UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Exam in:	FYS3415/FYS4415 Quantum Computing and Quantum Information
Day of examination:	27 May 2026
Examination hours:	09:00 – 13:00

This examination paper consists of 13 pages.

Appendices:	Formula sheet
Permitted aids:	Approved calculator

Please make sure that your copy of the examination paper is complete before you attempt to answer anything.

Solutions

Problem 1 (weight 35%)

(a) Let

$$|\phi_1\rangle = |0\rangle, \qquad |\phi_2\rangle = |+\rangle. \tag{1}$$

Compute the fidelity $F(|\phi_1\rangle, |\phi_2\rangle)$. Now send both states through the following circuit:

$$|\phi_i\rangle \text{ ——} \boxed{H} \text{—— } |\phi_i'\rangle \tag{2}$$

Here $i = 1, 2$. Find the fidelity $F(|\phi_1'\rangle, |\phi_2'\rangle)$ after the circuit.

Solution:
We have

$$F(|\phi_1\rangle, |\phi_2\rangle) = |\langle\phi_1|\phi_2\rangle| = |\langle 0|+\rangle| = \frac{1}{\sqrt{2}}.$$

Fidelity is invariant under unitary transformations, so

$$F(|\phi_1'\rangle, |\phi_2'\rangle) = F(H|\phi_1\rangle, H|\phi_2\rangle) = F(|\phi_1\rangle, |\phi_2\rangle) = \frac{1}{\sqrt{2}}.$$

(b) What is a qubit physically? Briefly list the main things that must be implemented in hardware to do quantum computing.

Solution:
A qubit is physically a controllable quantum system with two chosen states, or a chosen two-dimensional subspace, for example two energy levels.

To build a quantum computer, the hardware must be able to:

- initialize qubits to a known state
- perform a suitable/universal set of single-qubit and two-qubit gates
- measure qubits reliably
- maintain coherence long enough with sufficiently low noise and error rates, possibly using error correction

(c) Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and let

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle \tag{3}$$

be a corresponding quantum oracle. Here $x \in \{0,1\}^n$, $y \in \{0,1\}$, and $\oplus$ denotes XOR (addition mod 2). Show that

$$U_f \left|x\right\rangle \left|-\right\rangle = (-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle, \tag{4}$$

by considering the two cases $f(x) = 0$ and $f(x) = 1$. Name one quantum algorithm where oracle information is encoded into phases in this way.

Solution:
If $f(x) = 0$, then

$$U_f \left|x\right\rangle \left|-\right\rangle = \left|x\right\rangle \frac{\left|0 \oplus 0\right\rangle - \left|1 \oplus 0\right\rangle}{\sqrt{2}} = \left|x\right\rangle \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} = \left|x\right\rangle \left|-\right\rangle.$$

If $f(x) = 1$, then

$$U_f \left|x\right\rangle \left|-\right\rangle = \left|x\right\rangle \frac{\left|0 \oplus 1\right\rangle - \left|1 \oplus 1\right\rangle}{\sqrt{2}} = \left|x\right\rangle \frac{\left|1\right\rangle - \left|0\right\rangle}{\sqrt{2}} = -\left|x\right\rangle \left|-\right\rangle.$$

Hence in both cases:

$$U_f \left|x\right\rangle \left|-\right\rangle = (-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle.$$

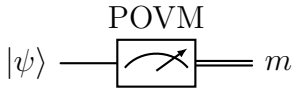
This is phase kickback. It is used for example in the Deutsch–Jozsa algorithm, the Bernstein–Vazirani algorithm, and in Grover search.

(d) Explain in 2–3 sentences what it means to violate a Bell inequality and the basic idea of how such a violation can be used to certify security in device-independent quantum key distribution. Mention one assumption that is still needed in device-independent quantum key distribution.

Solution:
To violate a Bell inequality, for example observing a CHSH parameter of $|S| > 2$, means that under the usual Bell assumptions, the observed measurement correlations of an experiment cannot be explained by any local hidden-variable model. In device-independent quantum key distribution, such a violation certifies that Alice and Bob share nonclassical correlations, which can be used to bound the possible information about their measurement outcomes that any third party can have. This certification is based only on the observed measurement statistics, and does not require knowing details about the signal source or the internal workings of the measurement devices, such as which measurements they actually perform.

Some assumptions are still needed, such as: Alice's and Bob's labs must be secure, so that the devices do not leak the key to Eve. The devices must not be able to communicate during the measurement rounds, for example because the labs are spacelike separated. Alice's and Bob's measurement choices must be random and unknown to Eve and to the devices before the measurements. The public classical communication channel must be authenticated. Finally, the Bell violation must be obtained without experimental loopholes such as postselection or undetected events that could fake nonlocal correlations.

(e) Consider a POVM measurement with two outcomes $m \in \{0, 1\}$ on a single qubit $|\psi\rangle$:



(5)

Assume that the measurement is described by two POVM operators $\{E_0, E_1\}$ such that $E_0 + E_1 = I$. You are given the measurement statistics:

$$\begin{aligned} \langle 0|E_0|0\rangle &= \frac{3}{4}, & \langle 1|E_0|1\rangle &= \frac{1}{4}, \\ \langle \phi_0|E_0|\phi_0\rangle &= \frac{3}{4}, & \langle \phi_1|E_0|\phi_1\rangle &= \frac{1}{2}, \end{aligned} \tag{6}$$

where

$$|\phi_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |\phi_1\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}. \tag{7}$$

Determine the POVM operators E_0 and E_1.

Solution:
Start by writing E_0 as a general 2×2 complex matrix in the computational basis:

$$E_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

From the measurement statistics:

$$\langle 0|E_0\,|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = a = \frac{3}{4},$$
$$\langle 1|E_0\,|1\rangle = \begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = d = \frac{1}{4},$$
$$\langle \phi_0|E_0\,|\phi_0\rangle = \frac{1}{2}\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = \frac{a+b+c+d}{2} = \frac{3}{4},$$
$$\langle \phi_1|E_0\,|\phi_1\rangle = \frac{1}{2}\begin{pmatrix}1 & -i\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1\\i\end{pmatrix} = \frac{a+d+ib-ic}{2} = \frac{1}{2}.$$

The first two equations give $a + d = 1$. Using this in the last two equations gives:

$$b + c = \frac{1}{2}$$
$$b - c = 0$$
$$\implies b = c = \frac{1}{4}.$$

Since $E_0 + E_1 = I$, we have

$$E_0 = \begin{pmatrix}\frac{3}{4} & \frac{1}{4}\\ \frac{1}{4} & \frac{1}{4}\end{pmatrix},$$
$$E_1 = I - E_0 = \begin{pmatrix}\frac{1}{4} & -\frac{1}{4}\\ -\frac{1}{4} & \frac{3}{4}\end{pmatrix}.$$

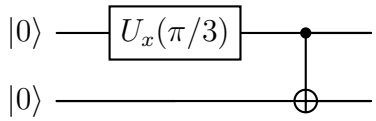
We can verify that these are valid POVM operators by checking that they both have only nonnegative eigenvalues. For E_0, the eigenvalues are found from

$$\det(E_0 - \lambda I) = \det\begin{pmatrix}\frac{3}{4}-\lambda & \frac{1}{4}\\ \frac{1}{4} & \frac{1}{4}-\lambda\end{pmatrix} = 0,$$
$$\implies \lambda^2 - \lambda + \frac{1}{8} = 0,$$
$$\implies \lambda_\pm = \frac{1}{2}\left(1 \pm \frac{1}{\sqrt{2}}\right) > 0.$$

Both eigenvalues are positive. Since $E_1 = I - E_0$, the eigenvalues of E_1 are $1 - \lambda_\pm$, which are the same two values in the opposite order. Therefore both E_0 and E_1 are positive operators, so they are valid POVM operators.

Problem 2 (weight 35%)

Consider the following circuit:



(8)

(a) Show that the output state of the circuit is

$$|\psi_1\rangle = \frac{\sqrt{3}}{2}|00\rangle - \frac{i}{2}|11\rangle, \tag{9}$$

where the first qubit corresponds to the upper wire.

Solution:
The state evolves as

$$\begin{aligned}|00\rangle &\mapsto \left(U_x\left(\frac{\pi}{3}\right)\otimes I\right)|00\rangle = \left(\cos\frac{\pi}{6}|0\rangle - i\sin\frac{\pi}{6}|1\rangle\right)|0\rangle \\ &= \left(\frac{\sqrt{3}}{2}|0\rangle - \frac{i}{2}|1\rangle\right)|0\rangle = \frac{\sqrt{3}}{2}|00\rangle - \frac{i}{2}|10\rangle \\ &\mapsto \frac{\sqrt{3}}{2}|00\rangle - \frac{i}{2}|11\rangle = |\psi_1\rangle.\end{aligned}$$

(b) Suppose both qubits in the state $|\psi_1\rangle$ are measured in the computational basis. What are the possible outcomes of the two-qubit measurement, and what is the probability of each outcome?

Solution:
The four possible outcomes for a joint two-qubit computational-basis measurement have probabilities:

$$\begin{aligned}p(0,0) &= |\langle 00|\psi_1\rangle|^2 = \frac{3}{4}, \\ p(0,1) &= |\langle 01|\psi_1\rangle|^2 = 0, \\ p(1,0) &= |\langle 10|\psi_1\rangle|^2 = 0, \\ p(1,1) &= |\langle 11|\psi_1\rangle|^2 = \frac{1}{4}.\end{aligned}$$

(c) Is $|\psi_1\rangle$ a product state or an entangled state? If it is a product state, give a decomposition. If it is entangled, explicitly show why.

Solution:
For a pure two-qubit state, the state is a product state if and only if the reduced

density matrix of one qubit is pure. We compute

$$\begin{aligned}\rho_1 &= \mathrm{tr}_2\left(|\psi_1\rangle\langle\psi_1|\right)\\ &= \mathrm{tr}_2\left(\frac{3}{4}|00\rangle\langle 00| + \frac{i\sqrt{3}}{4}|00\rangle\langle 11| - \frac{i\sqrt{3}}{4}|11\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11|\right)\\ &= \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|.\end{aligned}$$

Thus

$$\mathrm{tr}\left(\rho_1^2\right) = \left(\frac{3}{4}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{5}{8} < 1,$$

meaning that ρ_1 is mixed. Therefore $|\psi_1\rangle$ is not a product state, so it is entangled.

(d) Calculate the reduced density matrix of the first qubit for the state $|\psi_1\rangle$. Briefly explain what measurement statistics this reduced density matrix can predict, and what kind of measurement statistics it cannot predict.

Solution:
The reduced density operator for the first qubit is

$$\begin{aligned}\rho_1 &= \mathrm{tr}_2\left(|\psi_1\rangle\langle\psi_1|\right)\\ &= \mathrm{tr}_2\left(\frac{3}{4}|00\rangle\langle 00| + \frac{i\sqrt{3}}{4}|00\rangle\langle 11| - \frac{i\sqrt{3}}{4}|11\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11|\right)\\ &= \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|.\end{aligned}$$

The reduced density matrix ρ_1 predicts all statistics for measurements on the first qubit alone. For example measuring the first qubit in the computational basis gives probabilities 3/4 for outcome 0 and 1/4 for outcome 1. It cannot predict measurements on the second qubit, joint two-qubit measurement statistics, or correlations between the two qubit measurements, such as the fact that the two computational-basis measurement outcomes for the two qubits are always equal.

(e) Define

$$\sigma_1 = |\psi_1\rangle\langle\psi_1|, \qquad \sigma_2 = \frac{3}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11|. \tag{10}$$

For each of the two density operators σ_1 and σ_2, determine whether it is pure or mixed, and whether it is entangled or not entangled. Justify your answers mathematically.

Solution:
By inspection, $\sigma_1 = |\psi_1\rangle\langle\psi_1|$ is pure since it is the projector onto one normalized state. The state σ_1 is entangled if and only if $|\psi_1\rangle$ is entangled. The solution for part **(c)** shows how to determine that it is entangled. Thus σ_1 is pure and entangled.

For σ_2, we have

$$\sigma_2^2 = \frac{9}{16}\,|00\rangle\langle 00| + \frac{1}{16}\,|11\rangle\langle 11|.$$

Therefore

$$\mathrm{tr}\big(\sigma_2^2\big) = \frac{9}{16} + \frac{1}{16} = \frac{5}{8} < 1,$$

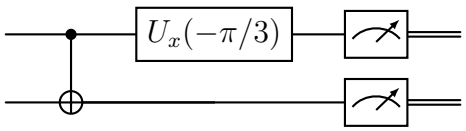
meaning that σ_2 is mixed. Finally, we see directly that σ_2 is separable, since it is a convex mixture of product states:

$$\sigma_2 = \frac{3}{4}\big(|0\rangle\langle 0| \otimes |0\rangle\langle 0|\big) + \frac{1}{4}\big(|1\rangle\langle 1| \otimes |1\rangle\langle 1|\big).$$

Thus σ_2 is mixed and not entangled.

(f) Does there exist a unitary circuit such that, after applying the circuit and measuring in the computational basis, there is an outcome whose probability is different for input σ_1 than for input σ_2? If so, draw such a circuit. If not, show why.

Solution:
Yes. The two states have the same computational-basis probabilities, but σ_1 contains coherence between $|00\rangle$ and $|11\rangle$, while σ_2 does not. We can reveal this difference by applying the inverse of the circuit that prepared $|\psi_1\rangle$ from $|00\rangle$:



We can verify that the probability of measurement outcome "00" really is different after this circuit, by considering the two inputs σ_1 and σ_2. For input $\sigma_1 = |\psi_1\rangle\langle\psi_1|$, the circuit maps

$$|\psi_1\rangle \mapsto |00\rangle,$$

so

$$p_{\sigma_1}(0,0) = 1.$$

For input σ_2, the CNOT gives

$$\sigma_2 \mapsto \frac{3}{4}\,|00\rangle\langle 00| + \frac{1}{4}\,|10\rangle\langle 10| = \sigma_2'.$$

Using

$$U_x\left(-\frac{\pi}{3}\right) = \frac{\sqrt{3}}{2}I + \frac{i}{2}X,$$

we have

$$U_x\left(-\frac{\pi}{3}\right)|0\rangle = \frac{\sqrt{3}}{2}\,|0\rangle + \frac{i}{2}\,|1\rangle, \qquad U_x\left(-\frac{\pi}{3}\right)|1\rangle = \frac{i}{2}\,|0\rangle + \frac{\sqrt{3}}{2}\,|1\rangle.$$

Thus, the $U_x(-\pi/3)$ gate gives:

$$\begin{aligned}\sigma_2' &\mapsto \left(U_x\left(-\frac{\pi}{3}\right)\otimes I\right)\sigma_2'\left(U_x\left(-\frac{\pi}{3}\right)^\dagger\otimes I\right)\\ &= \frac{3}{4}\left(\frac{\sqrt{3}}{2}|00\rangle + \frac{i}{2}|10\rangle\right)\left(\frac{\sqrt{3}}{2}\langle 00| - \frac{i}{2}\langle 10|\right)\\ &+ \frac{1}{4}\left(\frac{i}{2}|00\rangle + \frac{\sqrt{3}}{2}|10\rangle\right)\left(-\frac{i}{2}\langle 00| + \frac{\sqrt{3}}{2}\langle 10|\right)\\ &= \frac{5}{8}|00\rangle\langle 00| - \frac{i\sqrt{3}}{8}|00\rangle\langle 10| + \frac{i\sqrt{3}}{8}|10\rangle\langle 00| + \frac{3}{8}|10\rangle\langle 10|.\end{aligned}$$

Therefore

$$p_{\sigma_2}(0,0) = \frac{5}{8} \neq 1.$$

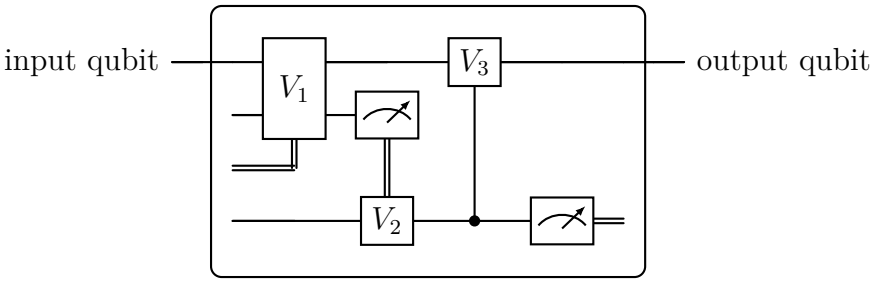
Problem 3 (weight 30%)

Alice wants to communicate with Bob by sending quantum states through some unknown black box:



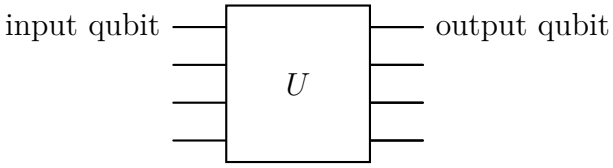
(11)

(a) Let the black box be implemented by the following quantum-classical circuit:



(12)

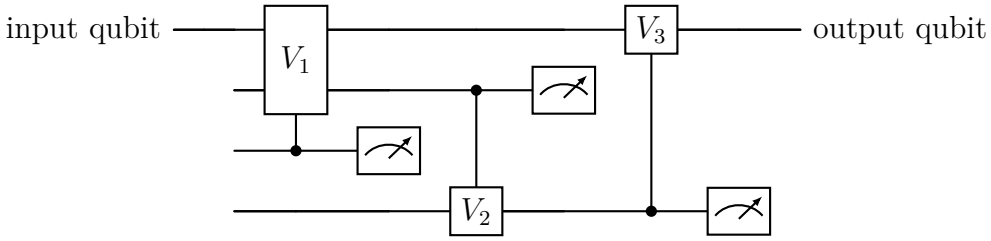
All wires other than the top input–output wire are internal to the black box and are not accessible to Alice or Bob. The internal registers are initialized in fixed states independently of the input qubit. The internal classical wire entering V_1 represents classical control of whether V_1 is applied. Explain why, as far as Alice and Bob are concerned, this circuit can be equivalently described by a single unitary operator U acting on the input qubit together with internal registers in the following way:



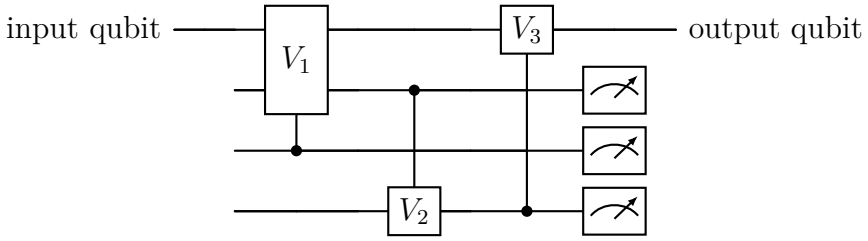
(13)

You may explain steps in your argument using circuit diagrams. Draw a circuit for U in terms of the quantum gates V_1, V_2, and V_3.

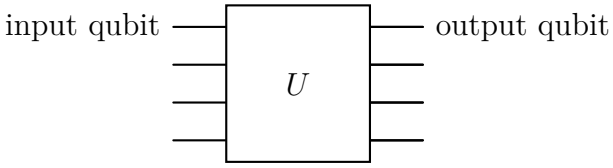
Solution:
First, the internal classical register can be represented by a corresponding internal quantum register in a computational-basis state. Any measurements followed by classical control can be replaced by quantum control followed by the same measurement immediately afterwards. This gives the equivalent circuit:



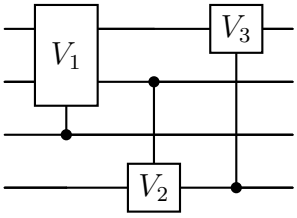
Next, by the principle of deferred measurement, any intermediate measurements can be postponed until the end of the circuit:



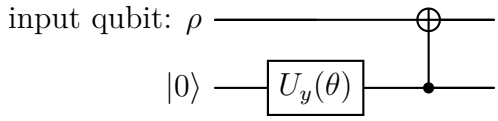
Finally, the measurement outcomes of the final measurements are not accessible to Alice or Bob. By the principle of implicit measurement, the perspective of Alice and Bob is unchanged whether the internal registers are measured or not. We may therefore omit these final measurements and instead discard the internal registers. Thus, the black-box circuit is for Alice and Bob equivalent to:



with the unitary operator U given by the circuit:



(b) We now consider a concrete example. Take the ancilla to be just one qubit initialized to $|0\rangle$, and take the unitary operator U to be the following two-qubit circuit:



(14)

Here $0 \leq \theta \leq \pi$. Find Kraus operators representing the induced channel from an input qubit ρ to the output qubit. Use this to show that the channel can be written as

$$\mathcal{E}(\rho) = (1-p)\rho + pX\rho X, \tag{15}$$

and determine p in terms of θ.

Solution:

Let S denote the input/output qubit and E the ancilla qubit, and use the ordering $S \otimes E$. Write

$$c = \cos\frac{\theta}{2}, \qquad s = \sin\frac{\theta}{2}.$$

We have

$$U_y(\theta) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = c\,|0\rangle\langle 0| - s\,|0\rangle\langle 1| + s\,|1\rangle\langle 0| + c\,|1\rangle\langle 1|.$$

The CNOT gate has E as control and S as target, so

$$\mathrm{CNOT}_{E\mapsto S} = I \otimes |0\rangle\langle 0|_E + X \otimes |1\rangle\langle 1|_E.$$

Hence the full two-qubit unitary is

$$\begin{aligned} U &= \mathrm{CNOT}_{E\mapsto S}\,(I \otimes U_y(\theta)) \\ &= \Big(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|\Big)\Big[I \otimes (c\,|0\rangle\langle 0| - s\,|0\rangle\langle 1| + s\,|1\rangle\langle 0| + c\,|1\rangle\langle 1|)\Big] \\ &= c\,I \otimes |0\rangle\langle 0| - s\,I \otimes |0\rangle\langle 1| + s\,X \otimes |1\rangle\langle 0| + c\,X \otimes |1\rangle\langle 1|. \end{aligned}$$

The Kraus operators are obtained from

$$\begin{aligned} M_0 &= {}_E\langle 0|\,U\,|0\rangle_E \\ &= {}_E\langle 0|\,(c\,I \otimes |0\rangle\langle 0| - s\,I \otimes |0\rangle\langle 1| + s\,X \otimes |1\rangle\langle 0| + c\,X \otimes |1\rangle\langle 1|)\,|0\rangle_E \\ &= c\,I, \\ M_1 &= {}_E\langle 1|\,U\,|0\rangle_E \\ &= {}_E\langle 1|\,(c\,I \otimes |0\rangle\langle 0| - s\,I \otimes |0\rangle\langle 1| + s\,X \otimes |1\rangle\langle 0| + c\,X \otimes |1\rangle\langle 1|)\,|0\rangle_E \\ &= s\,X. \end{aligned}$$

Therefore

$$M_0 = \cos\frac{\theta}{2} I, \qquad M_1 = \sin\frac{\theta}{2} X.$$

We can verify that they satisfy the completeness relation, since

$$M_0^\dagger M_0 + M_1^\dagger M_1 = \cos^2\frac{\theta}{2} I + \sin^2\frac{\theta}{2} X^\dagger X = I.$$

The induced channel is

$$\begin{aligned}\mathcal{E}(\rho) &= \mathrm{tr}_E\left[U(\rho\otimes|0\rangle\langle 0|_E)U^\dagger\right]\\ &= \sum_{i=0}^{1} M_i\rho M_i^\dagger\\ &= \cos^2\frac{\theta}{2}\rho + \sin^2\frac{\theta}{2}X\rho X.\end{aligned}$$

Comparing with the expression for $\mathcal{E}(\rho)$ in the problem text gives

$$p = \sin^2\frac{\theta}{2}.$$

(c) Alice wants to communicate a uniformly random classical bit $M \in \{0,1\}$ to Bob by sending a qubit ρ through the black box, represented by the channel $\mathcal{E}$. Suppose Alice uses the encoding $0 \mapsto |0\rangle$ and $1 \mapsto |1\rangle$. Find the state Bob receives for each sent bit M, as well as Bob's average received density operator. Use this to compute the Holevo quantity $\chi(p)$ for Bob's received states in terms of the channel parameter p. Briefly explain what the Holevo quantity says about Bob's ability to learn Alice's bit M from the transmitted quantum states.

Solution:
For the two possible values of M, Bob receives

$$\begin{aligned}\rho_B^0 &= \mathcal{E}(|0\rangle\langle 0|)\\ &= (1-p)\,|0\rangle\langle 0| + pX\,|0\rangle\langle 0|X\\ &= (1-p)\,|0\rangle\langle 0| + p\,|1\rangle\langle 1|,\\ \rho_B^1 &= \mathcal{E}(|1\rangle\langle 1|)\\ &= (1-p)\,|1\rangle\langle 1| + pX\,|1\rangle\langle 1|X\\ &= p\,|0\rangle\langle 0| + (1-p)\,|1\rangle\langle 1|.\end{aligned}$$

Since Alice's bit is uniformly random, Bob's average received density operator is

$$\begin{aligned}\bar\rho_B &= \frac{1}{2}\rho_B^0 + \frac{1}{2}\rho_B^1\\ &= \frac{1}{2}\left[(1-p)\,|0\rangle\langle 0| + p\,|1\rangle\langle 1|\right] + \frac{1}{2}\left[p\,|0\rangle\langle 0| + (1-p)\,|1\rangle\langle 1|\right]\\ &= \frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}\,|1\rangle\langle 1| = \frac{I}{2}.\end{aligned}$$

The Holevo quantity is

$$\chi(p) = S(\bar\rho_B) - \frac{1}{2}S(\rho_B^0) - \frac{1}{2}S(\rho_B^1).$$

All three density operators are diagonal in the computational basis:

$$\rho_B^0 = \begin{pmatrix}1-p & 0\\ 0 & p\end{pmatrix}, \qquad \rho_B^1 = \begin{pmatrix}p & 0\\ 0 & 1-p\end{pmatrix}, \qquad \bar\rho_B = \begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{pmatrix}.$$

Therefore their von Neumann entropies are just the Shannon entropies of their diagonal entries. Hence

$$S(\rho_B^0) = h_{\mathrm{b}}(p), \qquad S(\rho_B^1) = h_{\mathrm{b}}(p), \qquad S(\bar{\rho}_B) = h_{\mathrm{b}}\left(\frac{1}{2}\right) = 1.$$

Therefore

$$\chi(p) = 1 - \frac{1}{2}h_{\mathrm{b}}(p) - \frac{1}{2}h_{\mathrm{b}}(p) = 1 - h_{\mathrm{b}}(p).$$

The Holevo quantity gives an upper bound on how much classical information Bob can obtain about Alice's bit M. For any measurement Bob can perform on his received qubit yielding an outcome N, the Holevo bound certifies that the mutual information satisfies

$$I(M:N) \leq \chi(p) = 1 - h_{\mathrm{b}}(p).$$

This gives an upper bound for the information Bob can obtain about Alice's bit per use of the channel $\mathcal{E}$.

(d) Alice now decides to transmit her classical bit M through the black box using quantum error correction. She first uses the same encoding as in part **(c)** to prepare a qubit state ρ. Then, instead of sending ρ directly, she encodes it into 3 physical qubits using the bit-flip code:

$$|0_{\mathrm{L}}\rangle = |000\rangle, \qquad |1_{\mathrm{L}}\rangle = |111\rangle. \tag{16}$$

She then sends the three physical qubits independently through the channel $\mathcal{E}$. Bob then performs the standard bit-flip-code recovery and decoding. This defines an effective logical channel $\mathcal{E}_{\mathrm{L}}(\rho)$ from Alice's qubit state ρ to Bob's decoded output state.

The probability of a single bit-flip error occurring for a physical qubit transmitted through the channel $\mathcal{E}$ is p. Therefore, the probability for getting n physical bit-flip errors for a transmitted encoded qubit is:

n	probability
0	$(1-p)^3$
1	$3p(1-p)^2$
2	$3p^2(1-p)$
3	p^3

(17)

Determine an expression for the logical channel $\mathcal{E}_{\mathrm{L}}$. Write down the Holevo quantity χ_{L} for this logical channel expressed in terms of the function $\chi(\cdot)$ from part **(c)** and the channel parameter p. Assume that the Holevo bound is tight in this case. How much obtainable classical information does this give per use of the physical channel $\mathcal{E}$?

Solution:
For zero or one bit flips, the recovery operation corrects the error and the logical state ρ is recovered. For two or three bit flips, the code fails. Then the majority vote gives the wrong logical value, which is equivalent to applying a logical bit flip X to the decoded qubit. Thus the logical channel has the same form as the original bit-flip channel:

$$\mathcal{E}_{\mathrm{L}}(\rho) = (1 - p_{\mathrm{L}})\rho + p_{\mathrm{L}} X \rho X,$$

but with logical error probability

$$p_{\mathrm{L}} = 3p^2(1-p) + p^3 = 3p^2 - 2p^3.$$

In line with part **(c)**, we let $\chi(p)$ denote the Holevo quantity for Alice's original state encoding sent through a bit-flip channel with error probability p. The Holevo quantity for the logical channel $\mathcal{E}_{\mathrm{L}}$ is then

$$\chi_{\mathrm{L}} = \chi(p_{\mathrm{L}}) = \chi(3p^2 - 2p^3) = 1 - h_{\mathrm{b}}(3p^2 - 2p^3).$$

Assuming that the Holevo bound is tight, this is the obtainable classical information per encoded logical qubit. Since each encoded logical qubit requires three physical uses of the channel $\mathcal{E}$, the obtainable classical information per use of the physical channel is

$$\frac{\chi_{\mathrm{L}}}{3} = \frac{\chi(3p^2 - 2p^3)}{3} = \frac{1 - h_{\mathrm{b}}(3p^2 - 2p^3)}{3}.$$