Assignment 2 - due April 17th

- This assignment corresponds to the material in Lectures 4 to 7.
- Lecture 4 was about composing systems. We discussed reduced states, partial trace, and two applications: superdense coding and quantum teleportation. It corresponding to sections 2.3 and 2.4 of Nielsen's, or 3.5 and 3.6 of Wilde's.
- Lecture 5 is about Schmidt's decomposition and purification. It corresponds roughly to Section 2.5 of Nielsen's or 3.8 of Wilde's. It also introduced the problem of distinguishing states, corresponding basically to Section 2.2.4 of Nielsen's.
- Lecture 6 introduces POVMs. You will find it in 2.2.6 of Nielsen's, or more generally Chapter 4 of Barnett's.
- Lecture 7 is about fidelity and quantum channels. Chapter 9 of Nielsen's, but more nicely the end of Chapter 2 and beginning of Chapter 3 of Preskill's.

Exercise 1. @

Consider the superdense coding protocol, in which Alice sends Bob a qubit with the intent of transmitting two qubits of information. Suppose a third party Eve intercepts Alice's qubit. Can she infer anything about which of the four possible bit strings Alice is trying to send? If so, how? If not, why not?

Solution:

No. The reduced state at Alice's qubit is $(1/2)I$, obtained from taking the partial of any of the four possible joint states she could have produced.

Exercise 2. @

Show an example of a state in a three party system for which a Schmidt decomposition is not available.

Solution:

Consider $|\phi\rangle$ a state in a three party system. If there were bases $|a_i\rangle$, $|b_i\rangle$ and $|c_i\rangle$ with $i \in \{1, 2\}$ so that

$$|\phi\rangle = \sum_{k=1}^{2} \lambda_i |a_i\rangle|b_i\rangle|c_i\rangle,$$

it would follow that all three reduced states at each system would have the same eigenvalues, namely, λ_1^2 and λ_2^2. So the idea now is to propose $|\phi\rangle = |a\rangle \otimes |\psi\rangle$, where $|a\rangle$ is an unentangled state in the first system, and $|\psi\rangle$ is an entangled state in the second and third systems. The reduced density matrix in the first system has eigenvalues 1 and 0, whereas in either the second or the third both eigenvalues will be positive.

Exercise 3. @

Let ρ be a mixed state, which can be realized in the following two ways:

$$\rho = \sum_i p_i |a_i\rangle\langle a_i| = \sum_i q_i |b_i\rangle\langle b_i|.$$

Find one purification for ρ which allows for either way to be obtained depending only on the observable that is used. Derive an expression for each observable.

Solution:

Consider

$$|\psi_1\rangle = \sum_i \sqrt{p_i}|a_i\rangle|i\rangle \quad \text{and} \quad |\psi_2\rangle = \sum_i \sqrt{q_i}|b_i\rangle|i\rangle.$$

Both these vectors admit Schmidt decomposition, and from the way we proved its existence, it follows that if $\rho = \sum_i \lambda_i|\lambda_i\rangle\langle\lambda_i|$ is a diagonalization of ρ, we can write

$$|\psi_1\rangle = \sum_i \sqrt{\lambda_i}|\lambda_i\rangle|x_i\rangle \quad \text{and} \quad |\psi_2\rangle = \sum_i \sqrt{\lambda_i}|\lambda_i\rangle|y_i\rangle,$$

where both $\{|x_i\rangle\}$ and $\{|y_i\rangle\}$ are orthonormal bases. There is, therefore, a unitary U so that $U|x_i\rangle = |y_i\rangle$, hence

$$(I \otimes U)|\psi_1\rangle = |\psi_2\rangle,$$

thus measuring $|\psi_1\rangle$ according to $\{|i\rangle\}$ or to $\{U|i\rangle\}$ will yield both ways of writing ρ.

Exercise 4. @

Assume $\{M_1, ..., M_m\}$ is a POVM, and ρ is a density matrix. Let $\{|i\rangle\}_{i=1}^m$ be a basis of an m dimensional system. Prove that

$$\rho' = \sum_{i=1}^m M_i \rho M_i^* \otimes |i\rangle\langle i|.$$

is a density matrix.

Solution:

Note that

$$\begin{aligned}
\operatorname{tr}\rho' &= \sum_{i=1}^m \operatorname{tr}(M_i\rho M_i^*)\operatorname{tr}(|i\rangle\langle i|) \\
&= \sum_{i=1}^m \operatorname{tr}(M_i^* M_i \rho) \\
&= \operatorname{tr}\sum_{i=1}^m (M_i^* M_i)\rho \\
&= \operatorname{tr}\rho = 1
\end{aligned}$$

Also, each $M_i\rho M_i^*$ is Hermitian and, for all $|v\rangle$,

$$\langle v|M_i\rho M_i^*|v\rangle = \langle M_i^* v|\rho|M_i^* v\rangle \geq 0$$

because $\rho \succeq 0$. So $M_i \rho M_i^* \succeq 0$. By taking products of eigenvalues it follows immediately that $M_i \rho M_i^* \otimes |i\rangle\langle i| \succeq 0$, and as the sum of positive semidefinite matrices is positive semidefinite, we obtain $\rho' \succeq 0$.

Exercise 5.

Let $|a\rangle$ and $|b\rangle$ be states, and $|a^\perp\rangle$ and $|b^\perp\rangle$ be perpendicular states to each respectively. Let

$$M_a = \frac{1}{1+|\langle a|b\rangle|}|a^\perp\rangle\langle a^\perp| \quad \text{and} \quad M_b = \frac{1}{1+|\langle a|b\rangle|}|b^\perp\rangle\langle b^\perp|.$$

Show that $I - M_a - M_b$ is positive semidefinite.

Solution:

As $\{|a\rangle, |a^\perp\rangle\}$ and $\{|b\rangle, |b^\perp\rangle\}$ are both orthonormal bases, there is a unitary that takes $|a\rangle$ to $|b\rangle$ and $|a^\perp\rangle$ to $|b^\perp\rangle$, thus $\langle a|b\rangle = \langle a^\perp|b^\perp\rangle$. If this is $= 0$, the result is straightforward. Assume it is > 0, for the other case is analogous.

The result now follows from noticing that $|a^\perp\rangle + |b^\perp\rangle$ is an eigenvector of $I - M_a - M_b$ with eigenvalue 0, and $|a^\perp\rangle - |b^\perp\rangle$ is an eigenvector of $I - M_a - M_b$ with eigenvalue

$$\frac{2\langle a|b\rangle}{1+\langle a|b\rangle} > 0.$$

Exercise 6.
Alice and Bob are each given one of the qubits of some 2-qubit state. Working as a team, they are required to distinguish between State I and State II with only local projective measurements. That means, they can each measure their own qubit according to some observable. After their measurements, they can send only classical bits to each other.

In each case below, either give a perfect distinguishing procedure or explain why there is no perfect distinguishing procedure.

(a)

$$\text{State 1: } \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{and} \quad \text{State 2: } \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

(b)

$$\text{State 1: } \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{and} \quad \text{State 2: } \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

(c)

$$\text{State 1: } \frac{1}{\sqrt{2}}(|00\rangle + \mathrm{i}|11\rangle) \quad \text{and} \quad \text{State 2: } \frac{1}{\sqrt{2}}(|00\rangle - \mathrm{i}|11\rangle)$$

Solution:

For (a), Alice and Bob measure according to $|0\rangle$ and $|1\rangle$. They communicate. The possible four strings 00, 01, 10 and 11 unequivocally determine the states: 00 and 11 are state 1, 10 and 01 are for state 2.

For (b), note that State 1 is equal to $(1/\sqrt{2})(|+\rangle|+\rangle + |-\rangle|-\rangle)$ and State 2 is equal to $(1/\sqrt{2})(|+\rangle|-\rangle + |-\rangle|+\rangle)$, so an analogous strategy as in (a) works.

For (c), use states $(1/\sqrt{2})(1\ ,\ \pm e^{i\pi/4})$ wisely.

Exercise 7.

Recall that in the teleportation protocol, Alice and Bob have a joint state of the form

$$(\alpha|0\rangle_A + \beta|1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}),$$

where subscripts are indicating who possesses each qubit. At the end of the protocol, Bob's qubit is at state $(\alpha|0\rangle_B + \beta|1\rangle_B)$.

Suppose that Alice's qubit which is going to be teleported is actually entangled with Charlie's, in state

$$\frac{1}{\sqrt{2}}(|00\rangle_{CA} + |11\rangle_{CA}).$$

Assume now Alice and Bob execute the teleportation protocol regardless. At the end, will the joint state of Charlie's and Bob's qubits be

$$\frac{1}{\sqrt{2}}(|00\rangle_{CB} + |11\rangle_{CB})?$$

Justify your answer.

Solution:

Recall that $|\Phi_+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ and $|\Psi_+\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle)$.

So we apply $I \otimes \texttt{CNOT} \otimes I$ to $|\Phi_+\rangle \otimes |\Phi_+\rangle$, obtaining 1/2 times the 1st, 4th, 13th and 16th columns of the matrix, that is:

$$\frac{1}{\sqrt{2}}(|00\rangle \otimes |\Phi_+\rangle + |11\rangle \otimes |\Psi_+\rangle).$$

Now she performs a measurement according to projectors $I \otimes E_i \otimes F_j \otimes I$, where $X = E_1 - E_2$

and $Z = F_1 - F_2$, obtaining the following four options with equal probability:

$$\begin{aligned}
+1,+1 \quad &: \quad \frac{1}{\sqrt{2}}\Big(|0+\rangle \otimes |00\rangle \; + \; |1+\rangle \otimes |01\rangle\Big). \\
+1,-1 \quad &: \quad \frac{1}{\sqrt{2}}\Big(|0+\rangle \otimes |11\rangle \; + \; |1+\rangle \otimes |10\rangle\Big). \\
-1,+1 \quad &: \quad \frac{1}{\sqrt{2}}\Big(|0-\rangle \otimes |00\rangle \; - \; |1-\rangle \otimes |01\rangle\Big). \\
-1,-1 \quad &: \quad \frac{1}{\sqrt{2}}\Big(|0-\rangle \otimes |11\rangle \; - \; |1-\rangle \otimes |10\rangle\Big).
\end{aligned}$$

Finally, Bob applies I, X, Z, or ZX in his qubit, obtaining, respectively:

$$\begin{aligned}
+1,+1 \quad &: \quad \frac{1}{\sqrt{2}}\Big(|0+\rangle \otimes |00\rangle \; + \; |1+\rangle \otimes |01\rangle\Big). \\
+1,-1 \quad &: \quad \frac{1}{\sqrt{2}}\Big(|0+\rangle \otimes |10\rangle \; + \; |1+\rangle \otimes |11\rangle\Big). \\
-1,+1 \quad &: \quad \frac{1}{\sqrt{2}}\Big(|0-\rangle \otimes |00\rangle \; + \; |1-\rangle \otimes |01\rangle\Big). \\
-1,-1 \quad &: \quad \frac{1}{\sqrt{2}}\Big(|0-\rangle \otimes |10\rangle \; + \; |1-\rangle \otimes |11\rangle\Big).
\end{aligned}$$

which is, fortunately, exactly what we wanted: all states are in $|\Phi_+\rangle$ in the first and last qubits, and respectively $|+\rangle|0\rangle$, $|+\rangle|1\rangle$, $|-\rangle|0\rangle$ and $|-\rangle|1\rangle$ in the second and third.

Exercise 8.

Alice wishes to commit a bit to Bob, and later he is supposed to unveil the value of the bit. This procedure is called binding if Alice is unable to change the value of her bit after commitment, and is called concealing if Bob is unable to check the value of the bit until the unveiling moment. The protocol is called secure if it is both binding and concealing.

Classically, one way to attempt this is for Alice to send her bit in a safe, and only at the unveiling phase she reveals the safe's secret. The process is concealing so as long as Bob is not a good safe cracker.

Quantumly, here is a proposition. Alice prepares one of two distinguishable density operators ρ_0 and ρ_1 in a bipartite system AB, sends system B to Bob, and keeps A to herself. Later, to unveil, she sends A to Bob, and he performs a measurement to determine whether it is ρ_0 or ρ_1.

Show that if a quantum bit commitment protocol is concealing, then it is not binding. Thus quantum bit commitment is insecure.

(you may assume that both states to be used are pure, but it would be nice to argue why this is possible as well)

Solution:

Assuming the procedure is concealing means that the reduced states ρ_{0B} and ρ_{1B} are equal (if they were different, Bob could devise a measurement that with some probability $> 1/2$ would correctly distinguish them). We can view ρ_0 and ρ_1 as different purifications (and the system Alice kept is the auxiliary system used to purify them), but according to Exercise 3, there is a unitary acting only on Alice's system that maps ρ_0 to ρ_1. So the procedure is absolutely not binding.