Quantum Information Theory
Series 3

HS 13
Dr. J.M. Renes

Exercise 3.1 Asymptotic Equipartition

Let (X_i, Y_i) be a sequence of n i.i.d pairs of random variables, meaning that $P_{X_1Y_1...X_nY_n} = P_{XY}^{\times n}$. Also, let $\epsilon_n = \frac{\sigma^2}{n\delta^2}$ for some $\delta > 0$, and σ^2 be the variance of the conditional surprisal $h(X|Y) = -\log_2 P_{X|Y}$. Use the weak law of large numbers to prove the asymptotic equipartition lemma:

$$\lim_{n\to\infty} \frac{1}{n} H_{\min}^{\epsilon_n}(X_1...X_n|Y_1...Y_n)_{P^n} = H(X|Y)_{P_{XY}}.$$
$$\lim_{n\to\infty} \frac{1}{n} H_{\max}^{\epsilon_n}(X_1...X_n|Y_1...Y_n)_{P^n} = H(X|Y)_{P_{XY}}.$$

Exercise 3.2 Data Processing Inequality

Random variables X, Y, Z form a Markov chain $X \to Y \to Z$ if the conditional distribution of Z depends only on Y: $p(z|x,y) = p(z|y)$. The goal in this exercise is to prove the data processing inequality, $I(X : Y) \geq I(X : Z)$ for $X \to Y \to Z$.

1. First show the chain rule for mutual information: $I(X : YZ) = I(X : Z) + I(X : Y|Z)$, which holds for arbitrary X, Y, Z. The conditional mutual information is defined as

$$I(X : Y|Z) = \sum_z p(z) I(X : Y|Z = z) = \sum_z p(z) \sum_{x,y} p(x,y|z) \log \frac{p(x,y|z)}{p(x|z)p(y|z)}.$$

2. Next show that in a Markov chain $X \to Y \to Z$, X and Z are conditionally independent given Y; that is, $p(x,z|y) = p(x|y)p(z|y)$.

3. By expanding the mutual information $I(X : YZ)$ in two different ways, prove the data processing in equality.

Exercise 3.3 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.