Quantum Information Theory
Series 8

Exercise 8.1 Fano's Inequality

Given random variables X and Y, how well can we predict X given Y? Fano's inequality bounds the probability of error in terms of the conditional entropy $H(X|Y)$. The goal of this exercise is to prove the inequality

$$P_{\text{error}} \geq \frac{H(X|Y)-1}{\log|X|}.$$

1. Representing the guess of X by the random variable $\widehat{X}$, which is some function, possibly random, of Y, show that $H(X|\widehat{X}) \geq H(X|Y)$.
2. Consider the indicator random variable E which is 1 if $\widehat{X} \neq X$ and zero otherwise. Using the chain rule we can express the conditional entropy $H(E, X|\widehat{X})$ in two ways:

$$H(E, X|\widehat{X}) = H(E|X, \widehat{X}) + H(X|\widehat{X}) = H(X|E, \widehat{X}) + H(E|\widehat{X})$$

   Calculate each of these four expressions and complete the proof of the Fano inequality. Hints: For $H(E|\widehat{X})$ use the fact that conditioning reduces entropy: $H(E|\widehat{X}) \leq H(E)$. For $H(X|E, \widehat{X})$ consider the cases $E = 0, 1$ individually.

Exercise 8.2 Quantum mutual information

Consider a composed system $A \otimes B \otimes C$ with a shared state ρ_{ABC}.
In a first step we ignore system C and consider only $A \otimes B$ (and the reduced state $\rho_{AB} = \text{Tr}_C(\rho_{ABC})$). One way of quantifying the correlations between A and B is to use the *mutual information* between them, defined as

$$I(A:B) = H(A) + H(B) - H(AB) \quad (1)$$
$$= H(A) - H(A|B). \quad (2)$$

If we have access to C, we can define a conditional version of the mutual information between A and B as

$$I(A:B|C) = H(A|C) + H(B|C) - H(AB|C) \quad (3)$$
$$= H(A|C) - H(A|BC). \quad (4)$$

(a) Assume a system formed by two qubits A and B that share a state ρ_{AB}. Consider bases $\{|0\rangle_A, |1\rangle_A\}$ and $\{|0\rangle_B, |1\rangle_B\}$ for the subsystems of each qubit.

   1. Check that the mutual information of the fully entangled state , $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, is maximal.
   2. See that for classically correlated states, $\rho_{AB} = p|0\rangle\langle 0|_A \otimes \sigma_B^0 + (1-p)|1\rangle\langle 1|_A \otimes \sigma_B^1$ (where $0 \leq p \leq 1$), the mutual information cannot be greater than one.

(b) Consider the so-called *cat state* shared by four qubits, $A \otimes B \otimes C \otimes D$, that is defined as

$$|☺\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle). \quad (5)$$

   Check how the mutual information between qubits A and B changes with the knowledge of the remaining qubits, namely:

1. $I(A : B) = 1$.
2. $I(A : B|C) = 0$.
3. $I(A : B|CD) = 1$.

Exercise 8.3 Mutual Information in a weather bet

After losing a bet with your Scottish grandfather about whether listening to the radio forecast would help you predict the weather, you have been studying information theory compulsively to try to come up with a clever argument that would make him stop mocking you. You are convinced that even though you did not guess correctly more often than he, you somehow have more *information* about the weather than he does.

a) The mutual information between two random variables is given by

$$I(X : Y)_P = H(X)_P - H(X|Y)_P,$$

where $H(X)$ is the Shannon entropy of X,

$$H(X)_P = \langle -\log P_X(x) \rangle_x = -\sum_x P_X(x) \log P_X(x)$$

and $H(X|Y)$ is the conditional Shannon entropy of X given Y,

$$H(X|Y)_P = \langle -\log P_{X|Y=y}(x) \rangle_{x,y} = -\sum_{x,y} P_{XY}(x, y) \ \log P_{X|Y=y}(x) = H(XY)_P - H(Y)_P.$$

Compute the mutual information between your guess and the actual weather, and do the same for your grandfather. Remember that your grandfather knows it rains on 80% of the days. You also listen to the forecst, knowing it is right 80% of the time and always correct when it predicts rain.

b) You devise the following betting game to prove that your extra information is useful. You and your grandfather start with £1. Every night each of you can bet part of your money on the next day's weather. If your guess was right you double the amount you bet (e.g., in the first night your grandfather bets £0.2 on rain; if it rains he ends up with £1.2, otherwise with £0.8). Any winnings can be used in future rounds.

What would your strategy be? And your grandfather's? After N days, what is the expected gain for each of you? And what is the probability that he finishes with more money than you?