ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Handout 24 Information Theory and Coding

Homework 10 (Graded - Due on Dec.8, 2014) Nov. 25, 2014

PROBLEM 1. (35 pts) Suppose we have a source that produces an independent and identically distributed sequence $U_1 U_2 \dots$ according to p_U. We design a source coder in the following fashion:

- generate $M = 2^{nR}$ sequences
  $U(1) = U(1)_1 \ \dots \ U(1)_n$
  $\vdots$
  $U(M) = U(M)_1 \ \dots \ U(M)_n$
  by drawing $\{U(m)_i : 1 \le i \le n, 1 \le m \le M\}$ independently according to p_U.
- encode $U_1 \dots U_n$ as follows:
  if there exists m such that $U_1 \dots U_n = U(m)$ send the $\log_2 M = nR$ bit representation of m else declare encoding failure.

(a) (10 pts) Conditioned on $U^n = u^n$, what is the probability that $U(1) \neq U^n$?

(b) (10 pts) Conditioned on $U^n = u^n$, what is the probability of encoding failure?

(c) (10 pts) Show that $\mathbb{P}(\text{"failure"} | u^n \in \mathcal{T}_\epsilon^n(p_U)) \le \exp\left(-2^{nR + nH(U)(1+\epsilon)}\right)$.
Hint: $(1-x)^M \le \exp(-Mx)$

(d) (5 pts) Show that if $R > H(U)$ then $\mathbb{P}(\text{error}) \to 0$ as n gets large.

PROBLEM 2. (30 pts) Let $h_2(p) = -p \log p - (1-p)\log(1-p)$ denote the binary entropy function defined on the interval $[0, \frac{1}{2}]$. Note that on this interval h_2 is a bijection, so its inverse $h_2^{-1} : [0,1] \longrightarrow [0, \frac{1}{2}]$ is well defined. Define $p * q = p(1-q) + q(1-p)$ and let $\oplus$ be the XOR operation.

Suppose X_1 and X_2 are two binary independent random variables with $H(X_1) = h_2(p_1)$, $H(X_2) = h_2(p_2)$, where $0 \le p_1, p_2 \le \frac{1}{2}$.

(a) (5 pts) Show that $H(X_1 \oplus X_2) = h_2(p_1 * p_2)$.

(b) (5 pts) Suppose that (X_1, Y) is independent of X_2, where Y is a random variable in $\mathcal{Y}$. For every $y \in \mathcal{Y}$, let $0 \le p_1(y) \le \frac{1}{2}$ be such that $H(X_1|Y=y) = h_2(p_1(y))$. We again assume that $H(X_2) = h_2(p_2)$ and $0 \le p_2 \le \frac{1}{2}$.
Show that $H(X_1|Y) = \sum_y h_2(p_1(y))q(y)$, $H(X_1 \oplus X_2|Y) = \sum_y h_2(p_2 * p_1(y))q(y)$, where $q(y) = \mathbb{P}_Y(y)$ for every $y \in \mathcal{Y}$.

(c) (10 pts) Show that for every $0 \le p_2 \le \frac{1}{2}$, the mapping $f : [0,1] \longrightarrow \mathbb{R}$ defined as $f(h) = h_2(p_2 * h_2^{-1}(h))$ is convex.
Hint: The graph of $f(h)$ can be drawn by the parametric curve $p \to (h_2(p), h_2(p_2 * p))$ so it is enough to show that $p \to \frac{\frac{\partial}{\partial p} h_2(p_2 * p)}{\frac{\partial}{\partial p} h_2(p)}$ is increasing in $0 \le p \le 1/2$.

(d) (5 pts) Suppose $H(X_1|Y) = h_2(p_1)$, $H(X_2) = h_2(p_2)$. Show that $H(X_1 \oplus X_2|Y) \ge h(p_1 * p_2)$.

(e) (5 pts) Suppose (X_1, Y_1) is independent of (X_2, Y_2) and $H(X_1|Y_1) = h_2(p_1)$, $H(X_2|Y_2) = h_2(p_2)$. Show that $H(X_1 \oplus X_2|Y_1, Y_2) \geq h(p_1 * p_2)$.

Problem 3. (35 pts) Fix $0 < \delta < 1$ and let (U, V) be a random pair in $\mathcal{U} \times \mathcal{V}$. For each $u^n \in \mathcal{U}^n$ and each $a \in \mathcal{U}$, let $n_a(u^n)$ be the number of appearances of a in the sequence u^n. Similarly, for each $u^n \in \mathcal{U}^n$,$v^n \in \mathcal{V}^n$, $a \in \mathcal{U}$ and $b \in \mathcal{V}$ let $n_{a,b}(u^n, v^n)$ be the number of appearances of (a, b) in (u^n, v^n). Recall that for every $\delta > 0$, $u^n \in \mathcal{T}_\delta^n(p_U)$ if and only if $\mathbb{P}_U(a)(1-\delta) \leq \dfrac{n_a(u^n)}{n} \leq \mathbb{P}_U(a)(1+\delta)$ for every $a \in \mathcal{U}$. Similarly, $(u^n, v^n) \in \mathcal{T}_\delta^n(p_{U,V})$ if and only if $\mathbb{P}_{U,V}(a, b)(1-\delta) \leq \dfrac{n_{a,b}(u^n, v^n)}{n} \leq \mathbb{P}_{U,V}(a, b)(1+\delta)$ for every $a \in \mathcal{U}$ and $b \in \mathcal{V}$. Throughout this problem we fix $u^n \in \mathcal{T}_\delta^n(p_U)$.

(a) (10 pts) Show that if

$$n_a(u^n)\mathbb{P}_{V|U}(b|a)(1-\delta) \leq n_{a,b}(u^n, v^n) \leq n_a(u^n)\mathbb{P}_{V|U}(b|a)(1+\delta) \qquad (1)$$

for every $a \in \mathcal{U}$ and $b \in \mathcal{V}$, then $(u^n, v^n) \in \mathcal{T}_{3\delta}^n(p_{U,V})$.

(b) (10 pts) Show that for n large enough, there are at least $\prod_{a \in \mathcal{U}} \left[(1-\delta)2^{n_a(u^n)(H(V|U=a)-\delta)}\right]$ sequences v^n which satisfy (1) for every $a \in \mathcal{U}$ and every $b \in \mathcal{V}$. Hint: Recall that for any random variable X, we have $|\mathcal{T}_\delta^n(p_X)| \geq (1-\delta)2^{n[H(X)-\delta]}$.

(c) (5 pts) Deduce that for n large enough, the number of sequences $v^n \in \mathcal{V}^n$ satisfying $(u^n, v^n) \in \mathcal{T}_{3\delta}^n(p_{U,V})$ is at least $(1-\delta)^{|\mathcal{U}|}2^{n[H(V|U)-(\log|\mathcal{U}|+1)\delta]}$.

Now let $V_1, \ldots, V_n$ be n independent random variables in $\mathcal{V}$ which have the same distribution as V.

(d) (5 pts) Show that if $(u^n, v^n) \in \mathcal{T}_{3\delta}^n(p_{U,V})$, then $\mathbb{P}_{V^n}(v^n) \geq 2^{-n[H(V)+3\delta]}$.

(e) (5 pts) Deduce that $\mathbb{P}[(u^n, V^n) \in \mathcal{T}_{3\delta}^n(p_{U,V})] \geq (1-\delta)^{|\mathcal{U}|}2^{-n[I(U;V)+(\log|\mathcal{U}|+4)\delta]}$.