

1 Classical Information

EXERCISES

1.1 Entropic quantum uncertainty principle. Let A, B be two quantum observables, with eigenvectors $\{|a\rangle\}, \{|b\rangle\}$. Let $F(A, B) := \sup_{a,b} |\langle b|a\rangle|$ the maximum fidelity between any couple $|a\rangle, |b\rangle$. Let ψ be a state vector. If $p_{\psi,A}, p_{\psi,B}$ denote the distribution probabilities $\{|\langle a|\psi\rangle|^2\}, \{|\langle b|\psi\rangle|^2\}$, then it can be shown that

$$H(p_{\psi,A}) + H(p_{\psi,B}) \geq 2 \log_2 \frac{1}{F(A, B)}.$$

Prove the following weaker result:

$$H(p_{\psi,A}) + H(p_{\psi,B}) \geq 2 \log_2 \frac{2}{1 + F(A, B)}.$$

1.2 N random cubes have average volume $\langle V \rangle = 1000$. The average of the lengths of their sides is $\langle \ell \rangle = 10$. What can be said of the size of the largest of these N cubes?

1.3 The entropy distance between the random variables X and Y is defined as

$$d_H(X, Y) := H(X|Y) + H(Y|X).$$

i/ Prove that d_H satisfies the triangle inequality

$$d_H(X, Z) \leq d_H(X, Y) + d_H(Y, Z).$$

However it is not a distance. ii/ Why?

1.4 Let X be a real-valued random variable. Prove that $H(X^2|X) = 0$, but $H(X|X^2)$ is not necessarily zero.

1.5 Suppose X is the value obtained by throwing a fair die. Let Y be 1 if the value of X is odd and 0 otherwise. Compute $H(X), H(Y), H(X|Y), H(Y|X)$.

1.6 Principle of maximum entropy (maxent). Let X be a random variable with real values $\{x_1, \dots, x_N\}$. Let $\mu := \langle X \rangle$ its expectation value. Prove that,

given μ , the probability distribution which maximizes the entropy $H(X)$ satisfies

$$p_j := P(X = x_j) = Ae^{\alpha x_j},$$

where A, α are determined by $\langle X \rangle = \mu, \sum_i p_i = 1$.

1.7 Chaining rule for conditional entropies. Prove that

$$H(X_1, X_2, \dots, X_n | Y) = \sum_i H(X_i | Y, X_1, \dots, X_{i-1}).$$

1.8 Mutual information is not necessarily subadditive: $H(X, Y : Z) \not\leq H(X : Z) + H(Y : Z)$. Give an example.

1.9 Chain rule for mutual information. Prove that

$$H(X : Y, Z) = H(X : Y) + H(X : Z | Y),$$

where $H(X : Z | Y) := H(X | Y) + H(Z | Y) - H(X, Z | Y)$.

1.10 Data processing can only destroy information. A Markov chain is a sequence of random variables $X_1 \rightarrow X_2 \rightarrow \dots \rightarrow X_n \rightarrow \dots$ such that X_n is independent of X_1, \dots, X_{n-2} , given X_{n-1} . I.e.

$$\begin{aligned} P(X_n = x_n | X_{n-1} = x_{n-1}, \dots, X_1 = x_1) &= \\ &= P(X_n = x_n | X_{n-1} = x_{n-1}). \end{aligned}$$

In particular, for such chains

$$P(x_1, \dots, x_n) = P(x_n | x_{n-1}) \dots P(x_3 | x_2) P(x_2 | x_1) P(x_1).$$

The data processing theorem states that if $X \rightarrow Y \rightarrow Z$ is Markov, then

$$H(X : Z) \leq H(X : Y) \leq H(X).$$

In other words, if X is a random variable subject to noise, producing Y , then data processing (further actions on our part) cannot be used to increase the mutual information between the output of the process and the original information X . Prove it.

1.11 Prove that $X \rightarrow Y \rightarrow Z \implies Z \rightarrow Y \rightarrow X$, and hence the data pipelining inequality for any Markov chain $X \rightarrow Y \rightarrow Z$:

$$H(Z : X) \leq H(Z : Y) \leq H(Y).$$

Any information that Z shares with X is also shared by Z and Y , i.e. the information is pipelined from X to Z through Y .

1.12 In a game over a chessboard, player A has to guess where player B has placed a queen. A is allowed six questions which B has to answer truthfully by a yes/no reply. Find a strategy by which A can always win the game, but winning is not assured if only five questions are permitted. Generalize to an $n \times n$ board.

1.13 The weighing problem and why entropy considerations allow designing optimal strategies. You are given a balance and 9 apparently equal balls. You are told that one ball weights different than the rest and asked to find which ball it is and whether it is heavier or lighter. Devise a strategy with 3 weighings. Generalize to n balls and k weighings, and prove that necessarily $3^k \gtrsim 2n$. (As a matter of fact, a strategy exists which allow to spot the odd ball whenever $3^k \geq 2n + 3$.)

1.14 Find the maximum number of words in a binary prefix code in which the maximum word length is 7.

1.15 Let $A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ be an alphabet with probability distribution $\{0.27, 0.19, 0.12, 0.1, 0.1, 0.1, 0.04, 0.03, 0.03, 0.015, 0.005\}$. Find a Huffman coding C of A . Compare $H(A)$ and $L(C)$.

1.16 Suppose that a noisy transmission channel Q has a matrix channel $P(Q)$ given by

$$\begin{pmatrix} \frac{1}{6} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{6} \end{pmatrix}.$$

Find its capacity $C(Q)$ and an optimal input probability distribution.

1.17 Consider the code C_4 consisting of the codewords $c_1 = 1000$, $c_2 = 0110$, $c_3 = 0001$, $c_4 = 1111$. Suppose that the probabilities of these codewords are $p(c_1) = p(c_2) = 1/3$, $p(c_3) = p(c_4) = 1/6$. If you receive the vector 1001 through a binary symmetric channel with error probability $p = 1/10$, find how you would decode it: 1/ using the minimum-error decoding rule, 2/ using the maximum-likelihood decoding rule.

1.18 Let $H_2(4) \subset \mathbb{F}_2^{15}$ be the Hamming code $H_q(r)$ with $q = 2, r = 4$. Suppose that the input message from the source is

$$01101010001001011101101101010001010100101110\dots$$

Encode it with $H_2(4)$.

Suppose now that in the transmission of a message encoded with such Hamming code a single bit of a codeword c is corrupted, and instead of c you get a binary string \bar{c} given by

$$\bar{c} = 010011101010101$$

Identify the corrupted bit, correct it, and decode the result.

2 Quantum Information

EXERCISES

2.1 Let AB be a bipartite system. Many copies of the system in a state ρ are available. Alice carries measurements on A , and Bob on B . By exchanging information classically they can determine how their outcomes are correlated and thus they can measure the mean value of any observable of the form $X_A \otimes Y_B$. 1/ Prove that this is sufficient to know the expectation value of any observable of the compound system. 2/ Would this remain true if the Hilbert space was a real linear space instead of a complex vector space?

2.2 A Schmidt decomposition for n -partite pure states would be of the form

$$|\Psi\rangle = \sum_j \sqrt{p_j} |j\rangle_1 \otimes |j\rangle_2 \otimes \dots \otimes |j\rangle_n,$$

with $p_j > 0$, $\sum_j p_j = 1$, $\{|j\rangle_i\}$ an orthonormal basis in \mathcal{H}_i . Prove that such a decomposition does not exist in general for $n \geq 3$.

2.3 Consider the Werner state of a pair of qN -its

$$\rho_\Phi(\lambda) := \lambda |\Phi\rangle\langle\Phi| + (1 - \lambda) \frac{1}{N^2} \mathbf{1},$$

where

$$|\Phi\rangle := \frac{1}{\sqrt{N}} \sum |j\rangle \otimes |j\rangle$$

is a maximally entangled state vector, $\{|j\rangle\}$ being an orthonormal basis in \mathbb{C}^N . Find for what values of λ is nonpositive the partial transpose of $\rho_\Phi(\lambda)$.

2.4 Consider the expansion channel $\mathcal{E} : \rho_A \mapsto \rho_A \otimes \rho_{B,0}$. Find a Kraus form for \mathcal{E} .

2.5 Prove that if $F = \{F_y : y \in Y\}$ is a positive-operator valued measure (POVM) in a Hilbert space \mathcal{H} of dimension $\dim \mathcal{H} =: N = |Y|$ such that all F_y are rank 1, then F is a von Neumann measurement.

2.6 Prove that a quantum operation \mathcal{E} is invertible iff it is a unitary map.

2.7 1/ Prove that any quantum operation from a single qubit system to itself is of the form

$$\rho' := \mathcal{E}(\rho) = \sum_{\alpha\beta} \mathcal{E}_{\alpha\beta} \sigma_\alpha \rho \sigma_\beta,$$

where Greek indices run from 0 to 3, $\sigma_0 := \mathbf{1}_2$, and the coefficients $\mathcal{E}_{\alpha\beta}$ satisfy $\mathcal{E}_{\alpha\beta} = \mathcal{E}_{\beta\alpha}^*$. 2/ Which other conditions must $\mathcal{E}_{\alpha\beta}$ fulfill? 3/ Show

that the polarizations \mathbf{P}, \mathbf{P}' of ρ, ρ' are related by an affine transformation: $\mathbf{P}' = \mathbf{a} + M\mathbf{P}$, where M is a real matrix.

2.8 The transposition in a fixed basis is a linear anti-automorphism of the algebra $\mathcal{B}(\mathcal{H})$ of observables: $(AB)^t = B^t A^t$. Show explicitly that the associated map $\Phi^t : A \mapsto A^t$ is positive, but not 2-positive, provided that $\dim \mathcal{H} \geq 2$

2.9 Let $\mathcal{A} := \mathcal{B}(\mathcal{H})$. Let the linear maps $\text{Tr}((A_{i,j})) := \sum_i A_{i,i}$, $\sigma((A_{i,j})) := \sum_{i,j} A_{i,j}$, of $\mathcal{M}_n(\mathcal{A}) \rightarrow \mathcal{A}$. Prove that Tr and σ are completely positive.

2.10 Let $\mathcal{A} := \mathcal{B}(\mathcal{H})$. Let $A = (A_{i,j}) \in \mathcal{A}$, and consider the linear map $\text{Diag}(A) = \text{Diag}((A_{i,j})) := (B_{i,j})$, where $B_{i,j} = \delta_{i,j} A_{i,i}$. Prove: i/ $n \text{Diag}(A) - A$ is completely positive; ii/ $(n-1) \text{Diag}(A) - A$ is not positive.

2.11 A qubit has a pure state ψ chosen randomly on the Bloch sphere. Estimate the average fidelity of a random guess ϕ .

2.12 As above, let qubit have a pure state $|\psi\rangle$ chosen randomly on the Bloch sphere. Suppose that we measure its spin along the z -axis. The resulting state is $\rho := p_+|+\rangle\langle+| + p_-|-\rangle\langle-|$, where $p_{\pm} := |\langle \pm | \psi \rangle|^2$. Calculate the average fidelity with which ρ represents P_{ψ} .

2.13 Analyze whether the state ρ of 2 qutrits given by

$$\rho = \frac{1}{1080} \begin{pmatrix} 79 & -15 & -79 & -9 & 15 & -39 & 39 & -15 & -40 \\ -15 & 55 & 35 & -15 & -35 & -25 & -15 & 55 & 0 \\ -79 & 35 & 163 & 5 & -55 & -5 & 25 & 11 & 20 \\ -9 & -15 & 5 & 103 & 15 & 33 & -13 & 9 & -40 \\ 15 & -35 & -55 & 15 & 95 & 25 & 35 & -55 & 40 \\ -39 & -25 & -5 & 33 & 25 & 163 & -23 & -61 & -20 \\ 39 & -15 & 25 & -13 & 35 & -23 & 143 & -79 & 0 \\ -15 & 55 & 11 & 9 & -55 & -61 & -79 & 139 & 20 \\ -40 & 0 & 20 & -40 & 40 & -20 & 0 & 20 & 140 \end{pmatrix}$$

is separable or entangled.

2.14 The state $\rho_{A,B}$ of a two-qubit system is

$$\rho_{A,B} = \frac{1}{15} \begin{pmatrix} 4 & -1 & 2 & 1 \\ -1 & 3 & 1 & -3 \\ 2 & 1 & 2 & -1 \\ 1 & -3 & -1 & 6 \end{pmatrix}.$$

Calculate the mutual information $S(\rho_A : \rho_B)$ of the partial states of the two qubits.