ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 30 | Information Theory and Coding
Final Exam | Jan. 22, 2015

4 problems, 100 points
3 hours
4 sheets (8 pages) of notes allowed

Good Luck!

PLEASE WRITE YOUR NAME ON EACH SHEET OF YOUR ANSWERS

PLEASE WRITE THE SOLUTION OF EACH PROBLEM ON A SEPARATE SHEET

PROBLEM 1. (25 pts) Suppose that $\{U_i\}$ is a stationary stochastic process with $U_i \in \{0,1\}$. Let $p_i = \Pr(U_i = 0)$, $a_i = \Pr(U_{i+1} = 1|U_i = 0)$, $b_i = \Pr(U_{i+1} = 0|U_i = 1)$.

(a) (5 pts) Show that $p_{i+1} = p_i(1-a_i) + (1-p_i)b_i$.

(b) (5 pts) Show that the quantities p_i, a_i, b_i do not change with i.

(c) (5 pts) Show that the entropy rate of the process U is upper bounded by

$$ph_2(a) + (1-p)h_2(b)$$

where $h_2(t) = -t\log_2(t) - (1-t)\log_2(1-t)$ is the binary entropy function.

(d) (5 pts) Given $a, b \in [0,1]$, show that among all binary-valued stationary stochastic processes with $P(U_{i+1} = 1|U_i = 0) = a$ and $P(U_{i+1} = 0|U_i = 1) = b$, the Markov processes has the highest entropy rate.

(e) (5 pts) Suppose $\{U_i\}$ is a binary-valued stationary process for which every 1 is immediately followed by a 0. Show that the largest possible entropy rate for such a process is equal to $\max\limits_{a\in[0,1]} \dfrac{h_2(a)}{1+a}$.

PROBLEM 2. (20 points) Given a discrete memoryless channel W and an input distribution Q let P denote the output distribution induced by Q, i.e., $P(y) = \sum_x Q(x)W(y|x)$. Let Q^* be a capacity achieving input distribution and let P^* be the corresponding output distribution. Let C denote the capacity of W.

(a) (5 pts) Show that

$$\sum_{x,y} Q^*(x)W(y|x)\log\frac{W(y|x)}{P(y)} \geq \sum_{x,y} Q^*(x)W(y|x)\log\frac{W(y|x)}{P^*(y)}.$$

[Hint: express the difference of left and right sides as a divergence]

(b) (5 pts) Show that

$$\max_x \sum_y W(y|x)\log\frac{W(y|x)}{P(y)} \geq C.$$

(c) (5 pts) What is the value of $\max_x \sum_y W(y|x)\log\frac{W(y|x)}{P^*(y)}$?

[Hint: use the Kuhn-Tucker conditions on the capacity achieving distribution.]

(d) (5 pts) Show that the channel capacity can be found as the value of a minimization:

$$C = \min_Q \max_x \sum_y W(y|x)\log\frac{W(y|x)}{P(y)}.$$

PROBLEM 3. (35 points) The Z-channel with crossover probability p (denoted Z(p)) is a channel with input $\mathcal{X} = \{0, 1\}$, output alphabet $\mathcal{Y} = \{0, 1\}$ and

$$P(0|0) = 1, \quad P(1|1) = 1 - p, \quad P(0|1) = p.$$

Say that an input symbol x and an output symbol y are *incompatible* if $x = 0$ and $y = 1$, otherwise, say that they are *compatible.*

(a) (5 pts) Let X and $\tilde{X}$ be i.i.d. with $P(X = 0) = 1/2$. Suppose X is transmitted over a Z(p) and Y is the channel output. Find the probability that $\tilde{X}$ and Y are compatible; call this value $\alpha(p)$. Find the probability that $\tilde{X}$ and Y are compatible, conditional on $Y = 1$; call this number by $\beta(p)$).

Say that a sequence $(x_1, \ldots, x_n)$ of input symbols and $(y_1, \ldots, y_n)$ of output symbols are compatible if x_i and y_i are compatible for every $i = 1, \ldots, n$.

(b) (5 pts) Let $X_1, \ldots, X_n, \tilde{X}_1, \ldots, \tilde{X}_n$ be i.i.d. as in (a). Suppose $X^n = (X_1, \ldots, X_n)$ is transmitted over a Z(p) and $Y^n = (Y_1, \ldots, Y_n)$ is the channel output. What is the probability that $\tilde{X}^n$ and Y^n are compatible? Express your answer in terms of n and $\alpha(p)$.

(c) (5 pts) Under the same assumptions as in (b), what is the probability that $\tilde{X}^n$ and Y^n are compatible, conditional on Y^n containing k 1's. Express your answer in terms of k and $\beta(p)$.

Suppose we construct a random code with M codewords of blocklength n

$$X^n(1), \ldots, X^n(M)$$

by choosing each $X_i(m)$ independently, each distributed as in (a). To communicate the message m, the transmitter sends $X^n(m)$ over a Z(p). Upon receiving the channel output Y^n, the receiver declares $\hat{m}$ if $\hat{m}$ is the only message for which $X^n(\hat{m})$ and Y^n are compatible. If there is no such $\hat{m}$ the receiver declares 0.

(d) (10 pts) Use (b) to show that reliable communication over Z(p) is possible as long as the communication rate R is less than $R_0 = -\log \alpha(p)$.

(e) (10 pts) Use (c) to show that reliable communication over Z(p) is possible as long as the communication rate R is less than $R_1 = -\frac{1-p}{2} \log \beta(p)$. [Hint: first argue that the number of 1's in Y^n will be close to $n\frac{1-p}{2}$ with high probability.]

Problem 4. (20 points) Suppose that $\mathcal{C}$ is a binary linear code with $M = 2^k$ codewords with blocklength n.

(a) (5 pts) For $i = 1, \ldots, n$, let Z_i be the number of codewords $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{C}$ for which $x_i = 0$. Show that for each i either $Z_i = M$ or $Z_i = M/2$.

(b) (5 pts) Suppose X^n is the input of memoryless channel W, and Y^n is the channel output. Show that

$$I(X^n; Y^n) \leq \sum_{i=1}^{n} I(X_i; Y_i)$$

with equality if and only if $(Y_1, \ldots, Y_n)$ are independent.

(c) (5 pts) Suppose X^n is chosen uniformly from the binary linear code $\mathcal{C}$ and sent over a binary input channel W, and Y^n is the channel output. Show that for each i, either $I(X_i; Y_i) = 0$ or $I(X_i; Y_i) = I(W)$ where $I(W)$ is the 'symmetric capacity' of W.

[Note: The symmetric capacity of a channel W is the mutual information $I(X; Y)$ with X being a uniform input and Y being the output.]

(d) (5 pts) Show that for a binary input memoryless channel W, reliable communication is not possible at rates above $I(W)$ by using linear codes.