ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 15 | Information Theory and Coding
Midterm exam | Oct. 29, 2019

4 problems, 60 points
180 minutes
1 sheet (2 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. (20 points)

In a cryptosystem, a secret key K known to both Alice and Bob allows for secure communication. Using the key K, Alice converts her plain text U to a ciphertext V. Using the same key K, Bob converts the ciphertext V back into U. We model U, V and K as random variables. Secure communication requires U and V to be independent.

(a) (2 pts) What are the values of $H(U|VK)$ and $I(U;V)$?

(b) (4 pts) Determine the relation,(i.e., $<, \leq, =, >$, or $\geq$), between $H(U)$ and $I(U;K|V)$. Provide a proof for this relation.

(c) (4 pts) Determine the relation,(i.e., $<, \leq, =, >$, or $\geq$), between $H(K)$ and $I(U;K|V)$. Provide a proof for this relation.

(d) (4 pts) Show that $H(K) \geq H(U)$. Furthermore, show that if the equality holds, then (i) K and V are independent and (ii) $H(K|UV) = 0$.

Suppose further that (i) K is independent of U, (ii) the cryptosystem is implemented as $V = f(U,K)$ and $U = g(V,K)$, and (iii) the system is supposed to be secure regardless of the distribution of U on a given alphabet $\mathcal{U}$.

(e) (2 pts) Show that $H(K) \geq \log |\mathcal{U}|$.

(f) (4 pts) With $\mathcal{U} = \{0, 1, \ldots, |\mathcal{U}| - 1\}$, show that if we take K to be uniform on $\mathcal{U}$, the secrecy requirement is satisfied by $f(u,k) = u + k \mod |\mathcal{U}|$.

PROBLEM 2. (18 points)

Suppose $U_1, U_2, \ldots$ are i.i.d. random variables with finite alphabet and let p denote the distribution of each U_i. Suppose we do not know p, but we know that it is included in the set of K possible distributions, i.e., $p \in \mathcal{P} = \{p_k : k = 1, ..., K\}$.

For any distribution q on $\mathcal{U}$, define $r(q) = \max_k D(p_k \| q)$.

(a) (4 pts) Show that for any q there exists a prefix-free code $C : \mathcal{U} \to \{0,1\}^*$ such that

$$E\left[\text{length}\big(C(U)\big)\right] - H(U) \leq r(q) + 1$$

whenever the distribution of random variable U is in $\mathcal{P}$.

(b) (4 pts) Show that $\min_q r(q) \leq \log K$. [Hint: try $q(u) = \frac{1}{K}\sum_k p_k(u)$.]

(c) (4 pts) Show that for fixed K there exists a sequence of prefix-free codes $C_n : \mathcal{U}^n \to \{0,1\}^*$ such that

$$\lim_{n\to\infty} \frac{1}{n} E\left[\text{length}\big(C_n(U^n)\big)\right] = H(U)$$

whenever $U_1, U_2, \ldots$ are i.i.d. and have a distribution in $\mathcal{P}$. [Hint: use (b).]

(d) (2 pts) Let $Z = \sum_u \max_k p_k(u)$. Show that $\min_q r(q) \leq \log Z$. [Hint: try choosing $q(u)$ proportional to $\max_k p_k(u)$.]

(e) (4 pts) Show that $Z \leq \min\{K, |\mathcal{U}|\}$.

Problem 3. (12 points)

Suppose $p_1, p_2, \ldots, p_K$ are probability distributions on the finite alphabet $\mathcal{U}$. Let $H_1, \ldots, H_K$ be the entropies of these distributions, and let $H = \max_k H_k$. Fix $\epsilon > 0$ and for each $n \geq 1$ consider the set

$$T(n, \epsilon) = \bigcup_k T(n, p_k, \epsilon)$$

where $T(n, p_k, \epsilon)$ is the set of ϵ-typical sequences of length n with respect to the distribution p_k, i.e., $T(n, p_k, \epsilon) = \big\{u^n \in \mathcal{U}^n : \forall_{u' \in \mathcal{U}} \left|\frac{1}{n} N_{u'}(u^n) - p_k(u')\right| < \epsilon p_k(u')\big\}$ where $N_{u'}(u^n)$ is the number of occurrences of u' in sequence u^n.

Suppose that $U_1, U_2, \ldots$ are i.i.d. with distribution p where p is one of $p_1, \ldots, p_K$, i.e., $p \in \mathcal{P} = \{p_k : k = 1, ..., K\}$.

(a) (4 pts) Show that $\lim_{n\to\infty} \Pr\big((U_1, \ldots, U_n) \in T(n, \epsilon)\big) = 1$. (In particular for any $\delta > 0$, for n large enough $\Pr\big(U^n \in T(n, \epsilon)\big) > 1 - \delta$.)

(b) (4 pts) Show that for large enough n, $\frac{1}{n} \log |T(n, \epsilon)| < (1 + \epsilon)H + \epsilon$.

(c) (4 pts) Fix $R > H$ and $\delta > 0$. Show that for n large enough there is a prefix-free code $c : \mathcal{U}^n \to \{0, 1\}^*$ such that

$$\Pr\Big(\text{length}\big(c(U^n)\big) < nR\Big) > 1 - \delta$$

Problem 4. (10 points)

Suppose C_p is a prefix-free binary code for non-negative integers $\{0, 1, 2, \ldots\}$. Suppose C_i is an injective code for an alphabet $\mathcal{U}$.

(a) (4 pts) Show that C defined by $C(u) = C_p\big(l(u)\big)C_i(u)$, with $l(u) = \text{length}\big(C_i(u)\big)$ is a prefix-free code for $\mathcal{U}$.

Observe that (i) the code C_a with $C_a(j) = 0^j 1$, (i.e., $C_a(0) = 1$, $C_a(1) = 01$, $C_a(2) = 001, \ldots$) is prefix-free with $\text{length}\big(C_a(j)\big) = j + 1$, and (ii) the code C_b for non-negative integers with

$$C_b(0) = \lambda,\ C_b(j) = \text{bin}(j-1), \quad j > 0$$

where $\text{bin}(j)$ denotes the binary expansion of the integer j, (i.e., $\text{bin}(0) = 0$, $\text{bin}(1) = 1$, $\text{bin}(2) = 10$, $\text{bin}(3) = 11$, ...) is injective with $\text{length}\big(C_b(j)\big) = \lfloor \log_2(j+1) \rfloor$.

(b) (2 pts) Show that there exists a prefix-free code C' for non-negative integers with

$$\text{length}(C'(j)) = 2\lfloor \log_2(j+1) \rfloor + 1, \quad j \geq 0.$$

(c) (4 pts) Consider a sequence of functions

$$\begin{aligned} l_1(j) &= 2\lfloor \log_2(j+1) \rfloor + 1 \\ l_n(j) &= \lfloor \log_2(j+1) \rfloor + l_{n-1}\big(\lfloor \log_2(j+1) \rfloor\big), \quad n > 1. \end{aligned}$$

Show that for each $n > 0$ there exists a prefix-free code for non-negative integers C_n such that

$$\text{length}\big(C_n(j)\big) = l_n(j).$$

[Hint: use induction.]