Problem 1

Given the state:

\[ |\Psi\rangle = \left( \frac{1}{2} + \epsilon \right)^{1/2} |00\rangle + \left( \frac{1}{2} - \epsilon \right)^{1/2} |11\rangle \]

for some \( 0 \leq \epsilon \leq 1/2 \), notice that this is an approximate version of the maximally entangled state \( |\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \). We can quantify this closeness in two ways. One is to compute the overlap between this state and the \( |\Phi^+\rangle \). The second, is to compute the \( S \) quantity, from Tutorial 4, for the state.

A) Compute the “overlap” between \( |\Psi\rangle \) and \( |\Phi^+\rangle \), or, in other words, compute \( \langle \Psi | \Phi^+ \rangle \). This quantity gives us an indication as to how close \( |\Psi\rangle \) is to the maximally entangled state \( |\Phi^+\rangle \), as a function of \( \epsilon \).

B) Compute the \( S \) quantity, from Tutorial 4, for \( |\Psi\rangle \) and expand the expression into powers of \( \epsilon \) up to leading order\(^1\). In other words, you can assume \( \epsilon << 1/2 \). Recall that the \( S \) quantity was defined as:

\[ S = E_{00} - E_{01} + E_{10} + E_{11} \]

Where \( E_{xy} \) are the correlators, and we are using the observables from Tutorial 4:

\[
A_0 = Z, \quad A_1 = X, \\
B_0 = \frac{1}{\sqrt{2}}(X + Z), \quad B_1 = \frac{1}{\sqrt{2}}(X - Z)
\]

Solution:

A) To compute the overlap, we simply expand each state in the computational basis and compute the inner product:

\[
\langle \Psi | \Phi^+ \rangle = \left( \langle 00 | \left( \frac{1}{2} + \epsilon \right)^{1/2} \right) + \langle 11 | \left( \frac{1}{2} - \epsilon \right)^{1/2} \rangle \right) \frac{|00\rangle + |11\rangle}{2^{1/2}}
\]

\(^1\)Recall that if \( x << 1 \), we have that \( (1 + x)^a \approx 1 + ax \).
Expanding out we get:

\[
\langle \Psi | \Phi^+ \rangle = \langle 00 | 00 \rangle \left( \frac{1}{4} + \frac{\epsilon}{2} \right)^{1/2} + \langle 00 | 11 \rangle \left( \frac{1}{4} + \frac{\epsilon}{2} \right)^{1/2} + \langle 11 | 00 \rangle \left( \frac{1}{4} - \frac{\epsilon}{2} \right)^{1/2} + \langle 11 | 11 \rangle \left( \frac{1}{4} - \frac{\epsilon}{2} \right)^{1/2}
\]

But we know that \(\langle 00 | 00 \rangle = \langle 11 | 11 \rangle = 1\) and \(\langle 00 | 11 \rangle = \langle 11 | 00 \rangle = 0\) hence:

\[
\langle \Psi | \Phi^+ \rangle = \left( \frac{1}{4} + \frac{\epsilon}{2} \right)^{1/2} + \left( \frac{1}{4} - \frac{\epsilon}{2} \right)^{1/2}
\]

This concludes A), however, for a more direct comparison with B), let us square this overlap and expand up to leading order in \(\epsilon\). We first make the following notation, which we will also use in B):

\[
c_1 = \left( \frac{1}{2} + \frac{\epsilon}{2} \right)^{1/2}
\]

\[
c_2 = \left( \frac{1}{2} - \frac{\epsilon}{2} \right)^{1/2}
\]

We then have that:

\[
| \langle \Psi | \Phi^+ \rangle |^2 = \frac{1}{2} (c_1 + c_2)^2 = \frac{1}{2} (c_1^2 + c_2^2 + 2c_1c_2) = \frac{1}{2} (1 + 2c_1c_2) = \frac{1}{2} (1 + (1 - 4\epsilon^2)^{1/2})
\]

We now expand the square root term up to leading order, \((1 - 4\epsilon^2)^{1/2} \approx 1 - 2\epsilon^2\), so:

\[
| \langle \Psi | \Phi^+ \rangle |^2 \approx \frac{1}{2} (2 - 2\epsilon^2) = 1 - \epsilon^2
\]

Note that for \(\epsilon = 0\), the overlap is 1, as expected.

B) We start by computing the correlators in much the same way as was done in Tutorial 3:

\[
E_{00} = \langle \Psi | A_0 \otimes B_0 | \Psi \rangle = \frac{1}{\sqrt{2}} \langle \Psi | Z \otimes X | \Psi \rangle + \frac{1}{\sqrt{2}} \langle \Psi | Z \otimes Z | \Psi \rangle
\]

\[
\langle \Psi | Z \otimes X | \Psi \rangle = \langle \Psi | (c_1 | 01 \rangle - c_2 | 10 \rangle) = 0
\]

\[
\langle \Psi | Z \otimes Z | \Psi \rangle = \langle \Psi | (c_1 | 00 \rangle + c_2 | 11 \rangle) = c_1^2 + c_2^2
\]

So:

\[
E_{00} = \frac{c_1^2 + c_2^2}{\sqrt{2}} = \frac{1}{\sqrt{2}}
\]

Similarly, we have that:

\[
E_{01} = -\frac{1}{\sqrt{2}}
\]
Now, when computing $E_{10}$ and $E_{11}$ we need to compute the expectations of $X \otimes X$ and $X \otimes Z$:

$$\langle \Psi | X \otimes X | \Psi \rangle = \langle \Psi | (c_1 |11\rangle + c_2 |00\rangle) = 2c_1c_2$$
$$\langle \Psi | X \otimes Z | \Psi \rangle = \langle \Psi | (c_1 |10\rangle - c_2 |01\rangle) = 0$$

Therefore:

$$E_{10} = E_{11} = c_1c_2\sqrt{2}$$

So, in the end we have:

$$S = \sqrt{2}(1 + 2c_1c_2) = \sqrt{2}(1 + (1 - 4\epsilon^2)^{1/2})$$

Note that using what we’ve seen in A), we can also express this as:

$$S = 2\sqrt{2}|\langle \Psi | \Phi^+ \rangle|^2$$

This shows us how the $S$ quantity scales as a function of the overlap between the two states. Using the expansion up to leading order of $(1 - 4\epsilon^2)^{1/2} \approx 1 - 2\epsilon^2$, we have:

$$S \approx 2\sqrt{2}(1 - \epsilon^2)$$

We can see that for $\epsilon = 0$, we have the familiar $S = 2\sqrt{2}$. It would be interesting to compute the value of $\epsilon$ for which we get $S = 2$ (explainable through local hidden variables). If we substitute $S = 2$ in the original expression we computed, we get that $\epsilon = \frac{1}{2}\sqrt{2} - 2 \approx 0.455$. Therefore, we notice that non-local correlations are observed when $0 < \epsilon < 0.455$. Given that $\epsilon < 0.5$, we notice that there is a relatively small interval in which $\epsilon$ gives local correlations. It should be noted that this happens for this particular choice of observables and this particular choice of $S$. It can be shown that any pure entangled state gives rise to non-local correlations, the problem is just to find a good set of observables. To conclude, the observables we consider are just as important as the quantum state when looking for non-local correlations.

**Problem 2**

Alice and Bob decide to play the following game: Alice flips a fair coin. If the coin lands on heads she will prepare, uniformly at random, one of the states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ and send it to Bob. If the coin lands on tails she will prepare, uniformly at random, one of the states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ and send it to Bob, where:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Bob wins the game if he can determine what Alice’s coin landed on. Of course, he will try to infer this from the 2-qubit state that Alice sent him. What is the maximum probability that Bob wins this game? Justify your answer (Hint: try writing out the density matrices for the two situations).
Solution: As the hint suggests, we will write out the density matrices for the situations. For the first case, Alice prepares, with equal probability, one of the states of the 2-qubit computational basis hence:

\[ \rho_1 = \frac{1}{4}( |00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 10| + |11\rangle \langle 11|) \]

In matrix form, we can express \( \rho_1 \) as follows:

\[
\rho_1 = \begin{pmatrix}
\langle 00 \mid & \langle 01 \mid & \langle 10 \mid & \langle 11 \mid \\
|00\rangle & 1/4 & 0 & 0 \\
|01\rangle & 0 & 1/4 & 0 \\
|10\rangle & 0 & 0 & 1/4 \\
|11\rangle & 0 & 0 & 0 & 1/4
\end{pmatrix}
\]

This is essentially the identity matrix multiplied by 1/4, and thus the state corresponds to the maximally mixed state. An important property of this state is that it has the same form in all bases. In other words, if we were to re-express the state in another basis we would find that it is still the identity matrix. This stems from the simple fact that:

\[ UIU^\dagger = I \]

for any unitary matrix \( U^2 \).

For the second case, Alice prepares with equal probability one of the 4 entangled states, hence we have:

\[ \rho_2 = \frac{1}{4}( |\Phi^+\rangle \langle \Phi^+| + |\Phi^-\rangle \langle \Phi^-| + |\Psi^+\rangle \langle \Psi^+| + |\Psi^-\rangle \langle \Psi^-|) \]

The 4 entangled states are not arbitrary. It is not difficult to show that they, in fact, form an orthonormal basis. To show this, it is sufficient to show that there exists some unitary \( U \), which maps the computational basis states to the 4 entangled states. Let \( U = CNOT(H \otimes I) \). Note that:

\[ U |00\rangle = |\Phi^+\rangle \quad U |01\rangle = |\Psi^+\rangle \quad U |10\rangle = |\Phi^-\rangle \quad U |11\rangle = |\Psi^-\rangle \]

This means that \( \rho_2 \) in matrix form, in the basis of the entangled states is:

\[
\rho_2 = \begin{pmatrix}
\langle \Phi^+ \mid & \langle \Phi^- \mid & \langle \Psi^+ \mid & \langle \Psi^- \mid \\
|\Phi^+\rangle & 1/4 & 0 & 0 \\
|\Phi^-\rangle & 0 & 1/4 & 0 \\
|\Psi^+\rangle & 0 & 0 & 1/4 \\
|\Psi^-\rangle & 0 & 0 & 0 & 1/4
\end{pmatrix}
\]

But this is once again the totally mixed state which, if we re-express in the computational basis, should have

---

\footnote{Recall that diagonalizing a hermitian matrix \( \rho \), can be done by conjugating with a unitary operation. In other words, there exist a diagonal matrix \( D \) and a unitary \( U \), such that \( U \rho U^\dagger = D \). In our case, \( D = I/4 \).}
the same form hence:

\[
\rho_2 = \begin{pmatrix}
    \langle 00 | & \langle 01 | & \langle 10 | & \langle 11 |
    \\
    |00\rangle & 1/4 & 0 & 0 & 0 \\
    |01\rangle & 0 & 1/4 & 0 & 0 \\
    |10\rangle & 0 & 0 & 1/4 & 0 \\
    |11\rangle & 0 & 0 & 0 & 1/4
\end{pmatrix}
\]

Therefore \( \rho_1 = \rho_2 \). Since the density matrices of the two situations are identical, this means that there is no procedure, which Bob can perform, in order to distinguish between them. Thus, his probability of correctly guessing the outcome of Alice’s coin is the same as if he had not received any state from Alice, i.e. 1/2.

The situation presented here is another case of “quantum weirdness”. We know that Alice is preparing completely different types of states in the two situations. In the first case she prepares a separable state, whereas in the second case she prepares an entangled state. Given that we’ve seen that entangled states have fundamentally different properties from separable states it is natural to think that there should be some way to distinguish between the two situations. One could think “maybe Bob can perform some sort of Bell experiment with the two qubits to see if they produce non-local or local correlations and thus determine if the state is entangled or not”. But this will not work. Recall that for the particular CHSH inequality we studied, we only observed a violation from the classically predicted value if we measure a particular state with a particular set of observables. If, using the same observables, we measured a different entangled state we might not observe any non-local behaviour. While non-locality is fundamentally arising from entanglement, only a particular set of observables will reveal it. In our case, the problem is that, whatever observables Bob chooses to measure, are independent of the state that Alice sends. But since, even in the case where Alice sends an entangled state, she randomizes over the choice of the entangled state, this completely masks any non-local correlations.

One could come up with even more complicated experiments to detect entanglement, but all of them will fail in this case. While, mathematically, showing that the density matrices of the two situations are identical isn’t of great conceptual difficulty (though it might be tedious), physically there is a very profound implication of this result. Assuming quantum mechanics is correct, any measurement that Bob performs on the two qubits, will produce identical statistics for both of Alice’s scenarios. Therefore, the two scenarios are indistinguishable. It is facts such as this that are the basis for many quantum cryptographic protocols.

**Problem 3**

Many popular accounts of entanglement claim that it can be used in order to send information faster than the speed of light. Prove that this is not the case. Specifically, assume Alice and Bob share a general two-qubit state \( |\Psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle \), where \( \sum_{i=0}^{3} |\alpha_i|^2 = 1 \). The aim is to show that no matter what Alice does to her qubit (whether she does nothing, applies a unitary operation or measures it), the reduced state of Bob’s qubit remains the same (therefore, he cannot infer any information about Alice’s operations).

A) Assuming Alice does nothing to her qubit, compute the reduced density matrix of Bob’s qubit. Recall from the lectures that the reduced density matrix of Bob’s qubit is just \( Tr_A(\rho) \), where \( Tr_A \) is the partial
trace over Alice’s qubit (tracing out Alice’s qubit) and \( \rho \) is the state of the system. Start by first writing down \( \rho \) explicitly.

**B)** Now assume Alice applies some general unitary \( U \) to her qubit. Compute the reduced density matrix for Bob’s qubit. Compare with the previous result.

**C)** Lastly, assume Alice performs a measurement in the computational basis on her qubit. Compute again the reduced density matrix for Bob’s qubit. Compare with the previous results. How do you interpret these results? **(Hint:** If the state of the system prior to Alice’s measurement is \( \rho \), then after measurement it will be \( \rho' = (M_0 \otimes I)\dagger \rho (M_0 \otimes I) + (M_1 \otimes I)\dagger \rho (M_1 \otimes I) \), where \( M_0 = |0\rangle \langle 0|, M_1 = |1\rangle \langle 1| \) )

**Solution:**

**A)** Since \( |\Psi\rangle \) is a pure state, we have that \( \rho = |\Psi\rangle \langle \Psi| \). Expanding out in the computational basis, this yields:

\[
\rho = (\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle)(\langle 00|\alpha_0^* + \langle 01|\alpha_1^* + \langle 10|\alpha_2^* + \langle 11|\alpha_3^*)
\]

Or:

\[
\rho = |\alpha_0|^2 |00\rangle \langle 00| + \alpha_0\alpha_1^* |00\rangle \langle 01| + \alpha_0\alpha_2^* |00\rangle \langle 10| + \alpha_0\alpha_3^* |00\rangle \langle 11| + ... + |\alpha_3|^2 |11\rangle \langle 11|
\]

In matrix form, \( \rho \) looks like this:

\[
\rho = \begin{pmatrix}
|00\rangle & |01\rangle & |10\rangle & |11\rangle \\
|00\rangle & |0\alpha_0|^2 & \alpha_0\alpha_1^* & \alpha_0\alpha_2^* & \alpha_0\alpha_3^* \\
|01\rangle & \alpha_1\alpha_0^* & |\alpha_1|^2 & \alpha_1\alpha_2^* & \alpha_1\alpha_3^* \\
|10\rangle & \alpha_2\alpha_0^* & \alpha_2\alpha_1^* & |\alpha_2|^2 & \alpha_2\alpha_3^* \\
|11\rangle & \alpha_3\alpha_0^* & \alpha_3\alpha_1^* & \alpha_3\alpha_2^* & |\alpha_3|^2
\end{pmatrix}
\]

Let us now compute \( Tr_A(\rho) \). Keep in mind that\(^3\):

\[
Tr_A(|ab\rangle \langle cd|) = \begin{cases} |b\rangle \langle d|, & \text{when } a = c \\ 0, & \text{otherwise} \end{cases}
\]

We therefore find that:

\[
Tr_A(\rho) = (|\alpha_0|^2 + |\alpha_2|^2) |0\rangle \langle 0| + (|\alpha_1|^2 + |\alpha_3|^2) |1\rangle \langle 1| + (\alpha_0\alpha_1^* + \alpha_2\alpha_3^*) |0\rangle \langle 1| + (\alpha_1\alpha_0^* + \alpha_3\alpha_2^*) |1\rangle \langle 0|
\]

**B)** Suppose that the unitary, \( U \), that Alice applies on her qubit, has the following effect on the computational basis:

\[
U |0\rangle = |\phi\rangle \quad U |1\rangle = |\phi^\perp\rangle
\]

where \( |\phi\rangle \) and \( |\phi^\perp\rangle \) form an orthonormal basis. If we consider the density matrix for this new state, \( (U \otimes I)\rho \), it is convenient to express it, not in the computational basis, but in the basis: \( |\phi\rangle \langle 0|, |\phi\rangle \langle 1|, |\phi^\perp\rangle \langle 0|, |\phi^\perp\rangle \langle 1| \).

---

\(^3\) And also keep in mind that \( |ab\rangle \langle cd| \) is simply a short-hand notation for \( |a\rangle |b\rangle \langle c\rangle \langle d| \), or \( |a\rangle \langle c| \otimes |b\rangle \langle d| \).
For this basis, it is easy to see that it has exactly the same form as $\rho$ does in the computational basis:

$$(U \otimes I)\rho = \begin{pmatrix} |\phi\rangle \langle 0| & |\phi\rangle \langle 1| & |\phi^+\rangle \langle 0| & |\phi^+\rangle \langle 1| \\ |\phi\rangle \langle 1| & |\alpha_0|^2 & \alpha_0 \alpha_1^* & \alpha_0 \alpha_2^* \\ |\phi^+\rangle \langle 0| & \alpha_1 \alpha_0^* & |\alpha_1|^2 & \alpha_1 \alpha_2^* \\ |\phi^+\rangle \langle 1| & \alpha_3 \alpha_0^* & \alpha_3 \alpha_1^* & |\alpha_3|^2 \end{pmatrix}$$

We now compute the partial trace, exactly as before, but keeping in mind that:

$$\text{Tr}(\rho) = \frac{1}{2} \sum_i |i\rangle \langle i| \rho |i\rangle \langle i|$$

Interestingly, the terms that have been eliminated are exactly the ones that did not feature in the partial trace of $\rho$. On the other hand, the action of $M$ on $\rho$ has the effect of removing all terms which are not of the form $|0\rangle \langle 0| \otimes |b\rangle \langle d|$. Given this fact, the action of $M_0 \otimes I$ on $\rho$ has the effect of removing all terms which are not of the form $|0\rangle \langle 1| \otimes |b\rangle \langle d|$. Putting things together means that our new density matrix will be:

$$\rho' = (M_0 \otimes I)^\dagger \rho (M_0 \otimes I) + (M_1 \otimes I)^\dagger \rho (M_1 \otimes I) = \begin{pmatrix} |00\rangle \langle 00| & |01\rangle \langle 01| & |10\rangle \langle 10| & |11\rangle \langle 11| \\ |00\rangle & |\alpha_0|^2 & 0 & 0 \\ |01\rangle & \alpha_0 \alpha_1^* & |\alpha_1|^2 & 0 \\ |10\rangle & 0 & 0 & |\alpha_2|^2 \\ |11\rangle & 0 & 0 & \alpha_3 \alpha_2^* \end{pmatrix}$$

Interestingly, the terms that have been eliminated are exactly the ones that did not feature in the partial trace of $\rho$. When we therefore compute $\text{Tr}(\rho')$, we find that:

$$\text{Tr}(\rho') = (|\alpha_0|^2 + |\alpha_2|^2) |0\rangle \langle 0| + (|\alpha_1|^2 + |\alpha_3|^2) |1\rangle \langle 1| + (\alpha_0 \alpha_1^* + \alpha_2 \alpha_3^*) |0\rangle \langle 1| + (\alpha_1 \alpha_2^* + \alpha_3 \alpha_4^*) |1\rangle \langle 0|$$

We have found that no matter what Alice does to her qubit, whether she does nothing, applies a unitary operation, or measures it, the reduced state of Bob is identical. This means that Bob cannot distinguish between the three situations. In other words, whatever Alice does, there is no way for her to force Bob’s reduced state to be different and thus convey information to him. One could object and say “but this doesn’t cover the full spectrum of Alice’s operations. What if she entangles her qubit with another qubit and then
measures? What if they shared multiple entangled qubits instead of just two?”. All of these situations are covered by the more general no-signalling theorem. The above reasoning can be generalized for any operation on Alice’s side and any shared state between Alice and Bob.

Problem 4

A) Show that the following 2-qubit observables all commute with each other (pair-wise): $X \otimes I$, $I \otimes X$, $X \otimes X$. Next, show the same for: $X \otimes Z$, $Z \otimes X$, $(XZ) \otimes (ZX)$. Finally, prove the same thing for: $X \otimes X$, $Z \otimes Z$, $(XZ) \otimes (XZ)$. Recall that two observables, $A$ and $B$, commute if $[A,B] = AB - BA = 0$.

B) When 2 observables commute, they can be simultaneously measured. Mathematically, commuting observables share at least one common eigenvector. The common eigenvectors are the possible measurement outcomes, when measuring both observables. Consider $X \otimes X$ and $Z \otimes Z$, each having eigenvalues $+1$ and $-1$ (so these are observables with 2 possible outcomes). These two observables will have a common $+1$ eigenvector, denoted $|\psi\rangle$, and a common $-1$ eigenvector, denoted $|\phi\rangle$. When they are measured simultaneously, on some two-qubit state, they will produce identical outcomes, collapsing the measured state to either $|\psi\rangle$, if both produced outcome $+1$ or to $|\phi\rangle$, if both produced outcome $-1$.

Compute $|\psi\rangle$ and $|\phi\rangle$. It is helpful to do so by expressing each state in the computational basis and then using the fact that these are eigenvectors. For instance, one can write $|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$, such that $\sum_{i=0}^{3} |\alpha_i|^2 = 1$ and $X \otimes X |\psi\rangle = |\psi\rangle$ and $Z \otimes Z |\psi\rangle = |\psi\rangle$. Use these facts to determine the $\alpha_i$ coefficients. Do the same for $|\phi\rangle$.

C) Suppose we have two commuting observables $A$ and $B$, each having eigenvalues $+1$ and $-1$. For simplicity, assume that either $A$ and $B$ have one common $+1$ eigenvector and one common $-1$ eigenvector (as in the previous example), or that $A$ has a $+1$ eigenvector which is a $-1$ eigenvector for $B$ and vice versa. Define the observable $C = AB$. Suppose we measure $C$ on some quantum state $|\psi\rangle$, obtaining outcome $c \in \{+1, -1\}$. Prove that, had we instead measured first $A$ on $|\psi\rangle$, with outcome $a$ and then $B$ on the resulting state, with outcome $b$ then $c = ab$. In other words, show that measuring $C$ is the same as measuring $A$ and then $B$ and multiplying the outcomes.

Solution:

A) First note that $[A \otimes B, C \otimes D] = (A \otimes B)(C \otimes D) - (C \otimes D)(A \otimes B) = AC \otimes BD - CA \otimes DB$. We will also be using the fact that $[A,B] = -[B,A]$. Thus, if we show that $[A,B] = 0$, clearly $[B,A] = 0$. Concerning the $X$ and $Z$ operators, we will use the facts that $X^2 = Z^2 = I$ and that $XZ = -ZX$. Finally, it is evident that an operator always commutes with itself. We therefore have:

$$[X \otimes I, I \otimes X] = X \otimes X - X \otimes X = 0$$
$$[X \otimes I, X \otimes X] = I \otimes X - I \otimes X = 0$$
$$[I \otimes X, X \otimes X] = X \otimes I - X \otimes I = 0$$
Next:

\[ [X \otimes Z, Z \otimes X] = (XZ) \otimes (ZX) - (ZX) \otimes (XZ) = -(XZ) \otimes (XZ) + (XZ) \otimes (XZ) = 0 \]
\[ [X \otimes Z, (XZ) \otimes (XZ)] = (X^2Z) \otimes (XZ) - (XZ) \otimes (XZ)^2 = -Z \otimes X + Z \otimes X = 0 \]
\[ [Z \otimes X, (XZ) \otimes (XZ)] = (XZ) \otimes (X^2Z) - (XZ^2) \otimes (XZX) = -X \otimes Z + X \otimes Z = 0 \]

Finally:

\[ [X \otimes X, Z \otimes Z] = (XZ) \otimes (XZ) - (ZX) \otimes (XZ) = (XZ) \otimes (XZ) - (XZ) \otimes (XZ) = 0 \]
\[ [X \otimes X, (XZ) \otimes (XZ)] = (X^2Z) \otimes (XZ) - (XZ) \otimes (XZX) = Z \otimes Z - Z \otimes Z = 0 \]
\[ [Z \otimes Z, (XZ) \otimes (XZ)] = (XZ) \otimes (XZX) - (XZ^2) \otimes (XZ) = X \otimes X - X \otimes X = 0 \]

B) We know that \( X \otimes X |\psi\rangle = |\psi\rangle \) and \( Z \otimes Z |\psi\rangle = |\psi\rangle \). Expanding in the computational basis, the two conditions equate to:

\[ \alpha_0 |11\rangle + \alpha_1 |10\rangle + \alpha_2 |01\rangle + \alpha_3 |00\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle \]

and

\[ \alpha_0 |00\rangle - \alpha_1 |01\rangle - \alpha_2 |10\rangle + \alpha_3 |11\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle \]

The first condition tells us that \( \alpha_0 = \alpha_3, \alpha_1 = \alpha_2 \). The second condition tells us that \( \alpha_1 = -\alpha_1 \) and \( \alpha_2 = -\alpha_2 \). These last two imply that \( \alpha_1 = \alpha_2 = 0 \). Our state therefore becomes:

\[ |\psi\rangle = \alpha_0 (|00\rangle + |11\rangle) \]

But this state should be normalized, meaning that \( 2|\alpha_0|^2 = 1 \), or \( |\alpha_0| = 1/\sqrt{2} \). The values of \( \alpha_0 \) compatible with this are \( \alpha_0 = e^{i\phi}/\sqrt{2} \) for any \( \phi \). This leads to:

\[ |\psi\rangle = e^{i\phi} (|00\rangle + |11\rangle)/\sqrt{2} \]

Finally, note that \( e^{i\phi} \) is simply a global phase, and the first postulate of quantum mechanics tells us that global phases don’t matter (quantum states are equivalence classes of vectors up to global phases), hence:

\[ |\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \]

The familiar |\Phi^+\rangle Bell state is the +1 eigenstate of \( X \otimes X \) and \( Z \otimes Z \). Let us now compute the −1 eigenstate.

We have that \( X \otimes X |\phi\rangle = -|\phi\rangle \) and \( Z \otimes Z |\phi\rangle = -|\phi\rangle \). Expanding in the computational basis, the two conditions equate to:

\[ \alpha_0 |11\rangle + \alpha_1 |10\rangle + \alpha_2 |01\rangle + \alpha_3 |00\rangle = -(\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle) \]
and
\[ \alpha_0 |00\rangle - \alpha_1 |01\rangle - \alpha_2 |10\rangle + \alpha_3 |11\rangle = -(\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle) \]
The first condition tells us that \( \alpha_0 = -\alpha_3 \), \( \alpha_1 = -\alpha_2 \). The second condition tells us that \( \alpha_0 = -\alpha_0 \) and \( \alpha_3 = -\alpha_3 \). These last two imply that \( \alpha_0 = \alpha_3 = 0 \). Our state therefore becomes:

\[ |\phi\rangle = \alpha_1 (|01\rangle - |10\rangle) \]

By imposing normalization and ignoring global phase we find that:

\[ |\phi\rangle = (|01\rangle - |10\rangle)/\sqrt{2} \]

C) Since \( A \) and \( B \) commute with each other, that means that they can be diagonalized in the same basis. More formally, it means that we can write:

\[ A = \sum_i \lambda_A^i |i\rangle \langle i| \quad B = \sum_i \lambda_B^i |i\rangle \langle i| \]

Where \( \{|i\rangle\}_i \) is the basis in which both \( A \) and \( B \) can be diagonalized, \( \{\lambda_A^i\} \) are the eigenvalues of \( A \) (which are either +1 or -1) and \( \{\lambda_B^i\}_i \) are the eigenvalues of \( B \) (also either +1 or -1).

Let us now look at \( C = AB \). First, note that \( C \) commutes with both \( A \) and \( B \):

\[ [C, A] = ABA - AAB = AAB - ABA = 0 \quad [C, B] = ABB - BAB = ABB - ABB = 0 \]

The two relations follow from the fact that \( AB = BA \). This means that \( C \) can also be diagonalized in the \( \{|i\rangle\}_i \) basis. Computing \( C \) explicitly yields:

\[ C = \sum_i \sum_j \lambda_A^i \lambda_B^j |i\rangle \langle i| \langle j| \]

But \( \langle i|j\rangle = 0 \), when \( i \neq j \) and \( \langle i|j\rangle = 1 \) when \( i = j \), thus:

\[ C = \sum_i \lambda_A^i \lambda_B^i |i\rangle \langle i| \]

We have therefore expressed \( C \) in the diagonal basis. Notice that its eigenvalues, which represent the possible measurement outcomes, are exactly the product of eigenvalues (measurement outcomes) of the \( A \) and \( B \) observables. This concludes the proof.

In the literature, this property of commuting observables is known as functional consistency and leads to some interesting situations involving non-locality and so-called contextuality. An example of this is encountered in the special square problem.
Problem 5

In the lectures, you were shown that one can use superdense coding in order to send 2 bits of information by only sending one qubit. You were also shown that quantum teleportation involves “sending” (teleporting) one qubit of quantum information by transmitting 2 classical bits. Suppose there exists a procedure, which we will call hyperdense coding, with which one can send k bits of information by sending a single qubit. Show, either for $k = 3$ or for $k = 4$, that if such a procedure existed, one could send an unbounded amount of information by sending a single qubit\(^4\). In other words, for any $N > 0$, show that there exists a procedure through which Alice can send $N$ bits of information to Bob by only sending him one qubit (and nothing else, not even classical bits).

**Solution:** Let’s look at two possible ways to solve this problem. We’re going to illustrate one solution for the $k = 4$ case and the other for the $k = 3$ case, though these can be interchanged.

First, for $k = 4$. Suppose Alice wants to send Bob a message having $M > 0$ bits of information. She can always pad the message to $N \geq M$ bits, so that $N$ is a power of 2. Now, suppose Alice and Bob were sharing $N/4$ Bell states\(^5\). She can use hyperdense coding in order to send Bob the $N$ bits, by simply sending him $N/4$ qubits (since each qubit equates to 4 bits of information, with hyperdense coding). We’ve turned our problem of Alice sending classical bits to Bob, to one in which Alice has to send qubits to Bob. But we have a procedure for doing this as well, which is teleportation. If Alice wishes to send $N/4$ qubits to Bob, she can do this by sending double that amount in classical bits, or $N/2$ bits.

Thus, we have shown that Alice can send $N$ bits of information to Bob by only sending him $N/2$ bits. If we go through the same procedure again, she is able to send $N$ bits of information by only sending $N/4$ bits. Repeating this $\log(N) - 2$ times, we eventually find that Alice can send $N$ bits of information by sending exactly 4 bits to Bob. But this can be done by sending one qubit. Hence, assuming Alice and Bob were sharing $N$ Bell states, hyperdense coding, together with teleportation allow for Alice to send $N$ bits of information to Bob by sending a single qubit.

Now let’s look at $k = 3$. In the previous case, we started from wanting to send an $N$-bit message and reduced it to sending one qubit. This time, we’ll look at things from the “other direction”. Once again, we’re assuming that Alice and Bob are sharing at least $N$ Bell pairs. If Alice sends one qubit to Bob, using hyperdense coding, that means that Bob obtains 3 bits of information from Alice. Out of these 3 bits, 2 can encode one qubit of quantum information, via teleportation. But that qubit encodes 3 other bits of information, so from the original 3 bits, Bob obtains 4 bits. Repeating this $N$ times, Bob can extract $N$ bits of information from the original qubit send by Alice.

If one takes the reasoning further, it is not too difficult to show that hyperdense coding also implies the ability to send information faster than the speed of light (in fact instantaneously). Why is that? Suppose that instead of $N$ Bell states, Alice and Bob share $8N$ Bell states. We know that had Alice sent one qubit to Bob, Bob would have recovered 3 bits of information. Then, through the iterative process described above, he can use this 3 bit message to “extract” (through measurement of his halves of the $N$ Bell states) whatever $N$ bit message Alice intended to send. We will refer to this extraction procedure as decoding. The question now is: instead of Alice even sending a qubit to Bob, why not have Bob just guess the 3-bit string associated

\(^4\)You do not need to prove this for both $k = 3$ and $k = 4$, either one is sufficient for full marks.

\(^5\)Since the task involves using hyperdense coding and teleportation, it is assumed that Alice and Bob were sharing a sufficient number of Bell states so that, at a later time, Alice could send Bob and $N$-bit message.
with that qubit? There are 8 possibilities, so he can apply the decoding procedure in each of the 8 cases (which is why we require them to share $8N$ Bell states). One of these 8 decoding procedure will result in a discernible message from Alice, whereas the other 7 will result in garbage. Thus, by sharing sufficiently many Bell pairs, Alice can transmit a message to Bob without any communication between the two. This contradicts a fundamental theorem of quantum information known as the no-signalling theorem (a weaker version of which is proven in Problem 3), which, roughly, states that entanglement cannot allow you to transmit information instantaneously.

The point of this exercise is to show that superdense coding and teleportation should be complementary to each other. If Alice can transmit $m$ bits of information to Bob by sending one qubit and if she can also transmit one qubit by sending $n$ bits of information, then it better be the case that $m = n$. Otherwise, we end up with situations that contradict known results from quantum information. For the case of quantum mechanics, we know that $m = n = 2$.

**Problem 6**

Alice and Bob decide to play yet another game. Suppose we have a $3 \times 3$ grid, as in Subfigure 1a, which we shall refer to as a special square. Alice and Bob are separated so that they cannot communicate. Alice will be given a number $i \in \{1, 2, 3\}$, representing one of the 3 lines in the square, whereas Bob is given a number $j \in \{1, 2, 3\}$, representing one of the 3 columns in the square. Alice must then provide a 3-tuple $(a_1, a_2, a_3)$, where each $a_i$ is either + or − and the number of + symbols must be even, whereas the number of − symbols must be odd. For instance, a valid response for Alice is $(-, +, +)$. If she received line $i = 1$, then line 1 of the square is completed with $(-, +, +)$.

Conversely, Bob must provide a 3-tuple $(b_1, b_2, b_3)$, also containing + and − symbols, but such that the number of + symbols is odd and the number of − symbols is even. For instance, a valid response for Bob is $(+, +, +)$. If he received line $j = 3$, then line 3 of the square is completed with $(+, +, +)$.

Alice and Bob win the game if they put the same symbol in their common square. In other words $a_j = b_j$. The example described above is shown in Subfigure 1b, where both Alice and Bob put a + in the upper right corner of the square. Alice’s responses are in green, Bob’s are in red, whereas their common square is purple. However, as shown in Subfigure 1c, if Alice provided the same tuple $(-, +, +)$, but Bob provided $(-, +, -)$ then they would lose, since $a_3 = +$, but $b_1 = -$. 

![Special square](image1.png)

(a) Special square

![Win](image2.png)

(b) Win

![Lose](image3.png)

(c) Lose
A) Assuming Alice and Bob are purely classical agents (no quantum operations or entanglement) and cannot communicate at all during the game, show that there is no deterministic strategy that can always win the game. By deterministic strategy we mean that Alice and Bob’s individual responses are completely determined by their inputs, $i$ and $j$, respectively. To always win the game means that for any possible choice of $i$ and $j$, Alice and Bob’s responses will match on their common square.

B) Now show that even if Alice and Bob share classical randomness they cannot win the game with 100% probability (Hint: each possible choice, for their shared randomness, leads to a deterministic strategy. In other words, we are randomizing over deterministic strategies).

C) You will now show that there exists a quantum strategy with which Alice and Bob can always win the game. Suppose they share $2\mid\Phi^+\rangle$ Bell pairs (such that each player has one qubit from the first Bell pair and one qubit from the second). Also consider the following square of observables:

\[
\begin{bmatrix}
X \otimes I & -X \otimes X & I \otimes X \\
X \otimes Z & -(XZ) \otimes (ZX) & Z \otimes X \\
I \otimes Z & -Z \otimes Z & Z \otimes I
\end{bmatrix}
\]

Notice, from problem 4, that the observables in each row (column) commute pair-wise. This means that all observables in a row (column) can be measured simultaneously. Alice will simultaneously measure the observables from row $i$ on her two qubits, whereas Bob will simultaneously measure the observables from row $j$ on his two qubits. An outcome of +1, for a measurement, is taken as the symbol +, whereas an outcome of −1 is taken as the symbol −.

Using problem 4C, show that Alice’s outcomes always produce an even number of + symbols and that Bob’s outcomes always produce an odd number of + symbols. This ensures that both Alice and Bob provide valid tuples.

Finally, show that, because they are sharing Bell states, Alice and Bob will always produce the same outcome on their common square. In other words, show that when they both measure the same observables on their respective qubits, they will obtain identical results.

Solution:

A) We’re going to prove this by contradiction. Assume there exists a deterministic strategy which succeeds in the magic square game. That means that Alice and Bob’s outcomes are determined by some (deterministic) functions $f$ and $g$. Mathematically, we would have that $(a_1^i, a_2^i, a_3^i) = f(i, \lambda)$ and $(b_1^j, b_2^j, b_3^j) = g(j, \lambda)$ where $i$ and $j$ are Alice and Bob’s respective inputs, and $\lambda$ is some shared secret that the two parties can have prior to commencing the game. Note that $f$ does not depend on $j$ and $g$ does not depend on $f$, since we don’t want Alice and Bob’s outcomes to depend on each other’s inputs (no signalling). Also, assume that the outputs of Alice and Bob in each tuple (the $a_k^i$’s and $b_k^j$’s) are either +1 or −1 (where +1 is interpreted as a + and −1 is interpreted as a −).

We now use the explicit constraints that we have for Alice and Bob. Alice must provide a response with an even number of +1’s, which means that for any $i$, and $\lambda$, $a_1^i a_2^i a_3^i = -1$ (the product of the outcomes must be −1). Similarly, Bob’s response should contain an odd number of +1’s, which means that for any $j$ and $\lambda$,
\[ b_1^i b_2^j b_3^j = +1. \] Additionally, since \( f \) and \( g \) should be defined and provide fixed values, for any choice of line and column \( i \) and \( j \), this means that we can compute the product of the outcomes for the entire square:

\[
\begin{align*}
(a_1^1 a_2^2 a_3^3)(a_1^1 a_2^2 a_3^3)(a_1^1 a_2^2 a_3^3) &= -1 \\
(b_1^1 b_2^1 b_3^1)(b_1^2 b_2^2 b_3^2)(b_1^3 b_2^3 b_3^3) &= +1 
\end{align*}
\]

But, to always satisfy the win condition, it must be the case that for any \( i \) and \( j \), this means that we can compute the product of the outcomes for the entire square:

\[
\begin{align*}
(a_1^1 a_2^2 a_3^3)(a_1^1 a_2^2 a_3^3)(a_1^1 a_2^2 a_3^3) &= -1 \\
(b_1^1 b_2^1 b_3^1)(b_1^2 b_2^2 b_3^2)(b_1^3 b_2^3 b_3^3) &= +1 
\end{align*}
\]

Which is a contradiction.

The wordy explanation of the above argument is the following: Alice and Bob must be able to provide responses (deterministically), for any choice of line and column such that their answer on the common square is the same. Since the common square can be any square, this essentially implies that Alice and Bob should be able to fill the square identically. But this cannot be, for Alice needs to put, in total, an even number of + symbols in the square, whereas Bob needs to put an odd number of + symbols. This is the contradiction.

Thus, there is no deterministic strategy which Alice and Bob can perform in order to always win the game.

B) Using the hint, we’re going to prove that no probabilistic strategy can always win the game by randomizing over deterministic strategies. More precisely, we are still assuming that Alice’s responses are given by \( f(i, \lambda) \), and Bob’s responses by \( g(j, \lambda) \), except \( \lambda \) is drawn from some probability distribution \( p(\lambda) \), such that:

\[
\int_\Lambda p(\lambda) d\lambda = 1 
\]

Just like in the proof of Bell’s theorem, this is sufficient, in the sense that any other source of randomness can be incorporated into \( \lambda \).

We therefore have:

\[
\begin{align*}
\int_\Lambda (a_1^1 a_2^2 a_3^3)(a_1^1 a_2^2 a_3^3)(a_1^1 a_2^2 a_3^3) d\lambda &= -1 \\
\int_\Lambda (b_1^1 b_2^1 b_3^1)(b_1^2 b_2^2 b_3^2)(b_1^3 b_2^3 b_3^3) d\lambda &= +1 
\end{align*}
\]

Note that each response, either \( a_i^j \) or \( b_j^i \), depends implicitly on \( \lambda \) even though is not shown explicitly in the above expression. A more correct notation would have been \( a_i^j(\lambda) \) and \( b_j^i(\lambda) \), but this was omitted for convenience.

Just like before, it must be the case that:

\[
\int_\Lambda (a_1^1 a_2^2 a_3^3)(a_1^1 a_2^2 a_3^3)(a_1^1 a_2^2 a_3^3) d\lambda = \int_\Lambda (b_1^1 b_2^1 b_3^1)(b_1^2 b_2^2 b_3^2)(b_1^3 b_2^3 b_3^3) d\lambda 
\]

But this leads to the same contradiction as in the deterministic case.
C) The first part of this question follows immediately from 4C. Let’s examine the product of Alice’s observables for each possible input (i.e. the rows of the square):

\[-(X \otimes I)(X \otimes X)(I \otimes X) = -I\]
\[-(X \otimes Z)((XZ) \otimes (ZX))(Z \otimes X) = -I\]
\[-(I \otimes Z)(Z \otimes Z)(Z \otimes I) = -I\]

In all cases, the outcome is \(-I\). Since \(-I\) has only the eigenvalue \(-1\), this means, using 4C, that the product of the outcomes of Alice’s measurements will be \(-1\). This can only occur if the three observables resulted in outcomes comprising an odd number of \(-1\)’s (or an even number of \(+1\)’s). This is exactly what we expect from Alice.

Similarly, for Bob, we can compute the product of Bob’s observables for each possible input (i.e. the columns of the square):

\[(X \otimes I)(X \otimes Z)(I \otimes Z) = I\]
\[-(X \otimes X)((XZ) \otimes (ZX))(Z \otimes Z) = I\]
\[(I \otimes X)(Z \otimes X)(Z \otimes I) = I\]

We notice that the outcome is always \(I\). Since \(I\) has only the eigenvalue \(+1\), this means, using 4C, that the product of the outcomes of Bob’s measurements will be \(+1\). This can only occur if the three observables resulted in outcomes comprising an even number of \(-1\)’s (or an odd number of \(+1\)’s). And once again, this is exactly what we expect from Bob.

So we’ve seen that both Alice and Bob will provide consistent replies with this strategy. What remains to be shown is that they will also provide identical outcomes for their common square. Let us denote the observable of the common square as \(P \otimes Q\). Also, let us label the qubits of the two Bell states. Say the first Bell state is \(|\Phi^+\rangle_{12}\) and the second is \(|\Phi^+\rangle_{34}\). Alice will have qubits 1 and 3, while Bob has qubits 2 and 4. Accordingly, Alice will measure the observable \(P_1 \otimes Q_3\), while Bob measures \(P_2 \otimes Q_4\).

Showing that Alice and Bob obtain the same outcome, when measuring these observables, is equivalent to showing that:

\[12 \langle \Phi^+ |_{34} \langle \Phi^+ | (P_1 \otimes Q_3) \otimes (P_2 \otimes Q_4) |\Phi^+\rangle_{34} |\Phi^+\rangle_{12} = 1\]

This is equivalent to:

\[12 \langle \Phi^+ | (P_1 \otimes P_2) |\Phi^+\rangle_{12} 34 \langle \Phi^+ | (Q_3 \otimes Q_4) |\Phi^+\rangle_{34} = 1\]

But note that \(P_1 = P_2\) and \(Q_3 = Q_4\) (since Alice and Bob are measuring the same observable, \(P \otimes Q\), but on different qubits). So, we simply have:

\[\langle \Phi^+ | P \otimes P |\Phi^+\rangle \langle \Phi^+ | Q \otimes Q |\Phi^+\rangle = 1\]
where $P, Q \in \{I, X, Z, XZ\}$. But we know that:

\[
\begin{align*}
\langle \Phi^+ | I \otimes I | \Phi^+ \rangle &= 1 \\
\langle \Phi^+ | X \otimes X | \Phi^+ \rangle &= 1 \\
\langle \Phi^+ | Z \otimes Z | \Phi^+ \rangle &= 1 \\
\langle \Phi^+ | (XZ) \otimes (XZ) | \Phi^+ \rangle &= \langle \Phi^+ | (X \otimes X)(Z \otimes Z) | \Phi^+ \rangle = \langle \Phi^+ | X \otimes X | \Phi^+ \rangle = 1
\end{align*}
\]

Thus:

\[
\langle \Phi^+ | P \otimes P | \Phi^+ \rangle = \langle \Phi^+ | Q \otimes Q | \Phi^+ \rangle = 1
\]

for any $P, Q \in \{I, X, Z, XZ\}$. Hence, Alice and Bob will obtain identical measurement outcomes and therefore always provide the same response, thus winning the game with 100% probability.