Assignment 2 - due April 13th

Answer 1. We will show that Eve can't infer about the bits ALice is trying to send to Bob. First, let's remember that Alice and Bob have a pair in one of the four possible Bell's states. Alice then performs one of four operations in her qubit: I, X, Y or Z. Applying one of these operators changes her qubit to other Bell state. Let's show that if Eve gets Alice's qubit, she can't know which of the operations she applied. All Bell states can be written as:

$$|Bell\rangle = \frac{|0\rangle \otimes |u\rangle + |1\rangle \otimes |v\rangle}{\sqrt{2}}$$

where $\{|u\rangle, |v\rangle\}$ are orthogonal states. So for any Bell state, the following holds:

$$|u\rangle\langle v| = 0, |u\rangle\langle u| = |v\rangle\langle v| = 1$$

Then, we calculate the partial trace of Alice's qubit, we have

$$\sum_j |\langle j|u\rangle|^2 = \langle u|u\rangle = 1$$

$$\sum_j |\langle j|v\rangle|^2 = \langle v|v\rangle = 1$$

and then

$$\rho_A = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2}$$

That's true for all Bell states. So, Eve can't know which operation Alice did, without Bob's qubit.

Answer 2. blank

Answer 3. A purification of ρ is a pure state $|\psi\rangle_{AB}$ in the joint system $A \otimes B$ such that:

$$\rho_A = Tr_B(|\psi\rangle\langle\psi|_{AB})$$

We have two different compositions for ρ, so we will write two different schmidt decompositions to match each eigenbasis $|a_i\rangle$ or $|b_i\rangle$. To match $\{|a_i\rangle\}$:

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}|a_i\rangle_A \otimes |v_i\rangle_B$$

where $\{|v_i\rangle_B\}$ is an arbitrary orthonormal basis for B. To match $\{|b_j\rangle\}$:

$$|\psi\rangle_{AB} = \sum_j \sqrt{q_j}|b_j\rangle_A \otimes |w_j\rangle_B$$

where $\{|w_j\rangle_B\}$ is an arbitrary orthonormal basis for B. We can now unify both decompositions expressing $\{|b_j\rangle\}$ in terms of $\{|a_i\rangle\}$:

$$|b_j\rangle = \sum_i c_{ji}|a_i\rangle, \quad where \quad c_{ji} = \langle a_i|b_j\rangle$$

Now we can have two observables for each decomposition.

$$H_1 = \sum_i \lambda_i |v_i\rangle\langle v_i|$$

and

$$H_2 = \sum_j \mu_j |w_j\rangle\langle w_j|$$

H_1 recovers the $\{|a_i\rangle\}$ decomposition and H_2 recovers the $\{|b_j\rangle\}$.

Answer 4. To show that ρ' is a density matrix, we need to show that is hermitian, the trace is unitary and is positive semidefinite. Hermitian($(\rho')^* = \rho'$): For each term

$$(M_i \rho M_i^*)^* = (M_i^*)^* \rho^* M_i^* = M_i \rho M_i^*$$

All $|i\rangle\langle i|$ is also hermitian. We know the sum of hermitians is also hermitian, so ρ' is hermitian. Unitary trace:

$$Tr(\rho') = \sum_{i=1}^{m} Tr(M_i \rho M_i^*) \cdot Tr(|i\rangle\langle i|)$$

We know that $|i\rangle$ is normalized, so $Tr(|i\rangle\langle i|) = 1$. Also by the properties of the trace, we have:

$$Tr(M_i \rho M_i^*) = Tr(M_i^* M_i \rho)$$

Then:

$$Tr(\rho') = \sum_{i=1}^{m} Tr(M_i^* M_i \rho)$$

because $\{M_i\}$ is a POVM, we have

$$\sum_{i=1}^{m} M_i^* M_i = I$$

Thus:

$$Tr(\rho') = Tr\left(\left(\sum_{i=1}^{m} M_i^* M_i\right)\rho\right) = Tr(I\rho) = Tr(\rho) = 1$$

Positive Semidefiniteness: we need to show that $\rho' \geq 0$, for any state $|\psi\rangle$

$$\langle\psi|\rho'|\psi\rangle \geq 0$$

Expressing $|\psi\rangle$ in the basis $\{|i\rangle\}$:

$$|\psi\rangle = \sum_{j=1}^{m} |\psi_j\rangle \otimes |j\rangle$$

So

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

Because the orthogonality of the basis we have

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

Since $\rho \geq 0$ and $M_i \rho M_i^*$ is a positive operator, because ρ is positive and $M_i \rho M_i^*$ is a conjugation of ρ, we have that each term $\langle\psi|M_i \rho M_i^*|\psi\rangle \geq 0$. Thus ρ' is positive semidefinite.

Answer 5. Firts, lets see what happens with $M_A + M_B$:

$$M_A + M_B = \frac{1}{1 + |\langle a|b\rangle|}(|a^\perp\rangle\langle a^\perp| + |b^\perp\rangle\langle b^\perp|)$$

Let's call $c = |\langle a|b\rangle|$ and $D = |a^\perp\rangle\langle a^\perp| + |b^\perp\rangle\langle b^\perp|$. Observe that

$$D = \begin{pmatrix} 1 & c \\ c^* & 1 \end{pmatrix}$$

So calculating the eigenvalues for D, we have:

$$\det D = \begin{pmatrix} 1-\lambda & c \\ c^* & 1-\lambda \end{pmatrix} = (1-\lambda)^2 - |c|^2 = 0$$

$$(1-\lambda)^2 = |c|^2$$

$$1 - \lambda = \pm\,|c|$$

$$\lambda = 1 \pm |c|$$

Since $c \leq 1$, we know that the eigenvalue λ satisfy:

$$0 \leq 1 - |c| \ \leq \lambda \leq 1 + |c| \ \leq 2$$

So $0 \leq \lambda \leq 2$. Then we have that $D \leq 2I$, thus

$$M_A + M_B = \frac{1}{1+c} D \leq \frac{2}{1+c} I \leq I$$

And so $I - M_A - M_B \geq 0$ thus positive semidefinite.

Answer 6. (a) Notice that the state 1 is the Bell state $|\phi^+\rangle$ and state 2 is the Bell state $|\psi^+\rangle$. We know that both states are entangled, with different correlations: for $|\phi^+\rangle$ both qubits are the same (00 or 11), and for $|\psi^+\rangle$ the qubits are different (01 or 10). We need a basis which the states can be distinguished based on the outcomes. If we choose $\{|0\rangle, |1\rangle\}$ we have for the state 1: 50% probabilty for 00 or 11. And for state 2: 50% probabilty for 01 or 10. So if Alice and Bob get the same results (00 or 11) thay have state 1, and if they get different results (01, 10) they have state 2. So in this case the states are perfect distinguishing.

(b) For this case we can apply an analogous reasoning from the last item, but this time using $\{|+\rangle, |-\rangle\}$ as basis. So for the state 1: 50% probabilty for ++ or –. And for state 2: 50% probabilty for +- or -+. And again, if Alice and Bob have the same results they have state 1, and if they get different results they have state 2. And again the states are perfect distinguishing.

(c) blank

Answer 7. To analyze the teleportation protocol, we need to consider Alice's two qubits (A and A') together. Let's expand the state:

$$|\psi_{CAB}\rangle = \frac{1}{2}(|0\rangle_C|0\rangle_A|0\rangle_{A'}|0\rangle_B + |0\rangle_C|0\rangle_A|1\rangle_{A'}|1\rangle_B + |1\rangle_C|1\rangle_A|0\rangle_{A'}|0\rangle_B + |1\rangle_C|1\rangle_A|1\rangle_{A'}|1\rangle_B)$$

Alice performs a Bell basis measurement on her qubits A and A'. The Bell basis consists of four states:

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

We can rewrite Alice's qubits (A and A') in this basis. For example:

$$|00\rangle_{AA'} = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle)$$

$$|11\rangle_{AA'} = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)$$

$$|01\rangle_{AA'} = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)$$

$$|10\rangle_{AA'} = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle)$$

When Alice performs her Bell measurement, she gets one of four possible outcomes, each occurring with equal probability (25%). The state of Charlie and Bob's qubits collapses accordingly

1. If Alice measures $|\Phi^+\rangle$:
$$|\psi_{CB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{CB} + |11\rangle_{CB})$$
No correction needed

2. If Alice measures $|\Phi^-\rangle$:
$$|\psi_{CB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{CB} - |11\rangle_{CB})$$
Bob applies Z

3. If Alice measures $|\Psi^+\rangle$:
$$|\psi_{CB}\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{CB} + |10\rangle_{CB})$$
Bob applies X

4. If Alice measures $|\Psi^-\rangle$:
$$|\psi_{CB}\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{CB} - |10\rangle_{CB})$$
Bob applies XZ

After correction, the state of CB will always be $\frac{1}{\sqrt{2}}(|00\rangle_{CB} + |11\rangle_{CB})$. So the teleportation protocol preserves the entanglement initially shared between Charlie and Alice, transferring it to Charlie and Bob.

Answer 8. Consider a quantum bit commitment protocol where Alice prepares either $\rho_0 = |\psi_0\rangle\langle\psi_0|_{AB}$ or $\rho_1 = |\psi_1\rangle\langle\psi_1|_{AB}$ in a bipartite system AB, sends subsystem B to Bob, and keeps A. For the protocol to be concealing, Bob's reduced states must satisfy:

$$\mathrm{Tr}_A(\rho_0) = \mathrm{Tr}_A(\rho_1) = \sigma_B$$

This implies the global states are related by a unitary on A:

$$|\psi_1\rangle_{AB} = (U_A \otimes I_B)|\psi_0\rangle_{AB}$$

Alice can exploit this structure to cheat:

- After committing to 0 (sending B of $|\psi_0\rangle$), she keeps A
- To change to 1, she applies U_A to A
- The final state becomes $|\psi_1\rangle$, which Bob will accept as commitment 1

Since the reduced state σ_B remains unchanged during this process, Bob cannot detect Alice's manipulation. Therefore, any concealing protocol necessarily violates binding - Alice can always change her commitment by applying the appropriate unitary to her subsystem.