

# ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

**Handout 32**  
Homework 13

Information Theory and Coding  
Dec. 15, 2025

PROBLEM 1. Suppose we are told that for any  $n$  and  $M$ , for any binary code with blocklength  $n$ , 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 the 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  $a_1, \dots, a_M$  be the  $i$ th bits of the  $M$  codewords. Suppose  $M_1$  of the  $a_m$ 's are '1' and  $M_0$  of them are '0'. Show that

$$\sum_{m=1}^M \sum_{\substack{m'=1 \\ m' \neq m}}^M d_H(a_m, a_{m'}) = 2M_0M_1 \leq M^2/2.$$

- (d) Show that for any binary code with  $M \geq 2$  codewords  $x_1, \dots, x_M$  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,  $d_{min} \leq \lfloor \frac{1}{2}n \frac{M}{M-1} \rfloor$ .

PROBLEM 2. Let  $W : \{0, 1\} \rightarrow \mathcal{Y}$  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  $W^- : \{0, 1\} \rightarrow \mathcal{Y}^2$  and  $W^+ : \{0, 1\} \rightarrow \mathcal{Y}^2 \times \{0, 1\}$  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

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

(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

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

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

**PROBLEM 3.** For a given value  $0 \leq z_0 \leq 1$ , define the following random process:

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

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 transformed 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  $i$ th level. The aim of this problem is to prove that for any  $\delta > 0$ ,  $\mathbb{P}[Z_i \in (\delta, 1 - \delta)] \rightarrow 0$  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

$$\mathbb{E}[Q_{i+1} \mid Z_0, \dots, Z_i] \leq \rho Q_i.$$

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

(d) Show that

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

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