INFORMATION THEORY
Master of Logic, Master AI, Master CS, University of Amsterdam, 2019
TEACHERS: Christian Schaffner, Yfke Dulek TAs: Esteban Landerreche, Maximilian Siemers

Practice problem set 4

This week's exercises deal with AEP and encryption. You do not have to hand in these exercises, they are for practicing only. During the work session, start with solving the exercises you may be presenting. Work out a full solution on paper/computer and get it approved by the teacher. Make sure that all your team members really understand the solution. Also think about the following questions: What is the point of the exercise? What kind of problems will students encounter when solving this problem? What kind of questions could be asked on Friday? Problems marked with a ★ are generally a bit harder. If you have questions about any of the exercises, please post them in the discussion forum on Canvas, and try to help each other. We will also keep an eye on the forum.

Problem 1: AEP and source coding

A discrete memoryless source emits a sequence of of statistically independent binary digits with probabilities $P_X(1) = 0.005$ and $P_X(0) = 0.995$. The digits are taken 100 at a time and a binary codeword is provided for every sequence of 100 digits containing three or fewer 1's.

(a) Assuming that all codewords are the same length, find the minimum length required to provide codewords for all sequences with three or fewer 1's.

(b) In the first homework problem set, you were asked to prove Markov's inequality. Use it to bound the probability of observing a source sequence for which no codeword has been assigned.

(c) In the first homework problem set, you were also asked to prove Chebyshev's inequality. Use it to bound the probability of observing a source sequence for which no codeword has been assigned.

(d) Calculate the actual probability of observing a source sequence for which no codeword has been assigned. Compare this number with the bounds computed in part (b) and (c).

Problem 2: The middle part of the entropy diagram

Show that the value

$$R(X;Y;Z) = I(X;Y) - I(X;Y|Z)$$

is invariant under permutations of its arguments, using only the definitions and properties on the canvas page for mutual information and conditional mutual information.

Problem 3: Entropy Inequalities

For each statement below, specify a joint distribution P_{XYZ} of random variables X, Y, and Z (P_{XY} of X and Y in (a)) such that the following inequalities hold.

(a) There exists a y such that $H(X|Y = y) > H(X)$.

(b) $I(X;Y) > I(X;Y|Z)$

(c) $I(X;Y) < I(X;Y|Z)$

Problem 4: Conditional mutual information

Consider a sequence of n binary random variables $X_1, X_2, ..., X_n$. Each sequence with an even number of 1's has probability $2^{-(n-1)}$ and each sequence with an odd number of 1's has probability 0. Find the mutual informations

$$I(X_1;X_2), I(X_2;X_3|X_1), ..., I(X_{n-1};X_n|X_1, ..., X_{n-2}).$$

Problem 5: Independence?

Let (X_i, Y_i) be drawn i.i.d. according to P_{XY}. We compare the hypothesis that X and Y are independent to the hypothesis that they are dependent, by defining a random variable

$$Z_n := \frac{P_{X^n}(X^n)P_{Y^n}(Y^n)}{P_{X^nY^n}(X^n, Y^n)}.$$

What does $\frac{1}{n}\log Z_n$ converge to in probability? (**Hint:** look at the proof of the AEP for inspiration.)

Problem 6: Bernoulli typical sets

Let X_i be i.i.d. random variables, distributed according to a Bernoulli(p) distribution: that is, $P_{X_i}(1) = p$ and $P_{X_i}(0) = 1-p$. Denote with $A_\varepsilon^{(n)}(p)$ the typical set for $X_1, ..., X_n$.

(a) For arbitrary $\varepsilon > 0$, what is $A_\varepsilon^{(n)}(1/2)$?

(b) Prove that for any $0 \leq p < q \leq 1/2$, there exists an $\epsilon > 0$ such that for big enough n, it holds that $|A_\varepsilon^{(n)}(p)| < |A_\varepsilon^{(n)}(q)|$.

★ Prove that for any $0 \leq p < q \leq 1$ such that $p \neq \frac{1}{2}$ and $q \neq \frac{1}{2}$, there exists an $\epsilon > 0$ such that for big enough n, it holds that $A_\varepsilon^{(n)}(p) \cap A_\varepsilon^{(n)}(q) = \emptyset$.