ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

**Handout 28** Information Theory and Coding
Homework 11 Dec. 7, 2021

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 $n \leq N$, 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.

(a) Show that in a binary linear code, either all codewords contain an even number of 1's or half the codewords contain an odd number of 1's and half an even number.

(b) Let $x_{m,n}$ be the $n$th digit in the $m$th codeword of a binary linear code. Show that for any given $n$, either half or all of the $x_{m,n}$ are zero. If all of the $x_{m,n}$ are zero for a given $n$, explain how the code could be improved.

(c) Show that the average number of ones per codeword, averaged over all codewords in a linear binary code of blocklength $N$, can be at most $N/2$.

PROBLEM 5. Suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ are binary linear codes of block-length $n$. Denote the number of codewords of $\mathcal{C}_i$ by $M_i$ and the minimum distance of $\mathcal{C}_i$ by $d_i$. For $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$ let $\langle \mathbf{u} | \mathbf{v} \rangle$ denote the concatenation of the two sequences, i.e.,

$$\langle \mathbf{u} | \mathbf{v} \rangle = (u_1, \ldots, u_n, v_1, \ldots, v_n).$$

Let $\mathcal{C}$ denote the binary code of block-length $2n$ obtained from $\mathcal{C}_1$ and $\mathcal{C}_2$ as follows:

$$\mathcal{C} = \{\langle \mathbf{u} | \mathbf{u} \oplus \mathbf{v} \rangle : \mathbf{u} \in \mathcal{C}_1, \, \mathbf{v} \in \mathcal{C}_2\}.$$

(a) Is $\mathcal{C}$ a linear code?

(b) How many codewords does $\mathcal{C}$ have? Carefully justify your answer. What is the rate $R$ of $\mathcal{C}$ in terms of the rates $R_1$ and $R_2$ of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$?

(c) Show that the Hamming weight of $\langle \mathbf{u} | \mathbf{u} \oplus \mathbf{v} \rangle$ satisfies

$$w_H(\langle \mathbf{u} | \mathbf{u} \oplus \mathbf{v} \rangle) \geq w_H(\mathbf{v}).$$

(d) Show that the Hamming weight of $\langle \mathbf{u} | \mathbf{u} \oplus \mathbf{v} \rangle$ satisfies

$$w_H(\langle \mathbf{u} | \mathbf{u} \oplus \mathbf{v} \rangle) \geq \begin{cases} w_H(\mathbf{v}) & \text{if } \mathbf{v} \neq \mathbf{0} \\ 2w_H(\mathbf{u}) & \text{else.} \end{cases}$$

(e) Show that the minimum distance $d$ of $\mathcal{C}$ satisfies

$$d \geq \min\{2d_1, d_2\}.$$

(f) Show that $d = \min\{2d_1, d_2\}$.