ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Handout 5 Information Theory and Coding

Homework 3 October 12, 2007

PROBLEM 1. Let X, Y and Z be binary valued discrete random variables.

(a) Find a joint probability assignment $P(x, y, z)$ such that $I(X; Y) = 0$ and $I(X; Y|Z) =$ 1 bit.

(b) Find a joint probability assignment $P(x, y, z)$ such that $I(X, Y) = 1$ bit and $I(X; Y|Z) = 0$.

The point of the problem is that no general inequality exists between $I(X, Y)$ and $I(X; Y|Z)$.

PROBLEM 2. Consider a cryptographic system in which we wish to encrypt a source X with entropy $H(X)$ using a secret key K with entropy $H(K)$. There is a function $f(x, k)$ that maps the source X and the key K to the encrypted output Y. This function is decryptable in the sense that for each key k, $f(x_1, k) \neq f(x_2, k)$ for source letters $x_1 \neq x_2$. Assume that X and K are independent random variables. Assume also that the encryption scheme has the property that $I(X; Y) = 0$, which is to say that the observation of the output y provides no information about the source if one does not know the key.

(a) Find the value of the following quantities in terms of $H(X)$ and $H(K)$.

(i) $H(X|Y)$

(ii) $H(X|K)$

(iii) $H(Y|X, K)$

(iv) $H(X|Y, K)$

(v) $I(X; Y|K)$

(vi) $H(Y|K)$

(b) Suppose now and for the rest of the problem, that all the source letters x have a positive probability $\Pr(X = x)$. Fix an output y_0 with positive probability, and let $\mathcal{K}(x)$ be the set of keys k for which $f(x, k) = y_0$. Show that $\mathcal{K}(x_1)$ and $\mathcal{K}(x_2)$ are disjoint when $x_1 \neq x_2$. [Hint: the decryptability condition says that from an output y and key k it is possible to uniquely determine the source letter x which produced the output y.]

(c) Suppose, in addition, and for the rest of the problem, that the number of keys is the same as the number of source letters. Using part (b) show that each set $\mathcal{K}(x)$ contains a single element.

(d) Let the single element of $\mathcal{K}(x)$ of part (c) be denoted by $k(x)$. Show that

$$\Pr(Y = y_0|X = x) = \Pr[K = k(x)]$$

(e) Using $I(X; Y) = 0$ conclude that for all x, $\Pr(Y = y_0|X = x) = \Pr(Y = y_0)$. Using part (d), conclude that $\Pr[K = k(x)]$ does not depend on x. Show that K is uniformly distributed.

PROBLEM 3. For a stationary process $X_1, X_2, \ldots$, show that

(a) $\frac{1}{n}H(X_1, \ldots, X_n) \leq \frac{1}{n-1}H(X_1, \ldots, X_{n-1})$.

(b) $\frac{1}{n}H(X_1, \ldots, X_n) \geq H(X_n|X_{n-1}, \ldots, X_1)$.

PROBLEM 4. Let $\{X_i\}_{i=-\infty}^{\infty}$ be a stationary stochastic process. Prove that

$$H(X_0|X_{-1}, \ldots, X_{-n}) = H(X_0|X_1, \ldots, X_n).$$

That is: the conditional entropy of the present given the past is equal to the conditional entropy of the present given the future.

PROBLEM 5. Show, for a Markov chain, that

$$H(X_0|X_n) \geq H(X_0|X_{n-1}), \quad n \geq 1.$$

Thus, initial state X_0 becomes more difficult to recover as time goes by.

PROBLEM 6. Let $X_1, X_2, \ldots$ be i.i.d., each with probability distribution $p(x)$. Let f be any function on the space of the random variables X_i. Show that with probability one

$$\lim_{n\to\infty} \left(\Pi_{i=1}^{n} f(X_i)\right)^{1/n}$$

exists, and find its value. Hint: use the AEP.

Now consider the following gambling game. At the n-th stage, you have an amount S_n. The casino tosses a fair coin. If the coin turns up heads, the casino doubles your amount(i.e., $S_{n+1} = 2S_n$). If the coin turns up tails, you give back two-thirds of your amount to the casino(i.e., $S_{n+1} = \frac{1}{3}S_n$). You start the game with 1 franc($S_1 = 1$).

(a) Evaluate $\lim_{n\to\infty} S_n^{1/n}$.

(b) Evaluate $\lim_{n\to\infty} S_n$.

(c) Evaluate $E(S_n)$.

(d) Is it true that $E\lim_{n\to\infty} S_n = \lim_{n\to\infty} E(S_n)$?