ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 28 Information Theory and Coding
Homework 12 December 09, 2014

PROBLEM 1. Let $W : \{0,1\} \longrightarrow \mathcal{Y}$ be a channel where the input is binary and where the output alphabet is $\mathcal{Y}$. The Bhattacharyya parameter of the channel W is defined as

$$Z(W) = \sum_{y\in\mathcal{Y}} \sqrt{W(y|0)W(y|1)}.$$

Let X_1, X_2 be two independent random variables uniformly distributed in $\{0,1\}$ and let Y_1 and Y_2 be the output of the channel W when the input is X_1 and X_2 respectively, i.e., $\mathbb{P}_{Y_1,Y_2|X_1,X_2}(y_1,y_2|x_1,x_2) = W(y_1|x_1)W(y_2|x_2)$. Define the channels $W^- : \{0,1\} \longrightarrow \mathcal{Y}^2$ and $W^+ : \{0,1\} \longrightarrow \mathcal{Y}^2 \times \{0,1\}$ as follows:

- $W^-(y_1,y_2|u_1) = \mathbb{P}[Y_1 = y_1, Y_2 = y_2 | X_1 \oplus X_2 = u_1]$ for every $u_1 \in \{0,1\}$ and every $y_1, y_2 \in \mathcal{Y}$, where $\oplus$ is the XOR operation.
- $W^+(y_1,y_2,u_1|u_2) = \mathbb{P}[Y_1 = y_1, Y_2 = y_2, X_1 \oplus X_2 = u_1 | X_2 = u_2]$ for every $u_1, u_2 \in \{0,1\}$ and every $y_1, y_2 \in \mathcal{Y}$.

(a) Show that $W^-(y_1,y_2|u_1) = \frac{1}{2}\sum_{u_2\in\{0,1\}} W(y_1|u_1\oplus u_2)W(y_2|u_2)$.

(b) Show that $W^+(y_1,y_2,u_1|u_2) = \frac{1}{2}W(y_1|u_1\oplus u_2)W(y_2|u_2)$.

(c) Show that $Z(W^+) = Z(W)^2$.

For every $y \in \mathcal{Y}$ define $\alpha(y) = W(y|0)$, $\beta(y) = W(y|1)$ and $\gamma(y) = \sqrt{\alpha(y)\beta(y)}$.

(d) Show that

$$Z(W^-) = \sum_{y_1,y_2\in\mathcal{Y}} \frac{1}{2}\sqrt{\Big(\alpha(y_1)\alpha(y_2) + \beta(y_1)\beta(y_2)\Big)\Big(\alpha(y_1)\beta(y_2) + \beta(y_1)\alpha(y_2)\Big)}.$$

(e) Show that for every $x, y, z, t \geq 0$ we have $\sqrt{x+y+z+t} \leq \sqrt{x} + \sqrt{y} + \sqrt{z} + \sqrt{t}$. Deduce that

$$\begin{aligned} Z(W^-) \leq & \frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}} \alpha(y_1)\gamma(y_2)\right) + \frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}} \alpha(y_2)\gamma(y_1)\right) \\ & + \frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}} \beta(y_2)\gamma(y_1)\right) + \frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}} \beta(y_1)\gamma(y_2)\right). \end{aligned} \tag{1}$$

(f) Show that every sum in (1) is equal to $Z(W)$. Deduce that $Z(W^-) \leq 2Z(W)$.

PROBLEM 2. For a given value $0 \leq z_0 \leq 1$, define the following random process:

$$Z_0 = z_0, \quad Z_{i+1} = \begin{cases} Z_i^2 & \text{with probability } 1/2 \\ 2Z_i - Z_i^2 & \text{with probability } 1/2 \end{cases} \qquad i \geq 0,$$

with the sequence of random choices made independently. Observe that the Z process keeps track of the polarization of a Binary Erasure Channel with erasure probability z_0 as it is tranformed by the polar transform: $\mathbb{P}(Z_i = z)$ is exactly the fraction of Binary Erasure Channels having an erasure probability z among the 2^i BEC channels which are synthesized by the polar transform at the ith level. The aim of this problem is to prove that for any $\delta > 0$, $\mathbb{P}\big[Z_i \in (\delta, 1-\delta)\big] \to 0$ as i gets large.

(a) Define $Q_i = \sqrt{Z_i(1-Z_i)}$. Find $f_1(z)$ and $f_2(z)$ so that

$$Q_{i+1} = Q_i \times \begin{cases} f_1(Z_i) & \text{with probability } 1/2, \\ f_2(Z_i) & \text{with probability } 1/2. \end{cases}$$

(b) Show that $f_1(z) + f_2(z) \leq \sqrt{3}$. Based on this, find a $\rho < 1$ so that

$$\mathbb{E}\big[Q_{i+1} \bigm| Z_0, \ldots, Z_i\big] \leq \rho Q_i.$$

(c) Show that, for the ρ you found in (b), $\mathbb{E}[Q_i] \leq \frac{1}{2}\rho^i$.

(d) Show that

$$\mathbb{P}\big[Z_i \in (\delta, 1-\delta)\big] = \mathbb{P}\big[Q_i > \sqrt{\delta(1-\delta)}\big] \leq \frac{\rho^i}{2\sqrt{\delta(1-\delta)}}.$$

Deduce that $\mathbb{P}\big[Z_i \in (\delta, 1-\delta)\big] \to 0$ as i gets large.

PROBLEM 3. Let P_1 and P_2 be two channels of input alphabet $\mathcal{X}_1$ and $\mathcal{X}_2$ and of output alphabet $\mathcal{Y}_1$ and $\mathcal{Y}_2$ respectively. Consider a communication scheme where the transmitter chooses the channel (P_1 or P_2) to be used and where the receiver knows which channel were used. This scheme can be formalized by the channel P of input alphabet $\mathcal{X} = (\mathcal{X}_1 \times \{1\}) \cup (\mathcal{X}_2 \times \{2\})$ and of output alphabet $\mathcal{Y} = (\mathcal{Y}_1 \times \{1\}) \cup (\mathcal{Y}_2 \times \{2\})$, which is defined as follows:

$$P(y, k'|x, k) = \begin{cases} P_k(y|x) & \text{if } k' = k, \\ 0 & \text{otherwise.} \end{cases}$$

Let $X = (X_k, K)$ be a random variable in $\mathcal{X}$ which will be the input distribution to the channel P, and let $Y = (Y_k, K) \in \mathcal{Y}$ be the output distribution. Define X_1 as being the random variable in $\mathcal{X}_1$ obtained by conditioning X_k on $K = 1$. Similarly define X_2, Y_1 and Y_2. Let α be the probability that $K = 1$.

(a) Show that $I(X;Y) = h_2(\alpha) + \alpha I(X_1;Y_1) + (1-\alpha) I(X_2;Y_2)$.

(b) What is the input distribution X that achieves the capacity of P?

(c) Show that the capacity C of P satisfies $2^C = 2^{C_1} + 2^{C_2}$, where C_1 and C_2 are the capacities of P_1 and P_2 respectively.