University of Oslo

FYS3415/FYS4415 — Quantum computing and quantum information

Problem set 12

This problem set will be discussed on **May 6**.

Unless otherwise stated, all logarithms are base 2, so entropies are measured in bits.

Problem 1: Quantum Relative Entropy and Mutual Information

In the previous set you studied the von Neumann entropy and proved a number of structural results, such as the joint entropy theorem and the equality of entropies for purifications. In this problem you continue along these lines and develop the *quantum relative entropy*, which plays the same fundamental role in quantum information that the classical relative entropy plays in Shannon theory.

For two density operators ρ and σ on the same Hilbert space, the quantum relative entropy is

$$S(\rho \,\|\, \sigma) \equiv \operatorname{Tr}(\rho \log \rho) - \operatorname{Tr}(\rho \log \sigma),$$

defined to be $+\infty$ when the support of ρ is not contained in the support of σ. Just as in the classical case, $S(\rho \,\|\, \sigma) \geq 0$ with equality iff $\rho = \sigma$ (*Klein's inequality*); we will take this as a given here.

a) Relative entropy in the commuting case.

Suppose ρ and σ commute, so they share an orthonormal eigenbasis $\{|x\rangle\}$ with eigenvalues $p(x)$ and $q(x)$, respectively.

Use the usual conventions $0 \log(0/q) = 0$, and if $p(x) > 0$ while $q(x) = 0$, the corresponding contribution is $+\infty$.

i) Show that

$$S(\rho \,\|\, \sigma) = H\big(p(x) \,\|\, q(x)\big),$$

where the right-hand side is the classical relative entropy of the eigenvalue distributions.

ii) Conclude that $S(\rho \,\|\, \sigma) \geq 0$ in this case, and identify when equality holds.

iii) As a concrete check, compute $S(\rho \,\|\, \sigma)$ for the qubit pair $\rho = |0\rangle\langle 0|$ and $\sigma = I/2$, and verify that the result is non-negative.

b) Quantum mutual information and subadditivity.

For a bipartite state ρ^{AB} with reduced states $\rho^A = \operatorname{Tr}_B \rho^{AB}$ and $\rho^B = \operatorname{Tr}_A \rho^{AB}$, the *quantum mutual information* is

$$I(A:B) \equiv S(A) + S(B) - S(A,B).$$

i) Show that $I(A:B) = S\big(\rho^{AB} \,\big\|\, \rho^A \otimes \rho^B\big)$.

ii) Conclude the *subadditivity* inequality $S(A,B) \leq S(A) + S(B)$, and identify when equality holds.

Hint[1].

[1] Use $\log\big(\rho^A \otimes \rho^B\big) = \log \rho^A \otimes I + I \otimes \log \rho^B$, which follows from the spectral decomposition of $\rho^A \otimes \rho^B$. The logarithms are understood on the supports of the corresponding density operators.

c) A bipartite computation.

Consider the bipartite state

$$\rho^{AB} \;=\; \tfrac{1}{2}\,|0\rangle\langle 0| \otimes |0\rangle\langle 0| \;+\; \tfrac{1}{2}\,|1\rangle\langle 1| \otimes |+\rangle\langle +|,$$

which can be read as Alice flipping a fair coin, recording the result on system A, and preparing system B in $|0\rangle$ if the coin came up 0 and $|+\rangle$ if it came up 1.

i) Compute the reduced states ρ^A and ρ^B and their von Neumann entropies $S(A)$ and $S(B)$. (You may reuse the eigenvalues of $\bar{\rho} = \frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}\,|+\rangle\langle +|$ from problem set 11, problem 2a.)

ii) Find the eigenvalues of ρ^{AB} and use them to compute $S(A, B)$.

iii) Combine your results to evaluate $I(A:B)$. Compare to $S(A) = 1$ bit and explain in one sentence why the two are different.

Hint[2].

[2] For ii), notice that ρ^{AB} is a sum of two rank-one terms whose supports lie in mutually orthogonal subspaces of $\mathcal{H}_A \otimes \mathcal{H}_B$ (because $\langle 0|1\rangle_A = 0$). The eigenvalues of such a sum are simply the weights of the rank-one pieces.

Problem 2: Holevo Information and the Holevo Bound

Suppose Alice prepares a quantum state ρ_x with probability p_x, drawn from an ensemble $\mathcal{E} = \{p_x, \rho_x\}$, and sends it to Bob. Bob performs a POVM $\{E_y\}$ and obtains classical outcome Y. How much classical information about Alice's choice X can Bob's measurement reveal? The *Holevo bound* answers this question:

$$I(X:Y) \leq \chi(\mathcal{E}), \qquad \chi(\mathcal{E}) \equiv S\left(\sum_x p_x \rho_x\right) - \sum_x p_x\, S(\rho_x).$$

The quantity $\chi(\mathcal{E})$ is the *Holevo information* of the ensemble; the inequality holds for every choice of POVM.

a) Holevo information as a mutual information.

Introduce a "label" register A with orthonormal basis $\{|x\rangle\}$, and form the classical-quantum state

$$\rho^{AB} \;=\; \sum_x p_x \; |x\rangle\langle x| \otimes \rho_x$$

on $A \otimes B$. Compute ρ^A, ρ^B, and $S(A,B)$, using the joint entropy theorem

$$S(A,B) = H(p_x) + \sum_x p_x S(\rho_x).$$

Then show that

$$I(A:B) = \chi(\mathcal{E}).$$

b) The ensemble from problem 1c.

The bipartite state in problem 1c arose from the ensemble

$$\mathcal{E} = \left\{ \left(\tfrac{1}{2}, |0\rangle\langle 0|\right), \left(\tfrac{1}{2}, |+\rangle\langle +|\right) \right\}.$$

Compute $\chi(\mathcal{E})$ from the formula in part a), and check that it equals the $I(A:B)$ computed there directly.

c) A three-state example.

Consider the three pure qubit states

$$|\psi_0\rangle = |0\rangle, \qquad |\psi_1\rangle = -\frac{1}{2}\,|0\rangle + \frac{\sqrt{3}}{2}\,|1\rangle, \qquad |\psi_2\rangle = -\frac{1}{2}\,|0\rangle - \frac{\sqrt{3}}{2}\,|1\rangle,$$

each prepared with probability 1/3.

i) Compute the average state

$$\bar{\rho} = \frac{1}{3}\sum_{x=0}^{2} |\psi_x\rangle\langle\psi_x|$$

and the Holevo information χ of this ensemble.

ii) Now define states $|\phi_x\rangle$ orthogonal to $|\psi_x\rangle$:

$$|\phi_0\rangle = |1\rangle, \qquad |\phi_1\rangle = \frac{\sqrt{3}}{2}\,|0\rangle + \frac{1}{2}\,|1\rangle, \qquad |\phi_2\rangle = \frac{\sqrt{3}}{2}\,|0\rangle - \frac{1}{2}\,|1\rangle.$$

Bob measures with the POVM

$$E_x = \frac{2}{3}\,|\phi_x\rangle\langle\phi_x|, \qquad x = 0, 1, 2.$$

You may use that $\sum_x E_x = I$. Show that

$$p(Y = y \mid X = x) = \begin{cases} 0, & y = x, \\ 1/2, & y \neq x, \end{cases}$$

and compute the resulting classical mutual information $I(X:Y)$. Compare it with χ.

Problem 3: The Threshold Theorem and the Cost of Fault Tolerance

Real qubits decohere and real gates fail. A representative superconducting-transmon estimate might use a coherence time $T_2 \sim 100\,\mu$s and gate time $\tau_g \sim 25\,$ns, giving the crude coherence budget

$$T_2/\tau_g \sim \frac{100\,\mu\text{s}}{25\,\text{ns}} \approx 4 \times 10^3$$

gate times. Useful algorithms require vastly longer computations: a rough classroom estimate for Shor's algorithm on an n-bit integer scales like n^3 logical gates, so RSA-2048 suggests a scale around 10^{10} logical gates.

The *quantum threshold theorem* says that if the physical error rate is below a code-dependent threshold, then encoding and repeated error correction can suppress logical errors to arbitrarily low levels, at the price of overhead. In this problem we study this scaling using concatenated codes.

a) One level of encoding.

Recall that the 3-qubit bit-flip code corrects zero or one bit flip, but fails if two or three physical qubits flip. If each physical qubit flips independently with probability p, the logical error rate is

$$p_L = \binom{3}{2} p^2(1-p) + p^3 = 3p^2 - 2p^3.$$

i) Solve $p_L < p$. For which physical error rates does the encoding improve the qubit?

ii) For $p \ll 1$, we have $p_L \approx 3p^2$. Show that this can be written as

$$\frac{p_L}{p_{\text{th}}} \approx \left(\frac{p}{p_{\text{th}}}\right)^2, \qquad p_{\text{th}} = \frac{1}{3}.$$

Why is this p_{th} not the same as the exact crossover found in part i)?

b) Concatenation.

In concatenated coding, each physical qubit is itself replaced by an encoded block. Assume that after one level the effective error rate obeys

$$\frac{p^{(k)}}{p_{\text{th}}} = \left(\frac{p^{(k-1)}}{p_{\text{th}}}\right)^2, \qquad p^{(0)} = p.$$

i) Show by induction that

$$p^{(k)} = p_{\text{th}} \left(\frac{p}{p_{\text{th}}}\right)^{2^k}.$$

ii) Explain why the logical error rate decreases double-exponentially in k when $p < p_{\text{th}}$, and why concatenation fails to help when $p \geq p_{\text{th}}$.

c) A concatenated-code overhead estimate.

The 3-qubit bit-flip code is only a toy model: it corrects only X-errors and assumes perfect syndrome extraction. A simple concatenated-code benchmark is a $[[7, 1, 3]]$-style code, where each concatenation level multiplies the number of physical data qubits by 7. Thus a level-k logical qubit uses 7^k physical data qubits. Use the rough threshold

$$p_{\text{th}} = 10^{-4}.$$

i) A benchmark physical error rate is $p = 10^{-3}$. Is this below threshold for this concatenated-code model? What does that imply?

ii) Now suppose improved hardware reaches

$$p = 10^{-5}.$$

Using

$$p^{(k)} = p_{\text{th}} \left(\frac{p}{p_{\text{th}}} \right)^{2^k},$$

find the smallest k such that

$$p^{(k)} \leq 10^{-15}.$$

iii) For this k, estimate the number of physical data qubits needed for 10^4 logical qubits. Briefly state what this estimate ignores.

Hint[3].

[3] For part ii), take base-10 logarithms.