ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 29 Information Theory and Coding
Homework 12 Dec. 10, 2019

Problem 1. Suppose $\mathcal{U} = \mathcal{V}$ are additive groups with group operation $\oplus$. (E.g., $\mathcal{U} = \mathcal{V} = \{0, \dots, K-1\}$, with modulo K addition.) Suppose the distortion measure $d(u, v)$ depends only on the difference between u and v and is given by $g(u \ominus v)$. Let $\phi(D)$ denote $\max H(Z) : E[g(Z)] \leq D$.

a) Show that $\phi(D)$ is concave.

b) Let (U, V) be such that $E[d(U, V)] \leq D$. Show that $I(U; V) \geq H(U) - \phi(D)$ by justifying

$$I(U;V) = H(U) - H(U|V) = H(U) - H(U \ominus V|V) \geq H(U) - H(U \ominus V) \geq H(U) - \phi(D).$$

c) Show that $R(D) \geq H(U) - \phi(D)$.

d) Assume now that U is uniform on $\mathcal{U}$. Show that $R(D) = H(U) - \phi(D)$.

Problem 2. Suppose $\mathcal{U} = \mathcal{V} = \mathbb{R}$, the set of real numbers, and $d(u, v) = (u - v)^2$. Show that for any U with variance σ^2, $R(D)$ satisfies

$$h(U) - \tfrac{1}{2}\log(2\pi e D) \leq R(D) \leq \left[\tfrac{1}{2}\log(\sigma^2/D)\right]^+.$$

Problem 3. Consider a two-way communication system where two parties communicate via a *common* output they both can observe and influence. Denote the common output by Y, and the signals emitted by the two parties by x_1 and x_2 respectively. Let $p(y|x_1, x_2)$ model the memoryless channel through which the two parties influence the output.

We will consider feedback-free block codes, i.e., we will use encoding and decoding functions of the form

$$\begin{aligned} &\mathrm{enc}_1\colon \{1, \dots, 2^{nR_1}\} \to \mathcal{X}_1^n \qquad &&\mathrm{dec}_1\colon \mathcal{Y}^n \times \{1, \dots, 2^{nR_1}\} \to \{1, \dots, 2^{nR_2}\} \\ &\mathrm{enc}_2\colon \{1, \dots, 2^{nR_2}\} \to \mathcal{X}_2^n \qquad &&\mathrm{dec}_2\colon \mathcal{Y}^n \times \{1, \dots, 2^{nR_2}\} \to \{1, \dots, 2^{nR_1}\} \end{aligned}$$

with which the parties encode their own message and decode the other party's messages. (Note that when a party is decoding the other party's message, it can make use of the knowledge of its own message).

We will say that the rate pair (R_1, R_2) is achievable, if for any $\epsilon > 0$, there exist encoders and decoders with the above form for which the average error probability is less than ϵ.

Consider the following 'random coding' method to construct the encoders:

(i) Choose probability distributions p_j on $\mathcal{X}_j$, $j = 1, 2$.

(ii) Choose $\{\mathrm{enc}_1(m_1)_i : m_1 = 1, \dots, 2^{nR_1},\ i = 1, \dots, n\}$ i.i.d., each having distribution as p_1. Similarly, choose $\{\mathrm{enc}_2(m_2)_i : m_2 = 1, \dots, 2^{nR_2},\ i = 1, \dots, n\}$ i.i.d., each having distribution as p_2, independently of the choices for enc_1.

For the decoders we will use typicality decoders:

(i) Set $p(x_1, x_2, y) = p_1(x_1)p_2(x_2)p(y|x_1, x_2)$. Choose a small $\epsilon > 0$ and consider the set T of ϵ-typical (x_1^n, x_2^n, y^n)'s with respect to p.

(ii) For decoder 1: given y^n and the correct m_1, dec_1 will declare $\hat{m}_2$ if it is the unique m_2 for which $(\mathrm{enc}_1(m_1), \mathrm{enc}_2(m_2), y^n) \in T$. If there is no such m_2, dec_1 outputs 0. (Similar description applies to Decoder 2.)

(a) Given that m_1 and m_2 are the transmitted messages, show that $(\mathrm{enc}_1(m_1), \mathrm{enc}_2(m_2), Y^n) \in T$ with high probability.

(b) Given that m_1 and m_2 are the transmitted messages, and $\tilde{m}_1 \neq m_1$ what is the probability distribution of $(\mathrm{enc}_1(\tilde{m}_1), \mathrm{enc}(m_2), Y^n)$?

(c) Under the assumptions in (b) show that the

$$\Pr\{(\mathrm{enc}_1(\tilde{m}_1), \mathrm{enc}_2(m_2), Y^n) \in T\} \doteq 2^{-nI(X_1;X_2Y)}.$$

(d) Show that all rate pairs satisfying

$$R_1 \leq I(X_1; YX_2), \quad R_2 \leq I(X_2; YX_1)$$

for some $p(x_1, x_2) = p(x_1)p(x_2)$ are achievable.

(e) For the case when X_1, X_2, Y are all binary and Y is the product of X_1 and X_2, show that the achievable region is strictly larger than what we can obtain by 'half duplex communication' (i.e., the set of rates that satisfy $R_1 + R_2 \leq 1$.)

Problem 4. Let

$$Z_1 = \begin{cases} 1, & p \\ 0, & q \end{cases}, \qquad Z_2 = \begin{cases} 1, & p \\ 0, & q \end{cases}$$

and let $U = Z_1 Z_2$, $V = Z_1 + Z_2$. Assume Z_1 and Z_2 are independent. Note that we have a joint distribution induced on $\mathcal{U} \times \mathcal{V}$. Suppose that (U_i, V_i) are i.i.d according to the distribution induced as above. Sender 1 compresses U^n at rate R_1 and sender 2 compresses V^n at rate R_2.

(a) Find the Slepian-Wolf rate region for recovering (U^n, V^n) at receiver.

(b) What is the residual uncertainty that receiver has about (Z_1^n, Z_2^n)? i.e. $H(Z_1^n Z_2^n | U^n V^n)$.

Problem 5. Suppose we are told that for any n and M, for any binary code with block-length n, with M codewords, the minimum distance d_{min} satisfies $d_{min} \leq d_0(M, n)$ where d_0 is a specified upper bound on minimum distance.

(a) Show that any upper bound d_0 can be improved to he following upper bound: for any n, M, for any binary code with blocklength n with M codewords

$$d_{min} \leq d_1(M, n)$$

where $d_1(M, n) = \min_{k:\ 0 \leq k \leq n} d_0(\lceil M/2^k \rceil, n - k)$.

(b) Consider the trivial bound

$$d_0(M, n) = \begin{cases} n, & M \geq 2 \\ \infty, & M \leq 1 \end{cases}$$

What is the bound d_1 constructed via (a) for this d_0?

(c) Suppose we are given a binary code with M words of blocklength n. Fix $1 \leq i \leq n$ and let $a_1, \ldots, a_M$ be the ith bits if the M codewords. Suppose M_1 of the a_m's are '1' and M_0 of them are '0'. Show that

$$\sum_{m=1}^{M} \sum_{\substack{m'=1 \\ m' \neq m}}^{M} d_H(a_m, a'_m) = 2M_0 M_1 \leq M^2/2.$$

(d) Show that for any binary code with $M \geq 2$ codewords $x_1, \ldots, x_M$ of blocklength n

$$M(M-1)d_{min} \leq \sum_{m=1}^{M} \sum_{\substack{m'=1 \\ m' \neq m}}^{M} d_H(x_m, x_{m'}) \leq nM^2/2;$$

consequently, $d_{min} \leq \lfloor \frac{1}{2} n \frac{M}{M-1} \rfloor$.