Homework Set #2

Due 8 October 2009, 6 pm, in INR036

Problem 1 (Secrecy Scenario)

Let X be the plain text, Y be the cipher text, and Z be the key in a secret key cryptosystem. Since X can be recovered from Y and Z, we have $H(X|Y,Z)=0$. Show that

$$I(X;Y) \geq H(X) - H(Z).$$

Problem 2 (Conditional Mutual Information)

Define $I(X_1;X_2;X_3) = I(X_1;X_2) - I(X_1;X_2|X_3)$.

(a) Prove or disprove $I(X_1;X_2;X_3) \geq 0$.

(b) Show that

$$-\min\{I(X_1;X_2|X_3), I(X_1;X_3|X_2), I(X_2;X_3|X_1)\} \leq I(X_1;X_2;X_3)$$

(c) Show that

$$I(X_1;X_2;X_3) \leq \min\{I(X_1;X_2), I(X_1;X_3), I(X_2;X_3)\}$$

Problem 3

Let the random variable X be a message we want to send to a receiver (receiver 1) and a good approximation $\hat{X}$ is required at that receiver. Consider another receiver, named receiver 2, which has access to a random variable Z, where Z and X are from a joint distribution $p(x,z)$. Receiver 2 is interested in another approximation of X, denoted by $\check{X}$. Imagine the encoding strategy is as follows. The encoder describes X, by $S = f_1(X)$, where S is such that we can find $\hat{X}$ as a function of S ($\hat{X} = f_2(S)$). Imagine that T is constructed from S ($T = f_3(S)$), such that $\check{X}$ is then found as a function of Z and T ($\check{X} = f_4(T,Z)$). This system is shown in Fig. 2. Show that

$$I(X;\check{X}) \leq I(X;\hat{X}) + I(X;SZ|\hat{X}).$$

Problem 4

Let $P = (p_1, \cdots, p_i, \cdots, p_j, \cdots, p_n)$ be a probability distribution.
(a) Show that the distribution $(p_1, \cdots, \frac{p_i+p_j}{2}, \cdots, \frac{p_i+p_j}{2}, \cdots, p_n)$ has a larger entropy than the original distribution.
(b) In general, let $A = [a_{i,j}]$ be a $n \times n$ stochastic matrix such that $0 \leq a_{i,j} \leq 1$, $\sum_{i=1}^n a_{ij} = 1$ and $\sum_{j=1}^n a_{ij} = 1$ for all $1 \leq i,j \leq n$. Prove that PA has a larger entropy than P. Try to do this using Jensen's inequality.

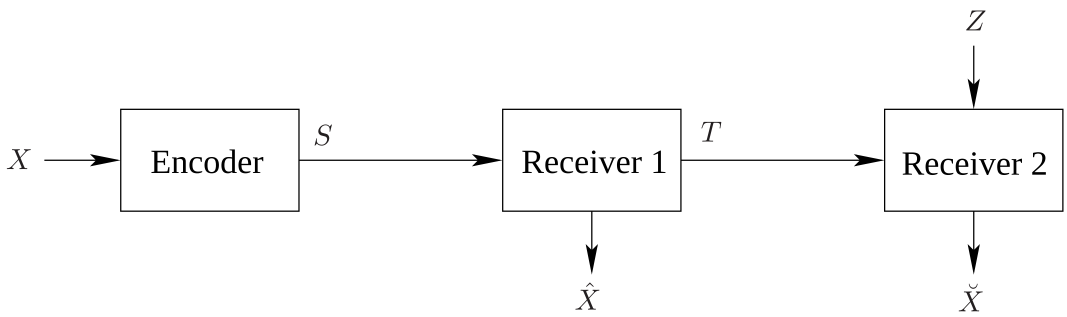

Figure 1: Transmission system in Problem 5.

Problem 5 (Sufficient Statistics)

Suppose that we have a family of probability mass functions $\{f_\theta(x)\}$ indexed by θ, and let X be a sample from a distribution in this family. Let $T(X)$ be any statistic (e.g. sample mean or sample variance is a possible statistic.)

(a) Show that

$$I(\theta; T(X)) \leq I(\theta; X)$$

for any distribution on θ.
A statistic $T(X)$ is called sufficient if equality holds for any distribution on θ, or equivalently if $\theta \to T(X) \to X$ forms a Markov chain for all distributions on θ.

(b) Let $f_\theta = \text{Uniform}(\theta, \theta + 1)$. Show that a sufficient statistic for θ is

$$T(X_1, X_2, \ldots, X_n) = (\max\{X_1, X_2, \ldots, X_n\}, \min\{X_1, X_2, \ldots, X_n\}).$$

Hint: To this end, you should show that

$$\Pr\{(X_1, X_2, \ldots, X_n) = (x_1, x_2, \ldots, x_n) | m, M\},$$

does not depend on θ for a fixed n where

$$m = \min\{x_1, x_2, \ldots, x_n\},$$

and

$$M = \max\{x_1, x_2, \ldots, x_n\}.$$