Random codes in communication   11 June 2010
(Dr. Permuter Haim and Mr. Iddo Naiss)

Final Exam
Total time for the exam: 3 hours!

This is a honor code assignment and each student should do it totaly by himself/herself. Please copy and sign the sentence below on your assignment (an assignment without the following sentence won't be graded.)

"I am respecting the honor code of this assignment: Signature_____"

1) **True or False** (35 points)
   Copy each relation to your notebook and write **true** or **false**. Then, if it's true, prove it. If it is false give a counterexample or prove that the opposite is true.

   a) Let X, Y be two independent random variables. Then
   $$H(X - Y) \geq H(X).$$

   b) Let $A, B, C.D$ be random variables with a finite alphabet that form the Markov chain $A - B - C - D$, namely $P(a, b, c, d) = P(a)P(b|a)P(c|b)P(d|c)$. Then,
   $$I(A; C|D) \leq H(B).$$

   c) For any finite alphabet random variables
   $$H(X, Y, Z) - H(X, Y) \leq H(X, Z) - H(X).$$

   d) Let $\{X_i\}_{i \geq 1}$ be an i.i.d. source distributed according to P_X. In addition, let $\{Y_i\}_{i \geq 1}$ and $\{Z_i\}_{i \geq 1}$ be two i.i.d. side information sequences that may be available at the encoder and decoder of a lossless source coding setting. If $I(X; Y) > I(X; Z)$, then the minimum rate that is needed to compress $\{X_i\}_{i \geq 1}$ losslessly with side information $\{Y_i\}_{i \geq 1}$ is smaller than the minimum rate that is needed to compress $\{X_i\}_{i \geq 1}$ losslessly with with side information $\{Z_i\}_{i \geq 1}$. Assume the side information is known both to the encoder and decoder.

   e) Suppose that (X, Y, Z) are jointly Gaussian and that $X - Y - Z$ forms a Markov chain. Let X and Y have correlation coefficient ρ_1 and let Y and Z have correlation coefficient ρ_2. Let the variance of each random variable X, Y, and Z be 1. be Let $g(z)$ be any deterministic function. Then
   $$h(X|g(Z)) \geq \frac{1}{2} \log 2\pi e (1 - \rho_1^2 \rho_2^2).$$

   f) If $f(x, y)$ is a convex function in the pair (x, y), then for a fixed y, $f(x, y)$ is convex in x, and for a fixed x, $f(x, y)$ is convex in y.

   g) If for a fixed y the function $f(x, y)$ is a convex function in x, and for a fixed x, $f(x, y)$ is convex function in y, then $f(x, y)$ is convex in the pair (x, y). (Examples of such functions are $f(x, y) = f_1(x) + f_2(y)$ or $f(x, y) = f_1(x)f_2(y)$ where $f_1(x)$ and $f_2(y)$ are convex.)

2) **Entropy and source coding of a source with infinite alphabet**(15 points)
   Let X be an i.i.d. random variable with an infinite alphabet, $\mathcal{X} = \{1, 2, 3, ...\}$. In addition let $P(X = i) = 2^{-i}$.

   a) What is the entropy of the random variable?
   b) Find an optimal variable length code, and show that it is indeed optimal.

3) **Empirical distribution of a sequence** (20 points)

A fair dice with 6 faces was thrown n times, where n is a very large number.

  a) Using Stirling approximation $n! \approx (\frac{n}{e})^n$, find how many different sequences there exists with an empirical pmf $(p_1, p_2, ..., p_6)$, where p_i is the portion of the sequence that is equal to $i \in \{1, 2, ..., 6\}$.

  b) Now, we were told that the portion of odd numbers in the sequence is $2/3$ (i.e., $p_1 + p_3 + p_5 = 2/3$). For n very large, what is the most likely empirical pmf of the sequence.

4) **For a Gaussian input in an additive channel, the worse noise is Gaussian.** (30 points)
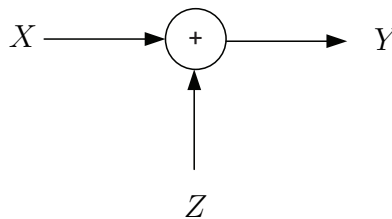

Fig. 1.   Fig. 1. An additive channel

Prove, that for an additive $Y = X + Z$ channel with Gaussian input, and power constraint

$$\frac{1}{n} \sum_{i=1}^{n} X_i^2 \leq P, \text{ with probability } 1$$

the worse noise with varaince $V(Z) \leq N$ is a Gaussian noise. We use the following notation: when a random variable X has a Gaussian distribution we denote it by X_G.

In short, prove that for $Y = X_G + Z$, where $V(Z) \leq N$

$$I(X_G; Y) \geq \frac{1}{2} \log(1 + \frac{P}{N}) = I(X_G; X_G + Z_G),$$

where $Z_G \sim N(0, N)$.

You can prove it on your own, or use the following steps

(a) Prove that for every $\alpha \in \mathbb{R}$,

$$I(X_G; Y) \geq \frac{1}{2} \log(2\pi e P) - \frac{1}{2} \log(2\pi e E((X_G - \alpha Y)^2)),$$

and justify your steps.

(b) Find such α that minimize $E((X_G - \alpha Y)^2)$, i.e., αY is the best linear approximation of X_G (hint: the orthogonality principle, or by differentiating).

(c) Using the parameter α you found, finish the question.

Conclude, what would you have done, as an adversary (someone who oppose the communication, and wants to block it), if you found out the encoder is using a Gaussian codebook?

Good Luck!