Problem 1: Doing the Impossible

Let $|\beta_{ab}\rangle$ for $a, b \in \{0, 1\}$ be the Bell states, and let

$$P_{bf} := |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|,$$
$$P_{pf} := |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{01}\rangle\langle\beta_{01}|.$$

(Remember that $\{P_{bf}, 1 - P_{bf}\}$ and $\{P_{pf}, 1 - P_{pf}\}$ are the measurements that Alice and Bob need to perform on their qubit pairs during the Bell test.)

(a) Consider the following two experiments on a two qubit system.

(i) The two qubits are (jointly) measured according to the measurement $\{P_{yes} := P_{bf}, P_{no} := 1 - P_{bf}\}$. Then the qubits are destroyed.

(ii) The two qubits are individually measured in the computational basis $\{|0\rangle, |1\rangle\}$. If the results are equal, output yes, otherwise output no. Then the qubits are destroyed.

Show that both experiments are equivalent. That is, show that for any two-qubit state $\rho \in S(\mathbb{C}^4)$, we have that the probability for getting outcome yes is the same.

(Hint: Let $P_{00}, P_{11}$ be the two projectors corresponding to both measuring 0 and both measuring 1, respectively, in the second experiment. Then the probability of yes in the second experiment is $\text{tr}P_{00}\rho + \text{tr}P_{11}\rho = \text{tr}(P_{00} + P_{11})\rho$.

(b) Consider the following two experiments on a two qubit system.

(i) The two qubits are (jointly) measured according to the measurement $\{P_{yes} := P_{pf}, P_{no} := 1 - P_{pf}\}$. Then the qubits are destroyed.

(ii) The two qubits are individually measured in the diagonal basis $\{|+, -\rangle\}$ with $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. If the results are equal, output yes, otherwise output no. Then the qubits are destroyed.

Show that both experiments are equivalent.

Note that in both cases, experiment (ii) can be implemented even if the two qubits are in different locations and only classical communication is possible between these locations. This allows to replace the Bell test from the lecture by a procedure that can actually be implemented.
Problem 2: Commuting Measurements

Let $\mathcal{H}$ be a Hilbert space and let $|\Psi_1\rangle, \ldots, |\Psi_n\rangle$ be an orthonormal basis of $\mathcal{H}$.

Let $M = \{P_1, \ldots, P_a\}$ and $M' = \{P'_1, \ldots, P'_b\}$ be measurements on $\mathcal{H}$. Assume that each $P_i$ and $P'_i$ is of the form $\sum_j \lambda_j |\Psi_j\rangle\langle\Psi_j|$. (Here the $\lambda_j$ may be different for the different projectors, but the $|\Psi_j\rangle$ are the same for all projectors.)

We will show that it does not matter in which order to apply the measurements $M$ and $M'$ for any density operator $\rho$.

More precisely, consider the following two experiments:

(i) Measure $\rho$ with measurement $M$ and then measure the resulting post-measurement state with measurement $M'$. Let $o$ and $o'$ denote the outcomes of $M$ and $M'$, respectively, and let $\tilde{\rho}$ denote the final post-measurement state.

(ii) Measure $\rho$ with measurement $M'$ and then measure the resulting post-measurement state with measurement $M$. (I.e., the measurements are applied in inverse order.) Let $o$ and $o'$ denote the outcomes of $M$ and $M'$, respectively, and let $\tilde{\rho}'$ denote the final post-measurement state.

Show the following facts:

(a) For all $i, j$ we have $\Pr[o = i \text{ and } o' = j : \text{ experiment (i)}] = \Pr[o = i \text{ and } o' = j : \text{ experiment (ii)}].$

(b) For all $i, j$, we have $\tilde{\rho} = \tilde{\rho}'$ where $\tilde{\rho}$ and $\tilde{\rho}'$ are the post-measurement states in the case of $o = i$ and $o' = j$.

Hint: You may assume without loss of generality that $|\Psi_1\rangle, \ldots, |\Psi_n\rangle$ is the computational basis $|1\rangle, \ldots, |n\rangle$. (Since otherwise one can just do a basis transformation to transform it into that basis.) In that case, all $P_i$ and $P'_i$ will be diagonal.

Problem 3: Alice and Bob are being clever

Alice and Bob had a few clever ideas. In each case, explain why the idea is not a good one.

1. Alice noticed that with a sufficiently strong laser pointer, she can make a beam that is still easily seen on the moon. Since Bob is on a holiday on the moon, they decide to do a key exchange. For this, they take an off-the-shelf QKD protocol (one that only requires that Alice sends randomly polarised photons, and that Bob measures in a random polarisation direction – no quantum computers needed). And as the photon source, Alice uses her laser pointer. That is, she sends short light flashes of the laser pointer through her polarisation filter as specified by the QKD protocol.

2. Alice and Bob want to use some QKD protocol over a long distance (300km). Unfortunately, all QKD protocols and implementations they know of do not manage
to do more than 250 km (because otherwise the error rate on the channel would
become too high). Fortunately, in the middle between Alice and Bob lives Charlie,
an untrusted yet helpful person. To get rid of the errors, they let Charlie work as
an amplifier: Each qubit is sent to Charlie, and Charlie measures the qubit and
resends it using a fresh photon.

3. In a usual QKD protocol Alice would first send the qubits. Then she would wait for
Bob to receive these. Then Alice sends the bases in which she produced the check
qubits (or some other classical information needed for the check/purification/privacy
amplification; this depends on the protocol they use). Alice and Bob decide to
be more efficient and do a “compressed QKD”. Since it is only Alice that sends
something, anyway, she sends all information simultaneously. I.e., she sends the
qubits and the classical information at the same time (over the quantum and the
authenticated classical channel, respectively) and thus achieves at least doubled
throughput.