Problem 1: 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 2: 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 (300 km).
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 pro-
duced 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.

Problem 3: Techniques from the QKD proof

Consider the following (rather useless) protocol. Alice gets a state \( \rho \in S(\mathbb{C}^{2^n}) \) consisting
of \( n \) qubits. Then Alice chooses a random \( i \in \{1, \ldots, n\} \) and measures the \( n \)-th qubit in
\( \rho \) in the computational basis. If this measurement returns 1, Alice aborts. Let \( \tilde{\rho} \) denote
the state that Alice has under the condition that she does not abort. Let \( P_{\text{success}} \) denote
the probability of not aborting.

In the following, by \( T(\rho) \) we denote the density operator \( p\tilde{\rho} \) where \( p \) is the probability
that \( \rho \) passes Alice’s test and \( \tilde{\rho} \) is the state that results after passing Alice’s test. (In
particular, \( \tilde{\rho} = \frac{T(\rho)}{\text{tr}T(\rho)} \) and \( p = \text{tr}T(\rho) \).) For any projector \( P \), we write short \( P(\rho) \) for
\( P\rho P^\dagger \).

Hint: The following proofs use techniques that have appeared in the proof of QKD. However, the present case is somewhat simpler.

(a) Assume that \( \rho = |x\rangle\langle x| \) for some \( x \in \{0, 1\}^n, x \neq 0^n \). Show that \( \rho \) passes Alice’s
test with probability at most \( \delta := \frac{n-1}{n} \).

(b) Assume that \( \rho = \sum_{x \in \{0,1\}^n} p_x |x\rangle\langle x| \) for some \( p_x \geq 0, \sum p_x = 1 \). Let \( P_{\text{ok}} := |0^n\rangle\langle 0^n| \).
Show that \( \text{tr} P_{\text{ok}}(\tilde{\rho}) \geq 1 - \frac{\delta}{P_{\text{success}}} = 1 - \frac{\delta}{\text{tr}T(\rho)} \).
(c) Assume that $\rho \in S(\mathbb{C}^{2^n})$ (arbitrary state). Show that $\mathrm{tr} P_{ok}(\tilde{\rho}) \geq 1 - \frac{\delta}{P_{success}}$.

(d) Show that $\mathrm{TD}(\tilde{\rho}, |0^n\rangle\langle 0^n|) \cdot P_{success} \leq \sqrt{\frac{n-1}{n}}$. 