University of Oslo

FYS3415/FYS4415 — Quantum computing and quantum information

Problem set 4

This problem set will be discussed on **Feb. 18**.

Problem 1: Types of Quantum Measurements

There are three related but distinct frameworks for describing quantum measurements:

1. **General measurements (measurement operators):** Described by operators $\{M_m\}$ satisfying completeness $\sum_m M_m^\dagger M_m = \mathbb{1}$. This description includes a state-update rule.
2. **Projective measurements:** A special case where $M_m = P_m$ are orthogonal projectors satisfying $P_m P_{m'} = \delta_{mm'} P_m$.
3. **POVM (Positive Operator-Valued Measure):** Described by positive operators $\{E_m\}$ with $\sum_m E_m = \mathbb{1}$. A POVM fixes the outcome probabilities but does not, in general, uniquely determine the post-measurement state.

In this problem, you will practice moving between these descriptions and see why a POVM does *not* uniquely specify the full physical measurement process.

a) Consider the following two measurement operators on a single qubit, parameterized by $0 < \eta < 1$:

$$M_0 = \sqrt{\eta}\ |0\rangle\langle 0|, \qquad M_1 = \sqrt{1-\eta}\ |0\rangle\langle 0| + |1\rangle\langle 1|.$$

i) Verify that the completeness relation holds for these two operators.

ii) Compute the POVM elements E_m corresponding to M_m and show that E_0 is *not* a projector.

iii) For the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\eta = 1/2$, compute the probability and post-measurement state for each outcome.

Solution:

i) Compute each term:

$$M_0^\dagger M_0 = \eta\ |0\rangle\langle 0|, \qquad M_1^\dagger M_1 = (1-\eta)\ |0\rangle\langle 0| + |1\rangle\langle 1|.$$

Summing:

$$M_0^\dagger M_0 + M_1^\dagger M_1 = \big(\eta + (1-\eta)\big)\ |0\rangle\langle 0| + |1\rangle\langle 1| = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{1}.$$

ii) The POVM elements are:

$$E_0 = M_0^\dagger M_0 = \eta\ |0\rangle\langle 0|, \qquad E_1 = M_1^\dagger M_1 = (1-\eta)\ |0\rangle\langle 0| + |1\rangle\langle 1|.$$

Check idempotency:

$$E_0^2 = \eta^2\ |0\rangle\langle 0| \neq \eta\ |0\rangle\langle 0| = E_0 \quad (\text{since } 0 < \eta < 1).$$

So E_0 is **not** a projector.

iii) With $\eta = 1/2$ and $|+\rangle$:

Outcome 0:

$$p(0) = \langle +|E_0|+\rangle = \frac{1}{2}\,|\langle 0|+\rangle|^2 = \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}.$$

The (normalized) post-measurement state is

$$|\psi_0\rangle = \frac{M_0\,|+\rangle}{\sqrt{p(0)}} = \frac{\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}}\,|0\rangle}{1/2} = |0\rangle.$$

Outcome 1: $p(1) = 1 - p(0) = \frac{3}{4}$.

$$M_1\,|+\rangle = \Big(\frac{1}{\sqrt{2}}\,|0\rangle\langle 0| + |1\rangle\langle 1|\Big)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle.$$

normalizing:

$$|\psi_1\rangle = \frac{M_1\,|+\rangle}{\sqrt{3/4}} = \frac{1}{\sqrt{3}}\,|0\rangle + \sqrt{\frac{2}{3}}\,|1\rangle.$$

b) Suppose $\{M_m\}$ is a set of measurement operators with POVM elements $E_m = M_m^\dagger M_m$. Define new measurement operators $M'_m = U_m M_m$ where each U_m is a unitary operator (possibly depending on m).

- **i)** Show that the POVM elements $E'_m = (M'_m)^\dagger M'_m$ are identical to E_m.
- **ii)** Let $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$ (computational basis projectors), and choose $U_0 = H$ and $U_1 = \mathbb{1}$. For the state $|+\rangle$, compute the post-measurement state for outcome 0 using both $\{M_m\}$ and $\{M'_m\}$. Verify that the probability of outcome 0 is the same in both cases.
- **iii)** In 2–4 sentences: explain why the POVM $\{E_m\}$ does *not* uniquely determine the full physical measurement process. What extra information is contained in the measurement operators $\{M_m\}$?

Solution:

i) Compute directly:

$$E'_m = (M'_m)^\dagger M'_m = (U_m M_m)^\dagger (U_m M_m) = M_m^\dagger U_m^\dagger U_m M_m = M_m^\dagger M_m = E_m.$$

ii) For $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

Original measurement $\{M_m\}$:

$$p(0) = \langle +|M_0^\dagger M_0\,|+\rangle = |\langle 0|+\rangle|^2 = \frac{1}{2}, \qquad |\psi_0\rangle = \frac{M_0\,|+\rangle}{\sqrt{p(0)}} = |0\rangle.$$

Modified measurement $\{M'_m\}$: Here $M'_0 = U_0 M_0 = H\,|0\rangle\langle 0| = |+\rangle\langle 0|$. Then

$$p'(0) = \langle +|(M'_0)^\dagger M'_0\,|+\rangle = |\langle 0|+\rangle|^2 = \frac{1}{2},$$

so the probability is the same. The post-measurement state is

$$|\psi_0'\rangle = \frac{M_0'|+\rangle}{\sqrt{p'(0)}} = \frac{H|0\rangle\langle 0|+\rangle}{1/\sqrt{2}} = |+\rangle.$$

iii) The POVM elements E_m determine only the outcome probabilities via $p(m) = \langle\psi|E_m|\psi\rangle$. The measurement operators M_m determine the *post-measurement state* $|\psi_m\rangle = M_m|\psi\rangle/\sqrt{p(m)}$. Different physical implementations (different $\{M_m\}$) can have the same POVM $\{E_m\}$ but disturb the system in different ways.

Problem 2: Unambiguous State Discrimination

In *unambiguous state discrimination* (USD), we are given an unknown state drawn from a known set $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ and must identify it with **zero error**, at the cost of sometimes returning an "inconclusive" outcome. Formally, a USD POVM $\{E_1, \ldots, E_n, E_?\}$ satisfies $\langle\psi_j|E_k|\psi_j\rangle = 0$ for all $j \neq k$: if outcome k occurs, then the state was definitely $|\psi_k\rangle$ (but if outcome ? occurs, the measurement is inconclusive).

a) Suppose there exists a USD POVM $\{E_1, \ldots, E_n, E_?\}$ for pure states $|\psi_1\rangle, \ldots, |\psi_n\rangle \in \mathbb{C}^d$ such that each state can be identified with nonzero probability, i.e. $\langle\psi_k|E_k|\psi_k\rangle > 0$ for all k. Show that the states must be linearly independent. Conclude that USD is possible only if $n \leq d$. Hint[1].

Solution: Since $E_k \geq 0$, we have a square root $\sqrt{E_k}$, and

$$\langle\psi_j|E_k|\psi_j\rangle = \|\sqrt{E_k}|\psi_j\rangle\|^2.$$

Thus the zero-error condition $\langle\psi_j|E_k|\psi_j\rangle = 0$ for $j \neq k$ implies $E_k|\psi_j\rangle = \sqrt{E_k}\sqrt{E_k}|\psi_j\rangle = 0$ for $j \neq k$.

Now suppose (for contradiction) that the states are linearly dependent. Then for some k we can write

$$|\psi_k\rangle = \sum_{j\neq k} c_j|\psi_j\rangle.$$

Applying E_k and using $E_k|\psi_j\rangle = 0$ for $j \neq k$ gives $E_k|\psi_k\rangle = 0$, hence

$$p(k|\psi_k) = \langle\psi_k|E_k|\psi_k\rangle = 0,$$

contradicting the assumption that $\langle\psi_k|E_k|\psi_k\rangle > 0$. Therefore the states must be linearly independent, and in $\mathbb{C}^d$ this implies $n \leq d$.

b) Consider the following three two-qubit states in $\mathbb{C}^4$:

$$|\psi_1\rangle = |00\rangle, \qquad |\psi_2\rangle = |0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle), \qquad |\psi_3\rangle = |++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

i) Verify that $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ is linearly independent.

ii) Verify that the states are pairwise non-orthogonal by computing the overlaps $\langle\psi_i|\psi_j\rangle$ for $i \neq j$.

[1] If the states were linearly dependent, write one state as a linear combination of the others and apply the corresponding detection operator E_k. Use that for $E_k \geq 0$, the condition $\langle\psi_j|E_k|\psi_j\rangle = 0$ implies $E_k|\psi_j\rangle = 0$.

iii) For each $k \in \{1,2,3\}$, find a normalized detection vector $|\tilde{\psi}_k\rangle \in \mathbb{C}^4$ such that

$$\langle\psi_j|\tilde{\psi}_k\rangle = 0 \quad \text{for all } j \neq k, \qquad \text{and} \qquad \langle\psi_k|\tilde{\psi}_k\rangle \neq 0.$$

Hint[2].

iv) For your chosen detection vectors, compute the three nonzero overlaps $\langle\psi_k|\tilde{\psi}_k\rangle$.

Solution:

i) Write the states as columns in the $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ basis:

$$\begin{pmatrix} 1 & 1/\sqrt{2} & 1/2 \\ 0 & 1/\sqrt{2} & 1/2 \\ 0 & 0 & 1/2 \\ 0 & 0 & 1/2 \end{pmatrix}.$$

The first three rows form an upper-triangular 3×3 matrix with nonzero diagonal entries, so the columns are linearly independent.

ii) Compute overlaps:

$$\begin{aligned} \langle\psi_1|\psi_2\rangle &= \langle 00|0+\rangle = \langle 0|0\rangle\langle 0|+\rangle = \tfrac{1}{\sqrt{2}}, \\ \langle\psi_1|\psi_3\rangle &= \langle 00|++\rangle = \langle 0|+\rangle^2 = \tfrac{1}{2}, \\ \langle\psi_2|\psi_3\rangle &= \langle 0+|++\rangle = \langle 0|+\rangle\langle +|+\rangle = \tfrac{1}{\sqrt{2}}. \end{aligned}$$

All are nonzero.

iii) One convenient choice of normalized detection vectors is:

$$|\tilde{\psi}_1\rangle = |0-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle), \qquad |\tilde{\psi}_2\rangle = |-1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle), \qquad |\tilde{\psi}_3\rangle = |10\rangle.$$

Check the "zero-error" overlaps for $j \neq k$:

$$\begin{aligned} &\langle\psi_2|\tilde{\psi}_1\rangle = \langle 0+|0-\rangle = \langle 0|0\rangle\langle +|-\rangle = 0, && \langle\psi_3|\tilde{\psi}_1\rangle = \langle ++|0-\rangle = \langle +|0\rangle\langle +|-\rangle = 0, \\ &\langle\psi_1|\tilde{\psi}_2\rangle = \langle 00|-1\rangle = \langle 0|-\rangle\langle 0|1\rangle = 0, && \langle\psi_3|\tilde{\psi}_2\rangle = \langle ++|-1\rangle = \langle +|-\rangle\langle +|1\rangle = 0, \\ &\langle\psi_1|\tilde{\psi}_3\rangle = \langle 00|10\rangle = 0, && \langle\psi_2|\tilde{\psi}_3\rangle = \langle 0+|10\rangle = \langle 0|1\rangle\langle +|0\rangle = 0. \end{aligned}$$

And each detection vector has nonzero overlap with its intended state.

iv) The nonzero overlaps are:

$$\begin{aligned} \langle\psi_1|\tilde{\psi}_1\rangle &= \langle 00|0-\rangle = \tfrac{1}{\sqrt{2}}, \\ \langle\psi_2|\tilde{\psi}_2\rangle &= \langle 0+|-1\rangle = \langle 0|-\rangle\langle +|1\rangle = \tfrac{1}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}} = \tfrac{1}{2}, \\ \langle\psi_3|\tilde{\psi}_3\rangle &= \langle ++|10\rangle = \tfrac{1}{2}. \end{aligned}$$

[2] Use product structure when possible. For $|\tilde{\psi}_1\rangle$, both $|\psi_2\rangle$ and $|\psi_3\rangle$ have $|+\rangle$ on the second qubit, so choosing $|-\rangle$ there makes $|\tilde{\psi}_1\rangle$ orthogonal to both. For $|\tilde{\psi}_3\rangle$, both $|\psi_1\rangle$ and $|\psi_2\rangle$ have $|0\rangle$ on the first qubit, so choosing $|1\rangle$ there makes $|\tilde{\psi}_3\rangle$ orthogonal to both.

Clarification added after the sheet was released. In part **b)**, the detection vectors are not unique. For the next part, however, the calculation depends on a concrete choice. Therefore, from this point on, please use

$$|\tilde{\psi}_1\rangle = |0-\rangle, \qquad |\tilde{\psi}_2\rangle = |-1\rangle, \qquad |\tilde{\psi}_3\rangle = |10\rangle.$$

If you solved part **b)** using different valid vectors, that is perfectly fine, just switch to the above choice from here on.

c) Define the POVM

$$E_1 = \frac{1}{2}\,|\tilde{\psi}_1\rangle\langle\tilde{\psi}_1|, \qquad E_2 = \frac{1}{2}\,|\tilde{\psi}_2\rangle\langle\tilde{\psi}_2|, \qquad E_3 = \frac{1}{2}\,|\tilde{\psi}_3\rangle\langle\tilde{\psi}_3|, \qquad E_? = \mathbb{1} - E_1 - E_2 - E_3.$$

i) Verify that $E_? \geq 0$ (so this is a valid POVM) by checking that all eigenvalues of $E_?$ are nonnegative. You may compute the eigenvalues analytically, or compute them with a computer. Hint[3].

ii) Compute the probability of successfully identifying each state, i.e. $p(1|\psi_1)$, $p(2|\psi_2)$, $p(3|\psi_3)$.

iii) Assuming equal prior probabilities $1/3$, compute the overall success probability p_{succ} and the inconclusive probability $p_? = 1 - p_{\text{succ}}$.

Solution:

i) In the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, one finds

$$E_? = \begin{pmatrix} 3/4 & 1/4 & 0 & 0 \\ 1/4 & 1/2 & 0 & 1/4 \\ 0 & 0 & 1/2 & 0 \\ 0 & 1/4 & 0 & 3/4 \end{pmatrix}.$$

The state $|10\rangle$ is an eigenvector with eigenvalue $1/2$. On the $\{|00\rangle, |01\rangle, |11\rangle\}$ block, convenient (unnormalized) eigenvectors are

$$|00\rangle - |11\rangle, \qquad |00\rangle + |01\rangle + |11\rangle, \qquad |00\rangle - 2\,|01\rangle + |11\rangle,$$

with eigenvalues $3/4$, 1, and $1/4$, respectively. Hence the eigenvalues of $E_?$ are

$$\{\,1,\ 3/4,\ 1/2,\ 1/4\,\},$$

all nonnegative, so $E_? \geq 0$.

ii) Since $E_k = \frac{1}{2}\,|\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|$,

$$p(k|\psi_k) = \langle\psi_k|E_k\,|\psi_k\rangle = \frac{1}{2}\,|\langle\psi_k|\tilde{\psi}_k\rangle|^2.$$

[3] If you want to do it analytically, write $E_?$ as a 4×4 matrix in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. The $|10\rangle$ row/column decouples, so one eigenvalue is immediate. For the remaining 3×3 block on $\{|00\rangle, |01\rangle, |11\rangle\}$, note the symmetry under swapping $|00\rangle \leftrightarrow |11\rangle$: the antisymmetric vector $|00\rangle - |11\rangle$ is an eigenvector. Then restrict to the symmetric subspace spanned by $|00\rangle + |11\rangle$ and $|01\rangle$ to find the two remaining eigenvalues.

Using the overlaps:

$$p(1|\psi_1) = \tfrac{1}{2} \cdot \left|\tfrac{1}{\sqrt{2}}\right|^2 = \tfrac{1}{4},$$
$$p(2|\psi_2) = \tfrac{1}{2} \cdot \left|\tfrac{1}{2}\right|^2 = \tfrac{1}{8},$$
$$p(3|\psi_3) = \tfrac{1}{2} \cdot \left|\tfrac{1}{2}\right|^2 = \tfrac{1}{8}.$$

iii) With equal priors 1/3,

$$p_{\text{succ}} = \frac{1}{3}\Big(\frac{1}{4} + \frac{1}{8} + \frac{1}{8}\Big) = \frac{1}{3} \cdot \frac{1}{2} = \frac{1}{6}, \qquad p_? = 1 - p_{\text{succ}} = \frac{5}{6}.$$

Problem 3: Density Operators and Ensemble Decompositions

A *density operator* (or *density matrix*) is used to describe quantum states when there is classical uncertainty about which pure state was prepared, or when we only care about measurement statistics. If a source prepares $|\psi_i\rangle$ with probability p_i, the corresponding density operator is

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i|.$$

A key point is that the same density operator can arise from *many different ensembles* of pure states. In this problem you will see the difference between superposition and mixture, practice computing probabilities from ρ, and prove the "unitary freedom" in ensemble decompositions.

a) Superposition vs. mixture. Consider the pure state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and the mixed state

$$\rho_{\text{mix}} = \frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big).$$

i) Write the density matrix $\rho_+ = |+\rangle\langle +|$ in the computational basis, and write ρ_{mix} in the same basis. What is the key difference between the two matrices?

ii) Compute the measurement statistics $p(0)$ and $p(1)$ when measuring in the computational (Z) basis, for both ρ_+ and ρ_{mix}. For ρ_{mix}, you may compute by averaging the Born-rule probabilities over a chosen ensemble decomposition (e.g. the one displayed above).

iii) Design a quantum circuit that produces different computational-basis measurement statistics for ρ_+ and ρ_{mix}. Compute the two resulting probability distributions. For ρ_{mix}, you may propagate the states in a chosen ensemble decomposition through your circuit and then average the measurement statistics.

iv) In 2–3 sentences: explain why part iii) works (what feature does ρ_+ have that ρ_{mix} lacks?).

Solution:

i) We compute

$$\rho_+ = |+\rangle\langle +| = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) = \frac{1}{2}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\Big).$$

In the $\{|0\rangle, |1\rangle\}$ basis this is

$$\rho_+ = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \rho_{\text{mix}} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}\mathbb{1}.$$

Key difference: ρ_+ has *off-diagonal* terms (coherences), while ρ_{mix} does not.

ii) For ρ_+ we have the pure state $|+\rangle$, so measuring in the Z basis gives

$$p(0) = |\langle 0|+\rangle|^2 = \frac{1}{2}, \qquad p(1) = |\langle 1|+\rangle|^2 = \frac{1}{2}.$$

For ρ_{mix}, use the decomposition displayed in the problem statement (one convenient choice). Conditioning on which pure state was prepared and averaging,

$$p(0) = \tfrac{1}{2}\,|\langle 0|0\rangle|^2 + \tfrac{1}{2}\,|\langle 0|1\rangle|^2 = \tfrac{1}{2}, \qquad p(1) = \tfrac{1}{2}\,|\langle 1|0\rangle|^2 + \tfrac{1}{2}\,|\langle 1|1\rangle|^2 = \tfrac{1}{2}.$$

(Any other ensemble decomposition of the same ρ_{mix} would give the same measurement statistics.)

iii) A simple circuit is: apply H and then measure in the computational basis.

For ρ_+ (pure state): $H\,|+\rangle = |0\rangle$, so the measurement outcome is 0 with probability 1.

For ρ_{mix}, use the same convenient ensemble decomposition as above. Propagate each branch through H:

$$|0\rangle \overset{H}{\longmapsto} |+\rangle, \qquad |1\rangle \overset{H}{\longmapsto} |-\rangle.$$

Measuring $|+\rangle$ or $|-\rangle$ in the Z basis gives $p(0) = p(1) = 1/2$ in either case. Averaging over the two branches, the overall distribution is $p(0) = p(1) = 1/2$.

iv) The pure state ρ_+ contains coherence between $|0\rangle$ and $|1\rangle$ (off-diagonal terms in the Z basis), which a basis change (the Hadamard) can convert into a population difference. In contrast, ρ_{mix} describes classical uncertainty with no definite relative phase; under H the two branches $|0\rangle$ and $|1\rangle$ become $|+\rangle$ and $|-\rangle$, each of which gives 50/50 outcomes in the Z basis, so the averaged statistics remain uniform.

b) Measurement probabilities from ρ. Suppose a source prepares $|\psi_i\rangle$ with probability p_i, so $\rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|$. Let $\{E_m\}$ be a POVM.

i) Starting from the definition of ρ, show that the probability of outcome m is

$$p(m) = \sum_i p_i\,\langle\psi_i|E_m\,|\psi_i\rangle.$$

ii) Show that this can be written compactly as

$$p(m) = \mathrm{Tr}(E_m\rho).$$

Solution:

i) If the state is $|\psi_i\rangle$, the Born rule for a POVM gives $p(m|\psi_i) = \langle\psi_i|E_m\,|\psi_i\rangle$. Averaging over the classical uncertainty (law of total probability):

$$p(m) = \sum_i p_i\,p(m|\psi_i) = \sum_i p_i\,\langle\psi_i|E_m\,|\psi_i\rangle.$$

ii) Using $\rho = \sum_i p_i \,|\psi_i\rangle\langle\psi_i|$ and linearity of trace:

$$\mathrm{Tr}(E_m\rho) = \mathrm{Tr}\Big(E_m \sum_i p_i \,|\psi_i\rangle\langle\psi_i|\Big) = \sum_i p_i \;\mathrm{Tr}\big(E_m \,|\psi_i\rangle\langle\psi_i|\big) = \sum_i p_i \,\langle\psi_i|E_m\,|\psi_i\rangle.$$

Thus $p(m) = \mathrm{Tr}(E_m\rho)$.

c) Unitary freedom in ensemble decompositions (equal lengths). Let ρ be a density operator on a d-dimensional Hilbert space with spectral decomposition

$$\rho = \sum_{k=1}^{r} \lambda_k \,|k\rangle\langle k|, \qquad \lambda_k > 0,$$

where $r = \mathrm{rank}(\rho)$. Suppose ρ can be written as *two* ensembles of the *same length* n:

$$\rho = \sum_{i=1}^{n} p_i \,|\psi_i\rangle\langle\psi_i| = \sum_{i=1}^{n} q_i \,|\phi_i\rangle\langle\phi_i|, \qquad p_i, q_i \geq 0.$$

Define the unnormalized kets $|\tilde{\psi}_i\rangle = \sqrt{p_i}\,|\psi_i\rangle$ and $|\tilde{\phi}_i\rangle = \sqrt{q_i}\,|\phi_i\rangle$ so that $\rho = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_i |\tilde{\phi}_i\rangle\langle\tilde{\phi}_i|$.

i) Show that each $|\tilde{\psi}_i\rangle$ lies in the support of ρ, i.e. it is in $(\ker\rho)^\perp$. Show that this means that each $|\tilde{\psi}_i\rangle$ can be expanded as

$$|\tilde{\psi}_i\rangle = \sum_{k=1}^{r} \sqrt{\lambda_k}\, a_{ki}\,|k\rangle$$

for some coefficients a_{ki}. Define the $r \times n$ matrix $A = (a_{ki})$. Do the same for the other ensemble, defining $B = (b_{ki})$ via $|\tilde{\phi}_i\rangle = \sum_{k=1}^{r} \sqrt{\lambda_k}\, b_{ki}\,|k\rangle$.

ii) Show that $AA^\dagger = \mathbb{1}_r$ and $BB^\dagger = \mathbb{1}_r$. (Interpret this as: the r rows of A (and of B) form an orthonormal set of vectors in $\mathbb{C}^n$.)

iii) Argue that there exists an $n \times n$ unitary matrix U such that

$$B = AU.$$

(You may use the fact that any orthonormal set can be extended to an orthonormal basis.)

iv) Translate $B = AU$ into a relation between the ensembles: show that for each i,

$$|\tilde{\phi}_i\rangle = \sum_{j=1}^{n} U_{ji}\,|\tilde{\psi}_j\rangle.$$

v) Prove the converse direction (the easy direction): if $|\tilde{\phi}_i\rangle = \sum_j U_{ji}\,|\tilde{\psi}_j\rangle$ for a unitary U, then the two ensembles generate the same ρ.

Hint[4].

[4] For i), if $|x\rangle$ is orthogonal to the support of ρ then $0 = \langle x|\rho\,|x\rangle = \sum_i |\langle x|\tilde{\psi}_i\rangle|^2$, so each $\langle x|\tilde{\psi}_i\rangle = 0$. For ii), compute matrix elements $\langle k|\rho\,|\ell\rangle$ in the eigenbasis. For iii), view the rows of A and B as orthonormal vectors in $\mathbb{C}^n$, extend each set to a full orthonormal basis, and define U to map one basis to the other.

Solution:

i) Let $|x\rangle$ be orthogonal to the support of ρ. Then $\rho\,|x\rangle = 0$, so

$$0 = \langle x|\rho\,|x\rangle = \sum_{i=1}^{n} \langle x|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|x\rangle = \sum_{i=1}^{n} |\langle x|\tilde{\psi}_i\rangle|^2.$$

Hence $\langle x|\tilde{\psi}_i\rangle = 0$ for all i, meaning that $|\tilde{\psi}_i\rangle$ must be in the support of ρ. Furthermore, each $|\tilde{\psi}_i\rangle$ lies in the span of $\{|k\rangle\}_{k=1}^{r}$. The same argument applies to $|\tilde{\phi}_i\rangle$.

ii) Using $\rho = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$ and the expansion $|\tilde{\psi}_i\rangle = \sum_k \sqrt{\lambda_k}\, a_{ki}\,|k\rangle$, we get

$$\rho = \sum_{i=1}^{n} \sum_{k,\ell=1}^{r} \sqrt{\lambda_k \lambda_\ell}\, a_{ki} a_{\ell i}^{*}\; |k\rangle\langle\ell|.$$

Taking matrix elements and comparing with $\langle k|\rho\,|\ell\rangle = \lambda_k \delta_{k\ell}$ gives

$$\sum_{i=1}^{n} a_{ki} a_{\ell i}^{*} = \delta_{k\ell},$$

i.e. $AA^\dagger = \mathbb{1}_r$. Similarly, $BB^\dagger = \mathbb{1}_r$.

iii) The rows of A and B are orthonormal vectors in $\mathbb{C}^n$. Extend each to a full orthonormal basis of $\mathbb{C}^n$ and define U to be the unitary that maps the extended basis associated with A to the one associated with B. Then $B = AU$.

iv) From $B = AU$, comparing columns and reconstructing the vectors gives

$$|\tilde{\phi}_i\rangle = \sum_{j=1}^{n} U_{ji}\,|\tilde{\psi}_j\rangle.$$

v) Conversely, if $|\tilde{\phi}_i\rangle = \sum_j U_{ji}\,|\tilde{\psi}_j\rangle$ with U unitary, then

$$\sum_i |\tilde{\phi}_i\rangle\langle\tilde{\phi}_i| = \sum_{j,\ell} \Big(\sum_i U_{ji} U_{\ell i}^{*}\Big)\, |\tilde{\psi}_j\rangle\langle\tilde{\psi}_\ell| = \sum_j |\tilde{\psi}_j\rangle\langle\tilde{\psi}_j| = \rho,$$

using $\sum_i U_{ji} U_{\ell i}^{*} = (UU^\dagger)_{j\ell} = \delta_{j\ell}$.

d) Different ensemble lengths (padding with zero-probability states). Suppose ρ has two decompositions of *different* lengths:

$$\rho = \sum_{j=1}^{n} |\tilde{\psi}_j\rangle\langle\tilde{\psi}_j| = \sum_{\mu=1}^{m} |\tilde{\phi}_\mu\rangle\langle\tilde{\phi}_\mu|, \qquad m \neq n.$$

Without loss of generality, assume $n > m$.

i) Define padded vectors $|\tilde{\phi}_{m+1}\rangle = \cdots = |\tilde{\phi}_n\rangle = 0$ and argue that

$$\rho = \sum_{\mu=1}^{n} |\tilde{\phi}_\mu\rangle\langle\tilde{\phi}_\mu|$$

still holds.

ii) Apply the previous task (equal lengths) to conclude that there exists an $n \times n$ unitary U such that, for all $\mu = 1, \ldots, n$,

$$|\tilde{\phi}_\mu\rangle = \sum_{j=1}^{n} U_{j\mu} \, |\tilde{\psi}_j\rangle.$$

iii) Restrict to $\mu = 1, \ldots, m$ (the original, non-padded ensemble). Let u be the $n \times m$ matrix consisting of the first m columns of U. Show that

$$|\tilde{\phi}_\mu\rangle = \sum_{j=1}^{n} u_{j\mu} \, |\tilde{\psi}_j\rangle \quad (\mu = 1, \ldots, m) \qquad \text{and} \qquad u^\dagger u = \mathbb{1}_m.$$

Solution:

i) If $|\tilde{\phi}_\mu\rangle = 0$ then $|\tilde{\phi}_\mu\rangle\langle\tilde{\phi}_\mu| = 0$, so padding adds zero operators:

$$\sum_{\mu=1}^{n} |\tilde{\phi}_\mu\rangle\langle\tilde{\phi}_\mu| = \sum_{\mu=1}^{m} |\tilde{\phi}_\mu\rangle\langle\tilde{\phi}_\mu| + \sum_{\mu=m+1}^{n} 0 = \rho.$$

ii) Now both decompositions have length n, so by the previous task there exists an $n \times n$ unitary U such that $|\tilde{\phi}_\mu\rangle = \sum_{j=1}^{n} U_{j\mu} \, |\tilde{\psi}_j\rangle$ for all $\mu = 1, \ldots, n$.

iii) Restricting to $\mu = 1, \ldots, m$ gives

$$|\tilde{\phi}_\mu\rangle = \sum_{j=1}^{n} U_{j\mu} \, |\tilde{\psi}_j\rangle = \sum_{j=1}^{n} u_{j\mu} \, |\tilde{\psi}_j\rangle.$$

Since U is unitary, its columns are orthonormal, so for $\mu, \nu \leq m$,

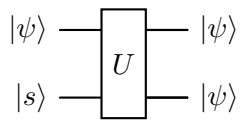
$$(u^\dagger u)_{\mu\nu} = \sum_{j=1}^{n} u^*_{j\mu} u_{j\nu} = \sum_{j=1}^{n} U^*_{j\mu} U_{j\nu} = (U^\dagger U)_{\mu\nu} = \delta_{\mu\nu}.$$

Hence $u^\dagger u = \mathbb{1}_m$.

Remark (formal viewpoint): The rectangular matrix u is an *isometry* (it preserves inner products on $\mathbb{C}^m$). Padding corresponds to extending an isometry to a full unitary by completing an orthonormal set of vectors to an orthonormal basis (e.g. via Gram–Schmidt).

Problem 4: The No-Cloning Theorem

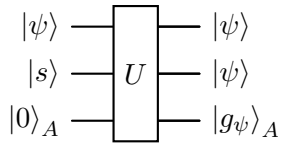
A *quantum cloning machine* is a unitary operator U that copies an unknown quantum state $|\psi\rangle$ into a blank register initially in state $|s\rangle$:



i.e., $\qquad U\big(|\psi\rangle \otimes |s\rangle\big) = |\psi\rangle \otimes |\psi\rangle.$

As shown in the lectures, the inner-product argument gives $\langle\psi|\phi\rangle = \big(\langle\psi|\phi\rangle\big)^2$, which only has solutions $\langle\psi|\phi\rangle \in \{0, 1\}$, proving that a universal cloning machine is impossible.

a) Cloning with ancilla ("garbage"). One might try to circumvent the no-cloning theorem by allowing the cloning machine to produce a state-dependent "garbage" output on an ancilla system:



i.e., $\quad U\big(|\psi\rangle \otimes |s\rangle \otimes |0\rangle_A\big) = |\psi\rangle \otimes |\psi\rangle \otimes |g_\psi\rangle_A,$

where $|g_\psi\rangle_A$ is an arbitrary state on the ancilla that may depend on $|\psi\rangle$.

i) Repeat the inner product argument and show that the constraint becomes

$$\langle\psi|\phi\rangle = \big(\langle\psi|\phi\rangle\big)^2 \langle g_\psi|g_\phi\rangle_A.$$

ii) Using $|\langle g_\psi|g_\phi\rangle_A| \leq 1$, show that the ancilla does not help: cloning of non-orthogonal states is still impossible. Hint[5].

Solution:

i) Suppose the machine clones both $|\psi\rangle$ and $|\phi\rangle$:

$$|\psi\rangle\,|s\rangle\,|0\rangle_A \overset{U}{\longmapsto} |\psi\rangle\,|\psi\rangle\,|g_\psi\rangle_A,$$
$$|\phi\rangle\,|s\rangle\,|0\rangle_A \overset{U}{\longmapsto} |\phi\rangle\,|\phi\rangle\,|g_\phi\rangle_A.$$

Taking the inner product, the left-hand side gives

$$\langle\psi|\phi\rangle \cdot \langle s|s\rangle \cdot \langle 0|0\rangle_A = \langle\psi|\phi\rangle,$$

and the right-hand side gives

$$\langle\psi|\phi\rangle \cdot \langle\psi|\phi\rangle \cdot \langle g_\psi|g_\phi\rangle_A = \big(\langle\psi|\phi\rangle\big)^2 \langle g_\psi|g_\phi\rangle_A.$$

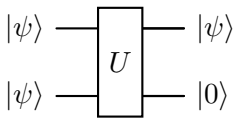
Equating them yields the stated constraint.

ii) Taking absolute values and using $|\langle g_\psi|g_\phi\rangle_A| \leq 1$:

$$|\langle\psi|\phi\rangle| = |\langle\psi|\phi\rangle|^2\,|\langle g_\psi|g_\phi\rangle_A| \leq |\langle\psi|\phi\rangle|^2.$$

Let $t = |\langle\psi|\phi\rangle| \in [0,1]$. Then $t \leq t^2$ implies $t(1-t) \leq 0$, hence $t \in \{0,1\}$. Therefore non-orthogonal, distinct states ($0 < t < 1$) cannot be cloned even with an ancilla producing arbitrary garbage.

b) The no-deleting theorem. Suppose a "quantum deleting machine" is a unitary U that, given two copies of an unknown state, erases one copy and returns a blank:



i.e., $\quad U\big(|\psi\rangle \otimes |\psi\rangle\big) = |\psi\rangle \otimes |0\rangle.$

i) Use the inner product argument (as in the no-cloning proof) to derive a constraint on $\langle\psi|\phi\rangle$.

[5] Take absolute values and set $t = |\langle\psi|\phi\rangle| \in [0,1]$.

ii) Conclude that a universal quantum deleting machine is impossible.

iii) In 2–4 sentences: what is the connection between no-deleting and no-cloning?

Hint[6].

Solution:

i) Suppose U deletes both $|\psi\rangle$ and $|\phi\rangle$:

$$U\big(|\psi\rangle\,|\psi\rangle\big) = |\psi\rangle\,|0\rangle,$$
$$U\big(|\phi\rangle\,|\phi\rangle\big) = |\phi\rangle\,|0\rangle.$$

Taking the inner product, the left-hand side gives

$$(\langle\psi|\otimes\langle\psi|)(|\phi\rangle\otimes|\phi\rangle) = \langle\psi|\phi\rangle^2,$$

while the right-hand side gives

$$(\langle\psi|\otimes\langle 0|)(|\phi\rangle\otimes|0\rangle) = \langle\psi|\phi\rangle.$$

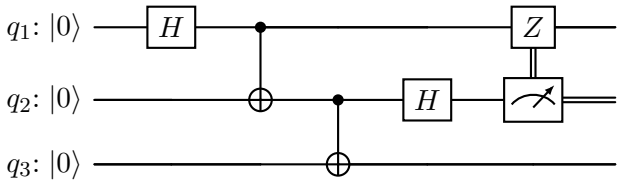
Hence $\langle\psi|\phi\rangle^2 = \langle\psi|\phi\rangle$.

ii) The only solutions are $\langle\psi|\phi\rangle \in \{0,1\}$, so a universal deleting machine cannot work on non-orthogonal, distinct states. Universal quantum deletion is therefore impossible.

iii) No-cloning and no-deleting are "dual" impossibility results for unitary evolution. If a unitary U could delete one of two copies, then running the inverse unitary $U^\dagger$ would *create* a second copy from a single copy plus a blank state — i.e. it would act like a cloning operation. Since universal cloning is impossible, universal deleting is impossible as well.

Problem 5: Multi-Qubit Circuit Analysis

Consider the following three-qubit circuit. The input state is $|000\rangle$.



The meter on q_2 denotes a mid-circuit measurement in the computational basis with outcome $m \in \{0,1\}$. The double classical wire indicates that the measurement result is sent forward classically. The Z gate on q_1 is applied *only if* $m = 1$ (classical feed-forward / classically controlled gate).

a) Compute the three-qubit state $|\Psi\rangle$ *just before* the measurement of q_2, i.e. after applying H, CNOT$(q_1 \mapsto q_2)$, CNOT$(q_2 \mapsto q_3)$, and H on q_2. Use the standard ordering $|q_1 q_2 q_3\rangle$.

[6] For i), assume U deletes for two states $|\psi\rangle$ and $|\phi\rangle$ and take the inner product of the two equations. For iii), think about reversibility.

Solution: Step-by-step:

1. H on q_1:
$$|000\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|00\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle).$$

2. CNOT($q_1 \to q_2$):
$$\frac{1}{\sqrt{2}}(|000\rangle + |110\rangle).$$

3. CNOT($q_2 \to q_3$):
$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

4. H on q_2:
$$\begin{aligned}|\Psi\rangle &= \frac{1}{\sqrt{2}}\Big(|0\rangle\,|+\rangle\,|0\rangle + |1\rangle\,|-\rangle\,|1\rangle\Big) \\ &= \frac{1}{2}\Big(|000\rangle + |010\rangle + |101\rangle - |111\rangle\Big).\end{aligned}$$

b) Rewrite $|\Psi\rangle$ in the reordered form

$$|\Psi\rangle = |0\rangle_{q_2}\,|\phi_0\rangle_{q_1q_3} + |1\rangle_{q_2}\,|\phi_1\rangle_{q_1q_3},$$

i.e. group terms by the state of q_2. What are the *unnormalized* states $|\phi_0\rangle$ and $|\phi_1\rangle$?

Solution: Grouping by q_2:

$$|\Psi\rangle = |0\rangle_{q_2}\,\frac{1}{2}\big(|00\rangle + |11\rangle\big)_{q_1q_3} + |1\rangle_{q_2}\,\frac{1}{2}\big(|00\rangle - |11\rangle\big)_{q_1q_3}.$$

Therefore the *unnormalized* conditional states are

$$|\phi_0\rangle = \frac{1}{2}\big(|00\rangle + |11\rangle\big), \qquad |\phi_1\rangle = \frac{1}{2}\big(|00\rangle - |11\rangle\big).$$

Their squared norms are $\|\phi_0\|^2 = \|\phi_1\|^2 = 1/2$, so each measurement outcome occurs with probability 1/2. The corresponding *normalized* states are $|\Phi^+\rangle$ and $|\Phi^-\rangle$.

c) For each measurement outcome $m \in \{0, 1\}$, write down the state of q_1 and q_3 *after* measuring q_2 and applying the classically controlled Z gate on q_1. Show that the final state is the same regardless of m.

Solution: **If $m = 0$:** No correction is applied. The state of q_1, q_3 is the normalized version of $|\phi_0\rangle$:

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

If $m = 1$: The state is initially the normalized version of $|\phi_1\rangle$, i.e. $|\Phi^-\rangle$, and we apply Z to qubit q_1:

$$(Z \otimes \mathbb{1})\,\big|\Phi^-\big\rangle = (Z \otimes \mathbb{1})\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \big|\Phi^+\big\rangle.$$

Thus the final state is $|\Phi^+\rangle$ regardless of m.

d) What would happen if the classically controlled Z correction were omitted?

i) Write down the post-measurement state of (q_1, q_3) conditioned on each outcome m, and the probability of each m.

ii) From the perspective of someone who does *not* know m, first describe the state of (q_1, q_3) as an *ensemble* of post-measurement pure states (with their probabilities), and then write the corresponding density operator ρ_{13}.

iii) Show that ρ_{13} can be written in two different ways:

$$\rho_{13} = \frac{1}{2}\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| + \frac{1}{2}\left|\Phi^-\right\rangle\!\left\langle\Phi^-\right| = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|.$$

where

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

Hint[7].

iv) Briefly interpret part iii): what does it say about "different ensembles giving the same density operator"?

Solution:

i) Without the correction:

$$m = 0: \ \left|\Phi^+\right\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad m = 1: \ \left|\Phi^-\right\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

Each occurs with probability $1/2$.

ii) If m is unknown, the observer assigns the ensemble

$$m = 0: \ \left|\Phi^+\right\rangle \text{ with probability } \tfrac{1}{2}, \qquad m = 1: \ \left|\Phi^-\right\rangle \text{ with probability } \tfrac{1}{2}.$$

The corresponding density operator is a classical mixture:

$$\rho_{13} = \frac{1}{2}\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| + \frac{1}{2}\left|\Phi^-\right\rangle\!\left\langle\Phi^-\right|.$$

iii) Expand:

$$\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|),$$

$$\left|\Phi^-\right\rangle\!\left\langle\Phi^-\right| = \frac{1}{2}(|00\rangle\langle 00| - |00\rangle\langle 11| - |11\rangle\langle 00| + |11\rangle\langle 11|).$$

Adding and dividing by 2:

$$\rho_{13} = \frac{1}{2}\big(|00\rangle\langle 00| + |11\rangle\langle 11|\big).$$

iv) The same density operator can be realised by different ensembles: here, an ensemble of *entangled* pure states $\{|\Phi^+\rangle, |\Phi^-\rangle\}$ with equal probabilities produces the same ρ_{13} as an ensemble of *product* states $\{|00\rangle, |11\rangle\}$ with equal probabilities. Operationally (for someone without access to m), these ensembles are indistinguishable by any measurement on (q_1, q_3) alone.

[7] Expand $\left|\Phi^\pm\right\rangle\!\left\langle\Phi^\pm\right|$ and add them; the off-diagonal terms cancel. This is the same phenomenon as in Problem 3: the same ρ can arise from different ensembles.

Problem 6: Quantum Teleportation in Qiskit (optional)

In this problem you will implement the quantum teleportation protocol in Qiskit, building the circuit step by step and verifying that it correctly transfers an arbitrary qubit state from Alice to Bob. A notebook with the tasks is available here:

https://colab.research.google.com/drive/1FbGKTBuqqxerf-js5IareBTYbJ1jPyYV

Solution: Solutions to the tasks are available here:

https://colab.research.google.com/drive/1G_TKwc73S0xkkfNQmMqOUvr1EEhRlceY