $s_\pm = \operatorname{tr} \Pi_\pm \sigma$ be the outcome probability distributions for the two states. Show that $\|\rho - \sigma\|_1 = \|r - s\|_1$.

b) Show that for binary random variables r and s,

$$S(r\|s) \geq \frac{1}{2}\|r - s\|_1^2. \tag{20}$$

Hint: First express $S(r\|s)$ and $\|r - s\|_1^2$ in terms of r_+ and s_+. Then differentiate $S(r\|s) - \|r - s\|_1^2/2$ with respect to s_+.

c) Combine your previous results with monotonicity to finish the proof of the quantum Pinsker inequality:

$$S(\rho\|\sigma) \geq \frac{1}{2}\|\rho - \sigma\|_1^2. \tag{21}$$

d) Confirm that for a density operator ρ_{AB} of a composite system that $I(A;B) = S(\rho_{AB}\|\rho_A \otimes \rho_B)$.

e) Note that $\|X\|_1 = \max_{\|\mathcal{O}\|_\infty \leq 1} \operatorname{tr} X\mathcal{O}$, where $\|\mathcal{O}\|_\infty$ is the largest singular value of $\mathcal{O}$. (You can assume this: it is a special case of Hölder's inequality for the Schatten-ℓ_p spaces.) For operators $\mathcal{O}_A$ and $\mathcal{O}_B$ acting respectively only on A and B, show that

$$I(A;B)_\rho \geq \frac{1}{2}\left(\frac{\langle \mathcal{O}_A \otimes \mathcal{O}_B\rangle_\rho - \langle \mathcal{O}_A\rangle_\rho \langle \mathcal{O}_B\rangle_\rho}{\|\mathcal{O}_A\|_\infty \|\mathcal{O}_B\|_\infty}\right)^2. \tag{22}$$

Solution:

a) Since $\rho - \sigma$ is Hermitian, it can be written as $\rho - \sigma = P - Q$ where P and Q are positive semidefinite and have orthogonal nonnegative eigenspaces. Since $\|\rho - \sigma\|_1$ is the sum of the absolute values of the eigenvalues of $\rho - \sigma$, it is equal to $\operatorname{tr}(P + Q)$. On the other hand, we also have that

$$\begin{aligned} \|r - s\|_1 &= |\operatorname{tr} \Pi_+(P - Q)| + |\operatorname{tr} \Pi_-(P - Q)| &(23)\\ &= \operatorname{tr} P + \operatorname{tr} Q = \operatorname{tr}(P + Q), &(24)\end{aligned}$$

making use of the fact that $\operatorname{tr} \Pi_+ Q = \operatorname{tr} \Pi_- P = 0$.

b) Substitution gives

$$S(r\|s) = r_+ \ln \frac{r_+}{s_+} + (1-r_+) \ln \frac{1-r_+}{1-s_+} \quad \text{and} \tag{25}$$

$$\|r-s\|_1 = 2|r_+ - s_+|, \tag{26}$$

so $\|r-s\|_1^2 = 4(r_+ - s_+)^2$. We then consider

$$f(r_+, s_+) = S(r\|s) - \frac{1}{2}\|r-s\|_1^2 \tag{27}$$

$$= r_+ \ln \frac{r_+}{s_+} + (1-r_+) \ln \frac{1-r_+}{1-s_+} - 2(r_+ - s_+)^2. \tag{28}$$

Then

$$\frac{\partial f}{\partial s_+} = (s_+ - r_+) \left(\frac{1}{s_+(1-s_+)} - 4 \right) \tag{29}$$

so the sign of the derivative is just the sign of $s_+ - r_+$. Since $f = 0$ when $r_+ = s_+$, this implies that $f \geq 0$.

c) Starting with the monotonicity of the relative entropy with respect to the channel implementing the Helstrom measurement and then applying (b) and (a) in turn gives:

$$S(\rho\|\sigma) \geq S(r\|s) \geq \frac{1}{2}\|r-s\|_1^2 = \|\rho-\sigma\|_1^2. \tag{30}$$

d)

$$S(\rho_{AB}\|\rho_A \otimes \rho_B) = \operatorname{tr} \rho_{AB} \log \rho_{AB} - \operatorname{tr} \rho_{AB} \log \rho_A \otimes \rho_B \tag{31}$$

$$= -S(AB)_\rho - \operatorname{tr} \rho_{AB} [(\log \rho_A) \otimes I_B + I_B \otimes (\log \rho_B)] \tag{32}$$

$$= -S(AB) - \operatorname{tr} \rho_A \log \rho_A - \operatorname{tr} \rho_B \log \rho_B \tag{33}$$

$$= I(A;B)_\rho. \tag{34}$$

The only tricky part is to properly evaluate the logarithm of the tensor product operator $\rho_A \otimes \rho_B$. If you're puzzled, try exponentiating $(\log \rho_A) \otimes I_B + I_B \otimes (\log \rho_B)$ and confirm that you get $\rho_A \otimes \rho_B$. Note also that the third line uses the definition of the partial trace to replace ρ_{AB} and ρ_A and ρ_B in the last two terms.

e) In order to use the given inequality, introduce operators $\tilde{\mathcal{O}}_A = \mathcal{O}_A / \|\mathcal{O}_A\|_\infty$ and $\tilde{\mathcal{O}}_B = \mathcal{O}_B / \|\mathcal{O}_B\|_\infty$. Then

$$I(A;B) = S(\rho_{AB}\|\rho_A \otimes \rho_B) \tag{35}$$

$$\geq \frac{1}{2}\|\rho_{AB} - \rho_A \otimes \rho_B\|_1^2 \tag{36}$$

$$\geq \frac{1}{2} \left(\operatorname{tr}(\tilde{\mathcal{O}}_A \otimes \tilde{\mathcal{O}}_B)\rho_{AB} - \operatorname{tr}(\tilde{\mathcal{O}}_A \otimes \tilde{\mathcal{O}}_B)(\rho_A \otimes \rho_B) \right)^2 \tag{37}$$

$$= \frac{1}{2} \left(\langle \tilde{\mathcal{O}}_A \otimes \tilde{\mathcal{O}}_B \rangle_\rho - \langle \tilde{\mathcal{O}}_A \rangle_\rho \langle \tilde{\mathcal{O}}_B \rangle_\rho \right)^2 \tag{38}$$

$$= \frac{1}{2} \left(\frac{\langle \mathcal{O}_A \otimes \mathcal{O}_B \rangle_\rho - \langle \mathcal{O}_A \rangle_\rho \langle \mathcal{O}_B \rangle_\rho}{\|\mathcal{O}_A\|_\infty \|\mathcal{O}_B\|_\infty} \right)^2. \tag{39}$$

4. *A useful POVM.*

Let $|\varphi\rangle$ and $|\psi\rangle$ be states in $\mathbb{C}^2$ such that $\langle\varphi|\psi\rangle = \alpha$. Choose states $|\varphi^\perp\rangle, |\psi^\perp\rangle \in \mathbb{C}^2$ such that $\langle\varphi|\varphi^\perp\rangle = \langle\psi|\psi^\perp\rangle = 0$. For $\lambda \in \mathbb{R}$, consider the triple of operators

$$E_1 = \lambda|\varphi^\perp\rangle\langle\varphi^\perp|, \quad E_2 = \lambda|\psi^\perp\rangle\langle\psi^\perp|, \quad E_3 = I - E_1 - E_2. \tag{40}$$

a) For which values of λ does $\{E_1, E_2, E_3\}$ form a POVM?

b) Consider the POVM with the largest such λ. If this POVM is applied to an unknown state which is either $|\varphi\rangle$ or $|\psi\rangle$, outcome E_1 implies the state must have been $|\psi\rangle$ while outcome E_2 implies the state must have been $|\varphi\rangle$. Explain why this does *not* provide a counterexample to the impossibility of perfectly distinguishing nonorthogonal states.

c) Suppose you are given a quantum state chosen from a set $\{|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_m\rangle\}$ of linearly independent states. Construct a POVM $\{E_1, E_2, \ldots, E_{m+1}\}$ such that if outcome E_j occurs for $1 \leq j \leq m$, then you can conclude with certainty that you were given state $|\varphi_j\rangle$. Your POVM must be such that $\langle\varphi_j|E_j|\varphi_j\rangle > 0$ for $1 \leq j \leq m$.

Solution:

a) Clearly $\sum_i E_i = I$, so we just need to check that $0 \leq E_i \leq I$. $0 \leq E_1, E_2 \leq I$ if and only if $0 \leq \lambda \leq 1$. E_3 requires a bit more work. We can assume without loss of generality that $|\varphi\rangle = |0\rangle$, $|\varphi^\perp\rangle = |1\rangle$ and $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\psi^\perp\rangle = \bar{\beta}|0\rangle - \bar{\alpha}|1\rangle$. Then we have

$$E_3 = \begin{pmatrix} 1 - \lambda|\beta|^2 & \lambda\alpha\bar{\beta} \\ \lambda\bar{\alpha}\beta & 1 - \lambda|\alpha|^2 - \lambda \end{pmatrix}. \tag{41}$$

This is a two by two Hermitian matrix with positive trace, so its eigenvalues are either both nonnegative or one is positive and one is negative. This second case can occur only if the determinant is negative. Therefore, it is sufficient to check that

$$0 \leq \det E_3 = 1 - 2\lambda + \lambda^2(1 - |\alpha|^2). \tag{42}$$

By solving the quadratic, this reduces to $\lambda \leq 1/(1 + |\alpha|)$.

b) The POVM doesn't distinguish between $|\varphi\rangle$ and $|\psi\rangle$ all of the time. Outcome 3 has non-zero probability for both $|\varphi\rangle$ and $|\psi\rangle$.

c) For $1 \leq j \leq m$, let V_j be the orthogonal complement to the span of the set $\{|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_m\rangle\}\backslash\{|\varphi_j\rangle\}$ and Π_j the projector onto V_j. Because the states are linearly independent, $\mathrm{Tr}(\Pi_j\varphi_j) > 0$. Also, by construction, $\mathrm{Tr}(\Pi_j\varphi_k) = 0$ if $j \neq k$. Our POVM elements will be $E_j = \frac{1}{m}\Pi_j$ for $1 \leq j \leq m$ and $E_{m+1} = I - \sum_{j=1}^m E_j$. Notice that for any state $|\psi\rangle$,

$$\langle\psi|E_{m+1}|\psi\rangle = 1 - \sum_{j=1}^m \langle\psi|\frac{1}{m}\Pi_j|\psi\rangle = 1 - \frac{1}{m}\sum_{j=1}^m \langle\psi|\Pi_j|\psi\rangle \geq 1 - \frac{1}{m} \cdot m \cdot 1 = 0. \tag{43}$$

Thus, $E_{m+1} \geq 0$ and all other required conditions have been verified or are clear.