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: 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 \( i \)-th qubit in \( \rho \) in the computational basis. (The qubit is not discarded after the measurement.) 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 $P_{ok} := |0^n\rangle\langle 0^n|$. Show that $\text{tr} P_{ok}(\tilde{\rho}) \geq 1 - \frac{\delta}{P_{\text{success}}} = 1 - \frac{\delta}{\text{tr} T(\rho)}$.

(c) Assume that $\rho \in S(\mathbb{C}^{2^n})$ (arbitrary state). Show that $\text{tr} P_{ok}(\tilde{\rho}) \geq 1 - \frac{\delta}{P_{\text{success}}}$.

**Hint:** Consider a complete measurement in the computational basis, and use the fact that it commutes with other measurements in the computational basis.

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