Mid-term exam, November 26, 2025

- *You have 1h30. You can write your answers either in French or in English.*
- *Exercises are independent.*
- *Questions marked with a ($\star$) are harder than the other ones.*
- In the two exercises **any code is linear**.

Exercise 1. (1) Give the full list of minimal cyclotomic classes corresponding to cyclic codes of length 15 over $\mathbb{F}_4$.

(2) What is the number of cyclic codes of length 15 over $\mathbb{F}_4$?

(3) Prove that there exists a $[15, 7, d]$ cyclic code over $\mathbb{F}_4$ with $d \geqslant 7$.

(4) More generally, when classifying cyclic codes of length $q^2 - 1$ over $\mathbb{F}_q$,

  (a) prove that minimal cyclotomic classes have cardinality either 1 or 2;

  (b) Give the exact number of cyclotomic classes of cardinality 1.

(5) Give the total number of cyclic codes of length $q^2 - 1$ over $\mathbb{F}_q$.

(6) Prove that for any $t < \frac{q^2-1}{2}$, there always exists a $[q^2 - 1, k, d]$ cyclic code over $\mathbb{F}_q$ with $k \geqslant q^2 - 2t$ and $d \geqslant t + 1$.

Exercise 2. In this exercise, **any code is binary** *i.e.* a linear subspace of $\mathbb{F}_2^n$.

For a vector $\mathbf{x} \in \mathbb{F}_2^n$ we denote by $w_{\mathrm{H}}(\mathbf{x})$ its Hamming weight. We denote by $*$ the component wise product in $\mathbb{F}_2^n$, namely

$$(x_1, \ldots, x_n) * (y_1, \ldots, y_n) \stackrel{\text{def}}{=} (x_1 y_1, \ldots, x_n y_n).$$

(1) Prove that for any $\mathbf{c}_1 \neq \mathbf{c}_2 \in \mathbb{F}_2^n$, then

$$w_{\mathrm{H}}(\mathbf{c}_1 + \mathbf{c}_2) = w_{\mathrm{H}}(\mathbf{c}_1) + w_{\mathrm{H}}(\mathbf{c}_2) - 2 w_{\mathrm{H}}(\mathbf{c}_1 * \mathbf{c}_2) \tag{1}$$

Let $r > 0$, a code $\mathscr{C} \subset \mathbb{F}_2^n$ is said to be *r–intersecting* if $\dim \mathscr{C} \geqslant 2$ and $\forall \mathbf{c}, \mathbf{c}' \in \mathscr{C} \setminus \{0\},\ w_{\mathrm{H}}(\mathbf{c} * \mathbf{c}') \geqslant r$.

(2) Prove that the binary code with generator matrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

is 1–intersecting.

Turn the page please $\longrightarrow$

(3) Let $\mathscr{C} \subset \mathbb{F}_2^n$ be a code of minimum distance $d_{\min}$. Let $d_{\max} \stackrel{\text{def}}{=} \max\{w_{\mathrm{H}}(\mathbf{c}) \mid \mathbf{c} \in \mathscr{C}\}$ and suppose that $d_{\min} > d_{\max}/2$. Prove that $\mathscr{C}$ is r-intersecting for $r = d_{\min} - \frac{d_{\max}}{2}$. *(Hint: Use (1).)*

(4) If $\mathscr{C} \subseteq \mathbb{F}_2^n$ is an r–intersecting code for some $r > 0$ and with minimum distance $d_{\min}$, prove that $r \leqslant \frac{d_{\min}}{2}$. *(Hint: take $\mathbf{c} \neq 0$ a minimum weight codeword, $\mathbf{c}'$ another codeword and consider $\mathbf{c} * \mathbf{c}'$ and $\mathbf{c} * (\mathbf{c} + \mathbf{c}')$.)*

(5) Let $K(n, d)$ be the maximal possible dimension of a linear code in $\mathbb{F}_2^n$ of minimum distance d. Let $r > 0$, prove that any r–intersecting code $\mathscr{C} \subset \mathbb{F}_2^n$ has parameters $[n, k, d]$ which satisfy

$$k \leqslant K(d, r).$$

(Hint: Take $\mathbf{c} \in \mathscr{C}$ of weight d and consider the map $\left\{ \begin{array}{ccc} \mathscr{C} & \longrightarrow & \mathbb{F}_2^d \\ \mathbf{x} & \longmapsto & \mathbf{x} * \mathbf{c} \end{array} \right.$, *where the entries at which $\mathbf{c}$ vanishes are removed.)*

(6) Let $r > 0$. Prove that for any $[n, k, d]$ code that is r-intersecting, $d - k + 1 \geqslant r$.

Hint : Same Hint as for question (5)

(7) Let $\mathscr{C} \subseteq \mathbb{F}_2^n$ be a 1–intersecting code with parameters $[n, k, d]$. let $G \in \mathbb{F}_2^{k \times n}$ be a generator matrix of $\mathscr{C}$. Denote by I_k the $k \times k$ identity matrix. Prove that the code with generator matrix:

$$\left[\begin{array}{c|c|c} & & 0 \\ & & 0 \\ G & I_k & 0 \\ & & \vdots \\ & & 0 \\ \hline 0 \; 0 \; 0 \quad \cdots \quad 0 & 1 \; 1 \quad \cdots \quad 1 & 1 \end{array}\right]$$

is

(a) 1-intersecting;
(b) with parameters $[n + k + 1, k + 1, d']$ such that $d' \geqslant \min(d + 1, k + 1)$.

(8) ($\star$) Prove that there are $(3^n - 2^{n+1} + 1)$ pairs $(\mathbf{a}, \mathbf{b})$ of nonzero vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ such that $\mathbf{a} * \mathbf{b} = \mathbf{0}$.

(9) ($\star$) Denote by $\begin{bmatrix} n \\ k \end{bmatrix}$ the number of binary codes of length n and dimension k. Given a pair $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ such that $\mathbf{a} * \mathbf{b} = \mathbf{0}$, prove that there are $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ codes of dimension k containing $\mathbf{a}$ and $\mathbf{b}$.

(Hint: Prove first that w.l.o.g, one can assume that $\mathbf{a}_1 = 1$, $\mathbf{a}_2 = 0$, $\mathbf{b}_1 = 0$, and $\mathbf{b}_2 = 1$, then look for a smart choice of a complement subspace of $\langle \mathbf{a}, \mathbf{b} \rangle$.)

(10) Prove that there exist at least $\max\left(\begin{bmatrix} n \\ k \end{bmatrix} - \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}(3^n - 2^{n+1} + 1)/2,\ 0\right)$ binary codes of length n and dimension k that are 1–intersecting.

(Hint : Take note that Question 9 considered ordered pairs $(\mathbf{a}, \mathbf{b})$ while the counting of spaces will be related to unordered pairs.)

(11) ($\star$) Admit that there is a constant $\kappa > 0$ such that $\begin{bmatrix} n \\ k \end{bmatrix} = \kappa 2^{k(n-k)}(1 + \circ(1))$ when $n \to +\infty$ and $k \sim Rn$ for some $0 < R < 1$. Prove that for $0 < R < \frac{1}{2}\log_2(\frac{4}{3})$ and for n large enough, there exist 1–intersecting codes of length n and dimension $k = \lfloor Rn \rfloor$.