ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 25 Information Theory and Coding
Final Exam Jan. 23, 2013

4 problems, 125 points
180 minutes
4 sheets of notes allowed

Good Luck!

PLEASE WRITE YOUR NAME ON EACH SHEET OF YOUR ANSWERS

PLEASE USE A SEPARATE SHEET TO ANSWER EACH QUESTION

Problem 1. (35 points) Consider an encryption system, where the encoder and the decoder share a secret key K. The plaintext X is encrypted by the encoder to ciphertext $Y = f(X,K)$ and decrypted by the decoder by computing $X = g(Y,K)$. Here f and g are *deterministic* functions. Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{K}$ denote the alphabets of X, Y and K.

(a) (5 pts) What are the values of $H(Y|X,K)$ and $H(X|Y,K)$?

(b) (5 pts) Show that $H(Y|K) = H(X|K)$.

(c) (5 pts) Assume additionally that the key K is independent of X. Show that $H(Y) \geq H(X)$.

(d) (5 pts) Under the same assumption show that $H(Y|X) \leq H(K)$.

An encryption system is secure if $I(X;Y) = 0$, i.e., an eavesdropper who observes Y (but does not know K) learns nothing about X.

(e) (5 pts) Assume that the system is secure and suppose that K is independent of X. Show that $H(K) \geq H(X)$.

(f) (5 pts) Suppose that the functions f, g and the secret key K are chosen so that the system is secure regardless of the distribution of X (but still assuming that X and K are independent). Show that $H(K) \geq \log|\mathcal{X}|$.

(g) (5 pts) Show that for $\mathcal{X} = \mathcal{Y} = \mathcal{K} = \{0, \ldots, m-1\}$, the choice: K uniform on $\mathcal{K}$, $f(x,k) = (x+k) \bmod m$ and $g(y,k) = (y-k) \bmod m$ satisfies the assumptions of (f).

Problem 2. (35 points) Recall that a binary erasure channel with erasure probability p (denoted by BEC(p)) is a channel with input alphabet $\mathcal{X} = \{0, 1\}$, output alphabet $\mathcal{Y} = \{0, 1, e\}$ and the following transition probabilities

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

Say that an input symbol x and an output symbol y are *incompatible* if $P(y|x) = 0$, i.e., if (x, y) is either $(0, 1)$ or $(1, 0)$. Otherwise, say that x and y are *compatible*. Assume throughout that $0 < p < 1$.

(a) (5 pts) Let X and $\tilde{X}$ be i.i.d. with $P(X = 0) = P(X = 1) = 1/2$. Suppose that X is transmitted over a BEC(p) and Y is the received symbol at the channel output. What is the probability that X and Y are compatible? What is the probability that $\tilde{X}$ and Y are compatible?

Say that a sequence $(x_1, \ldots, x_n)$ of input symbols and a sequence $(y_1, \ldots, y_n)$ of output symbols are compatible if x_i and y_i are compatible for every $i = 1, 2, \ldots, n$.

(b) (5 pts) Let $X_1, \ldots, X_n, X_1', \ldots, X_n'$ be i.i.d. as in (a). Assume that $X^n = (X_1, \ldots, X_n)$ is transmitted over a BEC(p) and $Y^n = (Y_1, \ldots, Y_n)$ is the channel output. What is the probability that X^n and Y^n are compatible? What is the probability that $\tilde{X}^n$ and Y^n are compatible?

(c) (5 pts) Under the same assumptions as in (b), what is the probability that $\tilde{X}^n$ and Y^n are compatible, conditioned on Y^n containing exactly k erasure symbols e?

Suppose we construct a random code with M codewords of block length n

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

by choosing each $X_i(m)$, independently, each distributed as in (a). To communicate a message $m \in \{1, \ldots, M\}$, the transmitter sends $X^n(m) = (X_1(m), \ldots, X_n(m))$ over a BEC(p). Upon receiving Y^n, the receiver declares $\hat{m} \in \{1, \ldots, M\}$ if $\hat{m}$ is the *only* message for which $X^n(\hat{m})$ and Y^n are compatible. The receiver declares 0 if there is no such $\hat{m}$. Let P_e denote the probability that the decoder declares a value different than the message sent by the transmitter.

(d) (5 pts) Use part (b) to find an upper bound on P_e of the form $P_e \leq (M - 1)\alpha(p)^n$.

(e) (5 pts) From (d), up to which rate R_0 may we conclude that reliable communication over a BEC(p) is possible?

(f) (5 pts) Use part (c) to find an upper bound on P_e of the form

$$P_e \leq \Pr(Y^n \text{ contains more than } k \text{ erasures}) + (M - 1)\beta^{n-k}.$$

[Hint: The answer to (c) is an increasing function of k.]

(g) (5 pts) From (f), up to which rate R_1 may we conclude that reliable communication over a BEC(p) is possible? [Hint: Fix a $q > p$, and choose $k = nq$; then allow q to approach p.]

Problem 3. (25 points) Consider a communication channel with input (X_1, X_2) and output (A, Y), where

(i) A is a random variable independent of the channel input with $P(A = 1) = p$, and $P(A = 2) = 1 - p$.

(ii) $Y = X_A + Z$, where Z is a Gaussian with zero mean and variance 1, independent of both A and Z.

In other words, the receiver observes either $X_1 + Z$ or $X_2 + Z$, with probabilities p and $1 - p$, and also knows which of the two alternatives it has observed.

Assume that we have a power constraint of the form $E[X_1^2] + E[X_2^2] \leq 1$.

(a) (5 pts) Show that the mutual information between the input and the output is given by $I(X_1, X_2; Y|A)$.

(b) (5 pts) Find $h(Y|X_1, X_2, A)$.

(c) (5 pts) Find an upper bound on $h(Y|A = 1)$ in terms of $E[X_1^2]$. State the conditions for equality.

(d) (5 pts) Show that the capacity of the channel is achieved when X_1 and X_2 are zero mean and Gaussian. Is it necessary for them to be independent? Is it necessary for them to be jointly Gaussian?

(e) (5 pts) For Gaussian and zero mean X_1, X_2, find the mutual information between the input and the output of the channel as a function of $(p, E[X_1^2], E[X_2^2])$ and describe how to allocate the total power of 1 unit between X_1 and X_2 as a function of p to achieve the capacity.

PROBLEM 4. (30 points) Suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ are binary linear codes of blocklength n.

Denote the number of codewords of $\mathcal{C}_i$ by M_i and the minimum distance of $\mathcal{C}_i$ by d_i.

For $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$ let $\langle \mathbf{u}|\mathbf{v} \rangle$ denote the concatenation of the two sequences, i.e.,

$$\langle \mathbf{u}|\mathbf{v} \rangle = (u_1, \ldots, u_n, v_1, \ldots, v_n).$$

Let $\mathcal{C}$ denote the binary code of blocklength $2n$ obrained from $\mathcal{C}_1$ and $\mathcal{C}_2$ as follows:

$$\mathcal{C} = \{\langle \mathbf{u}|\mathbf{u} \oplus \mathbf{v} \rangle \colon \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}.$$

(a) (5 pts) Is $\mathcal{C}$ a linear code?

(b) (5 pts) How many codewords does $\mathcal{C}$ have? Carefully justify your answer. What is the rate R of $\mathcal{C}$ in terms of the rates R_1 and R_2 of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$?

(c) (5 pts) Show that the Hamming weight of $\langle \mathbf{u}|\mathbf{u} \oplus \mathbf{v} \rangle$ satisfies

$$w_H(\langle \mathbf{u}|\mathbf{u} \oplus \mathbf{v} \rangle) \geq w_H(\mathbf{v}).$$

(d) (5 pts) Show that the Hamming weight of $\langle \mathbf{u}|\mathbf{u} \oplus \mathbf{v} \rangle$ satisfies

$$w_H(\langle \mathbf{u}|\mathbf{u} \oplus \mathbf{v} \rangle) \geq \begin{cases} w_H(\mathbf{v}) & \text{if } \mathbf{v} \neq \mathbf{0} \\ 2w_H(\mathbf{u}) & \text{else.} \end{cases}$$

(e) (5 pts) Show that the minimum distance d of $\mathcal{C}$ satisfies

$$d \geq \min\{2d_1, d_2\}.$$

(f) (5 pts) Show that $d = \min\{2d_1, d_2\}$.