Handout 34 | Information Theory and Coding
Final exam | Jan. 23, 2018

4 problems, 72 points (every sub-part 4 pts)
180 minutes
2 sheet (4 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. Suppose $U_1, U_2, \dots$ is an i.i.d. sequence of random variables, each taking value in an alphabet $\mathcal{U}$. Let N be a positive integer valued random variable determined by $U_1, U_2, \dots$. E.g., "the smallest n for which $U_{n-2} = U_{n-1} = U_n$", "the smallest n for which $U_n = a$", "smallest n such that $\sum_{i=1}^n U_i > 10$", etc.

Assume that for each $n \geq 1$, upon observing $U_1, \dots, U_n$ we can determine if $N \leq n$. (This is the case in the examples above, but will not be the case for "the largest n such that $U_1 = U_2 = \dots = U_n$.") Assume further that $N < \infty$ with probability 1.

Let $Z_n = \mathbb{1}\{N \geq n\}$, and $V = U^N$ (the word formed by the first N letters of $U_1, U_2, \dots$ — we are assured that V is a word of finite length because $N < \infty$ with probability 1).

(a) Find $H(Z_n | U^{n-1})$.

(b) Show that Z_n and U_n are independent.

(c) Let $\mathcal{V} \subset \mathcal{U}^*$ denote the set of possible values of V. Show that $\mathcal{V}$ is a prefix-free collection.

(d) Given a function $f : \mathcal{U} \to \mathbb{R}$, let $g(U_1, U_2, \dots) = \sum_{n=1}^N f(U_n)$. Show that

$$E[g(U_1, U_2, \dots)] = E[N]E[f(U_1)],$$

by first showing $\sum_{n=1}^N f(U_n) = \sum_{n=1}^\infty Z_n f(U_n)$. Hint: $Y = \sum_{n=1}^\infty \mathbb{1}\{Y \geq n\}$ for any Y which is non-negative integer valued.

(e) For $v = u_1 \dots u_n$ in $\mathcal{V}$ we have $\Pr(V = v) = \prod_{i=1}^n P_U(u_i)$. Show that

$$H(V) = E[N]H(U_1).$$

[Hint: use (d) to compute the expectation of $\log p_V(V)$.]

PROBLEM 2. A "K-ary erasure channel with erasure probability p" is described as follows: the input U belongs to the alphabet $\{1, \ldots, K\}$, the output V belongs to the alphabet $\{1, \ldots, K\} \cup \{?\}$, and if u is the input, the output V equals u with probability $1-p$, and equals ? with probability p. Note that $\Pr(V = ?) = p$ regardless of the input distribution.

(a) Show that $\Pr(U = u | V = ?) = p_U(u)$.

(b) Show that $I(U; V) = (1-p)H(U)$.

(c) Find the capacity of this channel and the input distribution that maximizes the mutual information.

Suppose we have a channel from X to Y with capacity C and we process the output Y by a $|\mathcal{Y}|$-ary erasure channel with erasure probability p to obtain Z.

(d) Show that $I(X; Z) = (1-p)I(X; Y)$.

(e) Find the capacity of the channel from X to Z in terms of p and C.

PROBLEM 3. Suppose $(X_1, \dots, X_n, Y_1, \dots, Y_m)$ is an $n+m$ dimensional Gaussian random vector with covariance matrix K. Partition the $(n+m) \times (n+m)$ matrix K as

$$K = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}$$

where K_{11} is $n \times n$ and K_{22} is $m \times m$.

(a) Express $h(X_1, \dots, X_n)$, $h(Y_1, \dots, Y_n)$ and $h(X_1, \dots, X_n, Y_1, \dots, Y_m)$ in terms of the matrices above.

(b) Show if the matrix $A = \left[\begin{smallmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{smallmatrix}\right]$ is positive definite, then $\det(A) \le \det(A_{11}) \det(A_{22})$. [Hint: for any positive definite matrix A, $f(x) = \det(2\pi A)^{-1/2} \exp(-\frac{1}{2} x^T A^{-1} x)$ is a probability density.]

Problem 4. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be binary two linear codes. Let n_i, 2^{k_i}, and d_i denote the blocklength, number of codewords, and the minimum distance of $\mathcal{C}_i$. Assume that the generator matrices of the codes are of the form

$$G_i = \begin{bmatrix} I_{k_i} \\ A_i \end{bmatrix}$$

Consider the code $\mathcal{C}$ of blocklength $n = n_1 n_2$ whose codewords X we will think of as binary matrices of size $n_1 \times n_2$ and is described as follows: a binary matrix X with n_1 rows and n_2 columns is a codeword in $\mathcal{C}$ if and only if each of its rows belongs to $\mathcal{C}_2$ and each of its columns belongs to $\mathcal{C}_1$.

(a) Show that $\mathcal{C}$ is a linear code.

(b) Suppose we are given $k_1 k_2$ data bits in the form of a binary matrix U of size $k_1 \times k_2$. We place U in the $k_1 \times k_2$ upper left corner of a matrix X

$$X = \begin{bmatrix} X_{11} = U & X_{12} \\ X_{21} & X_{22} \end{bmatrix}.$$

Explain how to determine the remaining submatrices X_{12}, X_{21}, X_{22} so that X belongs to $\mathcal{C}$. How many codewords does $\mathcal{C}$ have?

For the remainder of the problem X is related to U as above.

(c) Suppose $U_{rs} = 1$. What can you say about the weight w_1 of the s'th column of X?

(d) Again supposing $U_{rs} = 1$, consider a row t with $X_{ts} = 1$. What can you say about the weight of the t'th row of X?

(e) Suppose $c^{(i)} = (c_1^{(i)}, \dots, c_{n_i}^{(i)}) \in \mathcal{C}_i$ is a codeword with weight d_i, $i = 1, 2$. Show that X with $X_{rs} = c_r^{(1)} c_s^{(2)}$ is a codeword of $\mathcal{C}$.

(f) Show that the minimum distance d of $\mathcal{C}$ equals $d_1 d_2$. [Hint: use (b) and (c) to lower bound d.]