ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 25 Information Theory and Coding
Homework 10 Nov 26, 2019

PROBLEM 1. Show that, if H is the parity-check matrix of a code of length n, then the code has minimum distance d iff every $d-1$ rows of H are linearly independent and some d rows are linearly dependent.

PROBLEM 2. In this problem we will show that there exists a binary linear code which satisfies the Gilbert–Varshamov bound. In order to do so, we will construct a $n \times r$ parity-check matrix H and we will use Problem 1.

(a) We will choose rows of H one-by-one. Suppose i rows are already chosen. Give a combinatorial upper-bound on the number of distinct linear combinations of these i rows taken $d-2$ or fewer at a time.

(b) Provided this number is strictly less than $2^r - 1$, can we choose another row different from these linear combinations, and keep the property that any $d-1$ rows of the new $(i+1) \times r$ matrix are linearly independent?

(c) Conclude that there exists a binary linear code of length n, with at most r parity-check equations and minimum distance at least d, provided

$$1 + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2} < 2^r. \tag{1}$$

(d) Show that there exists a binary linear code with $M = 2^k$ distinct codewords of length n provided $M \sum_{i=0}^{d-2} \binom{n-1}{i} < 2^n$.

PROBLEM 3. The weight of a binary sequence of length N is the number of 1's in the sequence. The Hamming distance between two binary sequences of length N is the weight of their modulo 2 sum. Let $\mathbf{x}_1$ be an arbitrary codeword in a linear binary code of block length N and let $\mathbf{x}_0$ be the all-zero codeword. Show that for each $n \le N$, the number of codewords at distance n from $\mathbf{x}_1$ is the same as the number of codewords at distance n from $\mathbf{x}_0$.

PROBLEM 4. 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

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

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