MPRI **Year 2025–26**

Module CODES: Error-correcting codes and applications to cryptography

---

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 $\mathbb{F}_4$.

> **Answer :** $\{0\}, \{1,4\}, \{2,8\}, \{3,12\}, \{5\}, \{6,9\}, \{7,13\}, \{10\}, \{11,14\}$.

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

> **Answer :** 512.

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

> **Answer :** Consider the cyclotomic class $\{0, 1, 2, 3, 4, 5, 8, 12\}$. It contains 6 consecutive elements hence, by the BCH bound, gives rise to a code of minimum distance $\geqslant 7$. Since it has cardinality 8 the corresponding code has dimension 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;

> **Answer :** Let $I \subseteq \mathbb{Z}/(q^2-1)\mathbb{Z}$ be a minimal cyclotomic class. Let $a \in I$, then, either $aq \equiv a \mod q^2 - 1$ and then $I = \{a\}$ or $aq^2 = a(1 + q^2 - 1) \equiv a \mod q^2 - 1$ and hence $I = \{a, aq\}$.

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

> **Answer :** Let $0 \leqslant a < q^2 - 1$ and denote (by abuse of notation) also by a its class in $\mathbb{Z}/(q^2-1)\mathbb{Z}$. Suppose that $\{a\}$ is a cyclotomic class. Then, $a \equiv aq \mod (q^2-1)$ or equivalently $a(q-1) \equiv 0 \mod (q^2-1)$. Therefore, $a(q-1) = (q^2-1)h$ for some integer h. Equivalently $a = (q+1)h$ for some integer h. Therefore, since $0 \leqslant a < q^2 - 1$, we deduce that $a \in \{0, q+1, 2(q+1), \ldots, (q-2)(q+1)\}$. This yields $q - 1$ classes of cardinality 1.

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

Answer : According to Question 4b, there are $q-1$ minimal cyclotomic classes of cardinality 1. Next, from Question 4a, any other minimal cyclotomic classes has cardinality 2. This gives, $\frac{q^2-q}{2}$ other classes. Therefore, the overall number of minimal cyclotomic classes is

$$q-1+\frac{q^2-q}{2}=\frac{q^2+q}{2}-1.$$

Thus, there are $2^{\frac{q^2+q}{2}-1}$ 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 $d \geqslant t+1$.

Answer : Consider the smallest cyclotomic class I containing $0,1,\dots,t-1$. Since $\{0\}$ is a cyclotomic class and that any other element is contained in a minimal class of cardinality 2, we deduce that $|I| \leqslant 2t-1$. By the BCH bound, it gives rise to a $[q^2-1, \geqslant q^2-2t, \geqslant t+1]$ cyclic code.

Exercise 2.

Note: This exercise is inspired from the article:
Gérard Cohen, Abraham Lempel. *Linear Intersecting codes.* Discrete Mathematics. 56(1). pp 35–43. 1985. `https://doi.org/10.1016/0012-365X(85)90190-6`.

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

$$(x_1,\dots,x_n)*(y_1,\dots,y_n) \stackrel{\text{def}}{=} (x_1y_1,\dots,x_ny_n).$$

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

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

Answer : The support of $\mathbf{c}_1+\mathbf{c}_2$ is $(\mathrm{Supp}(\mathbf{c}_1)\cup\mathrm{Supp}(\mathbf{c}_2)) \setminus (\mathrm{Supp}(\mathbf{c}_1)\cap\mathrm{Supp}(\mathbf{c}_2))$. Since $\mathrm{Supp}(\mathbf{c}_1*\mathbf{c}_2)=\mathrm{Supp}(\mathbf{c}_1)\cap\mathrm{Supp}(\mathbf{c}_2)$, we get the result.

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.

Answer : The nonzero elements of the code are $(110),(011),(101)$ any two of these words have one 1 in common.

(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).*)

Answer : Let $\mathbf{c}_1, \mathbf{c}_2$ be two nonzero codewords. If $\mathbf{c}_1 = \mathbf{c}_2$ then their support intersect at $w_{\mathrm{H}}(\mathbf{c}) \geqslant d_{\min} \geqslant d_{\min} - \frac{d_{\max}}{2}$ positions. Otherwise, from Question (1),

$$d_{\max} \geqslant w_{\mathrm{H}}(\mathbf{c}_1 - \mathbf{c}_1) = w_{\mathrm{H}}(\mathbf{c}_1) + w_{\mathrm{H}}(\mathbf{c}_2) - 2w_{\mathrm{H}}(\mathbf{c}_1 * \mathbf{c}_2) \geqslant 2d_{\min} - w_{\mathrm{H}}(\mathbf{c}_1 * \mathbf{c}_2).$$

Thus

$$w_{\mathrm{H}}(\mathbf{c}_1 * \mathbf{c}_2) \geqslant 2d_{\min} - d_{\max}$$

and taking the minimum over all possible pairs $(\mathbf{c}_1, \mathbf{c}_2) \in (\mathscr{C} \setminus \{0\})^2$ yields the result.

(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 $\mathbf{c} * (\mathbf{c} + \mathbf{c}')$.)*

Answer : Take $\mathbf{c}$ a codeword of weight d and $\mathbf{c}'$ any other nonzero codeword. Let $s \stackrel{\text{def}}{=} w_{\mathrm{H}}(\mathbf{c} * \mathbf{c}')$. If $\mathbf{c}, \mathbf{c}'$ have supports intersecting at $s \leqslant \frac{d_{\min}}{2}$ positions, then we are done. Otherwise $\mathbf{c}$ and $\mathbf{c} + \mathbf{c}'$ will have supports that intersect at $w_{\mathrm{H}}(\mathbf{c}) - s \leqslant \frac{d_{\min}}{2}$ positions.

(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.)

Answer : Let $\mathscr{C}$ be an $[n, k, d]$ r–intersecting code with $k \leqslant K(d, r)$. Let $\mathbf{c} \in \mathscr{C}$ of weight d. Consider $\mathbf{c} \in \mathscr{C}$ the map

$$\phi : \left\{ \begin{array}{ccc} \mathscr{C} & \longrightarrow & \mathbb{F}_2^d \\ \mathbf{x} & \longmapsto & \mathbf{x} * \mathbf{c}. \end{array} \right.$$

By the intersecting property, the above map is injective and its image has minimum distance $\geqslant r$. Hence the result.

(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)

Answer : Consider the map ϕ of the previous question. Its image is a $[d, k, \geqslant r]$ code. The expected result is a direct consequence of Singleton bound applied to that code.

(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:

$$\begin{array}{|c|c|c|}\hline \qquad\qquad G \qquad\qquad & \qquad I_k \qquad & \begin{matrix}0\\0\\0\\\vdots\\0\end{matrix} \\ \hline 0\ \ 0\ \ 0\ \ \cdots\ \ 0 & 1\ \ 1\ \ \cdots\ \ 1 & 1 \\ \hline\end{array}$$

is

(a) 1-intersecting;

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

Answer : The length and dimension of the code are clear from the matrix shape. For the minimum distance, the last row has weight $k+1$ and any other linear combination of rows has the shape $(\mathbf{c} \mid \mathbf{c}')$ where $\mathbf{c} \in \mathscr{C}$ and $\mathbf{c}'$ is nonzero. Thus, such a word has weight $\geqslant d+1$.
There remains to prove the intersecting property. Two **nonzero** codewords have respective shapes $(\mathbf{c}_1, \mathbf{c}_1')$ and $(\mathbf{c}_2, \mathbf{c}_2')$ where $\mathbf{c}_1, \mathbf{c}_2 \in \mathscr{C}$ and $\mathbf{c}_1', \mathbf{c}_2'$ are nonzero. If both $\mathbf{c}_1, \mathbf{c}_2$ are nonzero, the intersecting property is satisfied since $\mathscr{C}$ is intersecting. Now, if for instance $\mathbf{c}_1 = 0$ then $(\mathbf{c}_1, \mathbf{c}_1') = (0 \cdots 011 \cdots 1)$. Since $\mathbf{c}_2'$ is nonzero, the two codewords' supports will intersect at least at one position among $n+1, \ldots, n+k+1$. Thus, the resulting code is 1-intersecting.

(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 $\mathbf{a} * \mathbf{b} = \mathbf{0}$.

Answer : Fix $a \in \mathbb{F}_2^n \setminus \{0\}$ of weight i. Then, there are $2^{n-i} - 1$ nonzero vectors $\mathbf{b}$ such that $\mathbf{a} * \mathbf{b} = \mathbf{0}$. If we sum these over all possible $\mathbf{a}$ this gives a number of ordered pairs $(\mathbf{a}, \mathbf{b})$ such that $\mathbf{a} * \mathbf{b} = \mathbf{0}$ equal to

$$\begin{aligned}
\sum_{\mathbf{a} \in \mathbb{F}_2^n \setminus \{0\}} (2^{n - w_{\mathrm{H}}(a)} - 1) &= \sum_{i=1}^{n} \sum_{\substack{\mathbf{a} \in \mathbb{F}_2^n \\ w_{\mathrm{H}}(\mathbf{a}) = i}} (2^{n-i} - 1) \\
&= \sum_{i=1}^{n} \binom{n}{i} (2^{n-i} - 1). \\
&= \sum_{i=1}^{n} \binom{n}{i} 2^{n-i} - \sum_{i=1}^{n} \binom{n}{i} \\
&= \left(\sum_{i=0}^{n} \binom{n}{i} 2^{n-i} \right) - 2^n - \left(\sum_{i=0}^{n} \binom{n}{i} \right) + 1 \\
&= 3^n - 2^{n+1} + 1.
\end{aligned}$$

(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* $\langle \mathbf{a}, \mathbf{b} \rangle$.)

Answer : The assumption $\mathbf{a} * \mathbf{b} = \mathbf{0}$ entails that $\mathbf{a}, \mathbf{b}$ are non collinear and hence span a code of dimension 2. To characterize codes of dimension k containing $\mathbf{a}, \mathbf{b}$ we have to look for a "canonical" complement subspace of the span $\langle \mathbf{a}, \mathbf{b} \rangle$ of $\mathbf{a}, \mathbf{b}$. After applying a possible permutation on the entries, one can assume w.l.o.g that $\mathbf{a}_1 \neq \mathbf{0}$ ($\mathbf{a}$'s first entry is nonzero) and $\mathbf{b}_2 \neq \mathbf{0}$. Note that the intersecting property entails that $\mathbf{a}_2 = \mathbf{b}_1 = \mathbf{0}$, that is, the code $\langle \mathbf{a}, \mathbf{b} \rangle$ has a generator matrix with shape:

$$\begin{pmatrix} \mathbf{a} \\ \mathbf{b} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \multirow{2}{*}{$(*)$} \\ 0 & 1 & \end{pmatrix}. \tag{2}$$

Now, for any code $\mathscr{C} \subseteq \mathbb{F}_2^n$ containing $\mathbf{a}, \mathbf{b}$, define the subcode

$$\mathscr{C}_{1,2} \stackrel{\text{def}}{=} \{\mathbf{c} \in \mathscr{C} \mid \mathbf{c}_1 = \mathbf{c}_2 = \mathbf{0}\}.$$

Let us prove that $\mathscr{C} = \langle \mathbf{a}, \mathbf{b} \rangle \oplus \mathscr{C}_{1,2}$. Indeed the two codes have zero intersection since any non trivial linear combinations of $\mathbf{a}, \mathbf{b}$ cannot vanish simultaneously at its two leftmost entries (see (2)). Next, for any element $\mathbf{c} = (c_1, c_2, \dots, c_n) \in \mathscr{C}$, we have $\mathbf{c} - c_1\mathbf{a} - c_2\mathbf{b} \in \mathscr{C}_{1,2}$ hence $\mathbf{c}$ can be written as the sum of an element of $\langle \mathbf{a}, \mathbf{b} \rangle$ and an element of $\mathscr{C}_{1,2}$.
Note that $\mathscr{C}_{1,2}$ is uniquely determined from $\mathscr{C}$ and, conversely, for any code $\mathscr{C}_{1,2} \in \mathbb{F}_2^n$ of dimension $k-2$ whose words all vanish at the two first entries, the code $\langle \mathbf{a}, \mathbf{b} \rangle \oplus \mathscr{C}_{1,2}$ gives a code of dimension k containing $\mathbf{a}, \mathbf{b}$. Thus counting such codes containing $\mathbf{a}, \mathbf{b}$ reduces to count codes of length n and dimension $k-2$ that are all zero at the two leftmost entries. This is equivalent to count codes of length $n-2$ and dimension $k-2$.

(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.)*

Answer : There are $\begin{bmatrix} n \\ k \end{bmatrix}$ codes of length n and dimension k. From Question 9, for any non ordered pair $\mathbf{a}, \mathbf{b}$ such that $\mathbf{a} * \mathbf{b} = \mathbf{0}$, there are $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ codes of parameters $[n, k]$ that contain $\mathbf{a}, \mathbf{b}$. From Question 8 there are $(3^n - 2^{n+1} + 1)$ such pairs $\mathbf{a}, \mathbf{b}$ and hence $(3^n - 2^{n+1} + 1)/2$ such non ordered pairs. This yields an upper bound $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix} (3^n - 2^{n+1} + 1)/2$ on the number of non intersecting codes. Hence the lower bound

$$\begin{bmatrix} n \\ k \end{bmatrix} - \begin{bmatrix} n-2 \\ k-2 \end{bmatrix} (3^n - 2^{n+1} + 1)/2$$

on the number of intersecting codes.

(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 $k = \lfloor Rn \rfloor$.

Answer : From Question 10, intersecting codes exist as soon as

$$\begin{bmatrix} n \\ k \end{bmatrix} - \begin{bmatrix} n-2 \\ k-2 \end{bmatrix} (3^n - 2^{n+1} + 1)/2 > 0.$$

Asymptotically, we aim to satisfy the inequality

$$\begin{aligned} \kappa \left(2^{k(n-k)} - 2^{(k-2)(n-k)+n\log_2(3)}\right)(1+\circ(1)) > 0 \\ \kappa \left(2^{k(n-k)}\left(1 - 2^{n\log_2(3)-2(n-k)}\right)\right)(1+\circ(1)) > 0 \\ \kappa \left(2^{k(n-k)}\left(1 - 2^{n(\log_2(3/4)+2R)}\right)\right)(1+\circ(1)) > 0. \end{aligned}$$

When $R < \frac{1}{2}\log_2\left(\frac{4}{3}\right)$, then, $2^{n(\log_2(3/4)+2R)} < 1$ and the above inequality holds for $n \gg 0$.