Information Theory, Coding and Cryptography

Homework Set 1

Please send your answers – either typeset on a computer, or handwritten (but readable) and scanned, preferably in PDF format – to `bouman@cwi.nl` *before February 16, 23h59. Do not forget to put your name on the first page. Good luck!*

1 Shuffling Cards

a) [1 point] Compute the entropy of a perfectly shuffled (i.e. uniformly distributed over all possible orders) deck of 52 playing cards.

Now suppose we have a perfectly shuffled big deck, consisting of two *identical* decks of 52 cards (so 104 cards in total).

b) [2 points] Compute the entropy of the shuffled big deck.

2 Monty Hall

The Monty Hall problem is a famous puzzle in probability theory, based on the American TV show "Let's make a deal", which was broadcast in the sixties and seventies. Monty Hall is the name of the show's quizmaster.

In the game, the player is given the choice between three doors. Behind one of the doors, the quizmaster has hidden a prize, and he has selected this door uniformly at random. Let this position be X. Then, the player announces her choice, Y, and Y is independent from X. (Y's distribution is unknown to us.) Formally, $P_X(1) = P_X(2) = P_X(3) = 1/3$ and $P_{XY} = P_X \cdot P_Y$. Next, the quizmaster opens door Z. He chooses Z such that $Z \neq X$ and $Z \neq Y$. In case $X = Y$, the quizmaster picks Z uniformly at random from the two possible choices. (In case $X \neq Y$, Z is already fully determined.) Then the player is asked if she wants to change her initial choice.

a) [4 points] Find the conditional probability distribution $P_{X|YZ}(x|y,z)$.

b) [1 point] Should the player change doors to increase the odds of winning? Why?

c) [3 points] Determine the conditional entropies $H(X|X)$, $H(X|Y)$ and $H(X|YZ)$. These quantities can be respectively interpreted as the quizmaster's uncertainty about X, and the player's uncertainty about X before and after the quizmaster opens Z.

d) [2 points] Compute the mutual information $I(X;Z|Y)$.

3 Throwing Dice

Consider the following random experiment with two fair dice. First, the first die is thrown, and let the outcome be A. Then, the second die is thrown until the outcome has the same parity (even, odd) as A. Let this final outcome of the second die be B. The random variables X, Y, and Z are defined as follows:

$$X = (A + B) \mod 2, \quad Y = (A \cdot B) \mod 2, \quad Z = |A - B|.$$

a) [1 point] Find the joint distribution P_{AB}.

b) [2 points] Determine $H(X)$, $H(Y)$ and $H(Z)$.

c) [1 point] Compute $H(Z|A = 1)$.

d) [2 points] Compute $H(AB)$, i.e. the joint entropy of A and B.

e) [2 points] A random variable M describes whether the sum $A + B$ is larger than seven, between five and seven, or smaller than five. How much entropy is present in this random variable M?

4 Relative Entropy

For two distributions P and Q over $\mathcal{X}$, the relative entropy or *Kullback-Leibler divergence* is defined as

$$D(P||Q) := \sum_{x \in \mathcal{S}_P} P(x) \log \frac{P(x)}{Q(x)}$$

where $\mathcal{S}_P := \{x \in \mathcal{X} : P(x) > 0\}$. Note that if $Q(x) = 0$ for some $x \in \mathcal{S}_P$, then $D(P||Q) = \infty$.

a) [5 points] Prove that $D(P||Q) \geq 0$, and that equality holds if and only if $P = Q$. **Hint:** Use Jensen's inequality.

b) [3 points] Show that the mutual information can be defined in terms of the relative entropy, i.e. that

$$I(X;Y) = D\big(P_{XY}||P_X P_Y\big)$$

c) [1 point] Use this to prove that $H(X|Y) \leq H(X)$.

5 Entropy, Mutual Information and Inequalities

a) [6 points] Show that the value

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

is invariant under permutations of its arguments.

b) [8 points] Let X, Y, Z be arbitrary random variables, and let f be any deterministic function acting on $\mathcal{Y}$. In the following, replace "?" by "$\geq$" or "$\leq$" to obtain the correct inequalities, and reason each time with the help of an entropy diagram. **Hint:** $H(f(Y)|Y) = 0$.

1. $H(f(Y))\,?\,H(Y)$
2. $I(X;f(Y))\,?\,I(X;Y)$
3. $H(X|f(Y))\,?\,H(X|Y)$
4. $I(X;Z|Y) = 0$ implies $I(X;Z)\,?\,I(X;Y)$ and $I(X;Z)\,?\,I(Y;Z)$.

c) [6 points] For each statement below, specify random variables X, Y and Z (X and Y in 1.) such that the inequalities hold.

1. There exists a y, such that $H(X|Y = y) > H(X)$
2. $I(X;Y) > I(X;Y|Z)$
3. $I(X;Y) < I(X;Y|Z)$