Mid-term exam, November 29, 2023

You have 1h30. You can write your answers either in French or in English.

Notes.
— In any exercise, any code is linear.
— Questions marked with a (⋆) are harder than the other ones.

Exercise 1. A code \( C \subseteq \mathbb{F}_q^n \) of dimension \( k \) is said to be systematic if it has a generator matrix of the form

\[
\begin{pmatrix}
I_k & R
\end{pmatrix},
\]

for some matrix \( R \in \mathbb{F}_q^{k \times (n-k)} \) and where \( I_k \) denotes the \( k \times k \) identity matrix.

1. Prove that a code \( C \subseteq \mathbb{F}_q^n \) with generator matrix \( G \) is systematic if and only if the \( k \) leftmost columns of \( G \) are linearly independent.

**Answer:** Suppose that \( G \)'s \( k \) leftmost columns are independent. Then, they form an invertible square matrix denoted by \( S \). Next, the matrix \( S^{-1}G \) has the expected shape. Conversely, suppose that \( C \) is systematic. Then, it has a generator matrix:

\[
G' = \begin{pmatrix} I_k & R \end{pmatrix}.
\]

Since \( G \) and \( G' \) are generator matrices of the same code, there exists an invertible matrix \( S \) such that \( G = SG' \). Hence \( G = (S | SR) \). Thus, the \( k \) leftmost columns of \( G \) are those of \( S \) which are independent since \( S \) is invertible.

2. Prove that \( ( -R^T | I_{n-k} ) \) is a parity check matrix of \( C \).

**Answer:** The matrix has rank \( n - k \), hence it suffices to prove that it generates a code contained in \( C^\perp \). A simple calculation gives:

\[
\begin{pmatrix} I_k & R \end{pmatrix} \begin{pmatrix} -R^T & I_{n-k} \end{pmatrix} \begin{pmatrix} I_{n-k} \end{pmatrix} = \begin{pmatrix} -R \end{pmatrix} = -R + R = 0.
\]

3. Give an example of non systematic code of length 4 and dimension 2 over \( \mathbb{F}_2 \).

**Answer:** For instance, the code with generator matrix

\[
\begin{pmatrix}
1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1
\end{pmatrix}.
\]

For any permutation \( \sigma \in \mathfrak{S}_n \) (the permutation group over \( n \) elements), denote by \( P_\sigma \) the corresponding permutation matrix. Then, for a code \( C \), denote by \( C P_\sigma \) the permuted code defined by

\[
C P_\sigma \overset{\text{def}}{=} \{ c P_\sigma \mid c \in C \}.
\]
4. Prove that for any linear code $C \subseteq \mathbb{F}_q^n$, there exists $\sigma \in \mathcal{S}_n$ such that $C\mathbf{P}_\sigma$ is systematic.

**Answer:** Let $G \in \mathbb{F}_q^{k \times n}$ be a generator matrix of $C$. It has rank $k$ and hence has $k$ linearly independent columns with indexes $i_1, \ldots, i_k$. Let $\sigma \in \mathcal{S}_n$ be a permutation sending $i_1, \ldots, i_k$ on $1, \ldots, k$. Then, the $k$ leftmost columns of $GP_\sigma$ are linearly independent and Question 1 permits to conclude.

5. Prove that an $[n, k, n - k + 1]$-code (i.e. a code achieving Singleton bound) is systematic.

**Answer:** Let $G \in \mathbb{F}_q^{k \times n}$ be a generator matrix of such a code $C$. Denote by $S \in \mathbb{F}_q^{k \times k}$ the submatrix formed by these $k$ leftmost columns of $G$. Suppose that the $k$ leftmost columns of $G$ of the code are not independent. Then, $S$ has not full rank and hence, there exists $T \in \text{GL}_k(\mathbb{F}_q)$ such that the last row of $TS$ is zero. Since $TG$ is another generator matrix of $C$ with independent rows, the last row of $TG$ is a nonzero codeword of $C$ with at least $k$ zero entries, i.e., with Hamming weight $\leq n - k$. A contradiction.

6. Prove that a cyclic code is systematic.

**Answer:** Let $C \subseteq \mathbb{F}_q^n$ be a cyclic code of dimension $k$. Let $g \in \mathbb{F}_q[X]/(X^n - 1)$ be a generating polynomial of $C$ with degree $n - k$ and whose constant coefficient is nonzero. Then, the generator matrix below has its $k$ leftmost columns which are independent:

$$
\begin{pmatrix}
g_0 & g_1 & \cdots & g_{n-k+1} & 0 & \cdots & 0 \\
0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k+1}
\end{pmatrix}
$$

A code of length $n = 2n_0$ for some positive integer $n_0$ is doubly circulant if it is stable by a “double cyclic shift”, i.e., it has a generator matrix of the form:

$$
\begin{pmatrix}
f_0 & f_1 & \cdots & f_{n_0-1} & g_0 & g_1 & \cdots & g_{n_0-1} \\
f_{n_0-1} & f_0 & f_1 & \cdots & f_{n_0-2} & g_{n_0-1} & g_0 & \cdots & g_{n_0-2} \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
f_{f_1} & f_2 & \cdots & f_{n_0-1} & f_0 & g_1 & \cdots & g_{n_0-1} & g_0
\end{pmatrix}
$$

Similarly to cyclic codes, doubly circulant codes can be represented as a pair of polynomials $(f(X), g(X)) \in (\mathbb{F}_q[X]/(X^{n_0} - 1))^2$. In particular, any element of the code is represented by a pair $(u(X)f(X) \mid u(X)g(X))$ for some $u \in \mathbb{F}_q[X]/(X^{n_0} - 1)$.

7. (⋆) Prove that a doubly circulant code defined by the pair $(f(X), g(X)) \in (\mathbb{F}_q[X]/(X^{n_0} - 1))^2$ has dimension $n_0$ if and only if $\text{gcd}(f, g, X^{n_0} - 1) = 1$.

**Hint. One could consider the map**

$$
\begin{align*}
&\mathbb{F}_q[X]/(X^{n_0} - 1) \rightarrow C \\
u(X) &\mapsto (u(X)f(X) \mid u(X)g(X))
\end{align*}
$$

**which turns out to be injective if and only if the code has dimension $n_0$.**
Answer: Suppose that the map
\[
\begin{array}{c}
\{ \frac{\mathbb{F}_q[X]}{(X^{n_0} - 1)} \} \\
\xrightarrow{u(X)} \xrightarrow{(u(X)f(X))} \mathcal{C} \\
\xrightarrow{u(X)g(X)}
\end{array}
\]

is not injective. Let \( u(X) \) such that \( u(X)f(X) \equiv u(X)g(X) \equiv 0 \mod X^{n_0} - 1 \). Choose representatives of \( u, f, g \) of degree \( < n_0 \). We allow ourselves to denote also these representatives as \( u, f, g \). Thus, \( X^{n_0} - 1 \) divides both \( uf \) and \( ug \). For degree reasons, \( X^{n_0} - 1 \) cannot divide \( u \). Let \( P \) be a irreducible factor of \( X^{n_0} - 1 \) that does not divide \( u \). Thus \( \gcd(f, g, X^{n_0} - 1) \) is nontrivial. Conversely, suppose this \( \gcd \) is \( 1 \), then the aforementioned map is injective, yielding a code of dimension \( n_0 \).

8. (*) Prove that a doubly circulant code defined by the pair \( (f(X), g(X)) \in (\mathbb{F}_q[X]/(X^{n_0} - 1))^2 \) is systematic if and only if \( f \) is invertible in \( (\mathbb{F}_q[X]/(X^{n_0} - 1))^2 \).

Answer: First observe that the product of two circulant matrices associated to polynomials \( a(X) \) and \( b(X) \) is nothing but the circulant matrix associated to the product \( ab \mod X^{n_0} - 1 \). Thus, if \( f \) is invertible, then the \( n_0 \) leftmost columns form an invertible matrix and hence, from Question 1 the code is systematic. Conversely, if the code is systematic, we deduce that the circulant matrix associated to \( f \) is invertible and hence that \( f \) is invertible modulo \( X^{n_0} - 1 \).

Exercise 2. Let \( n \) be a positive integer prime to \( q \). Let \( \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q^n \) be cyclic codes with generating polynomials \( g_\mathcal{C}, g_\mathcal{D} \) which both divide \( (X^n - 1) \) and cyclotomic classes \( I_\mathcal{C}, I_\mathcal{D} \subseteq \mathbb{Z}/n\mathbb{Z} \).

1. (a) Prove that \( \mathcal{C} \cap \mathcal{D} \) is cyclic;

Answer: Let \( \sigma \) denote the cyclic shift. Let \( c \in \mathcal{C} \cap \mathcal{D} \), then, by cyclicity of the codes, \( \sigma(c) \in \mathcal{C} \) and \( \sigma(c) \in \mathcal{D} \).

(b) express its generating polynomial in terms of \( g_\mathcal{C}, g_\mathcal{D} \);

Answer: Regarded as a polynomial, a codeword \( c(X) \in \mathcal{C} \cap \mathcal{D} \) is divisible by both \( g_\mathcal{C} \) and \( g_\mathcal{D} \). Hence it is divisible by \( \text{lcm}(g_\mathcal{C}, g_\mathcal{D}) \). Conversely, a word divisible by \( \text{lcm}(g_\mathcal{C}, g_\mathcal{D}) \) is both in \( \mathcal{C} \) and \( \mathcal{D} \).

(c) express its cyclotomic classes in terms of \( I_\mathcal{C}, I_\mathcal{D} \).

Answer: \( I_\mathcal{C} \cup I_\mathcal{D} \).
2. Same questions ((a), (b), (c)) for \( \mathcal{C} + \mathcal{D} \).

**Answer:**

(a) If \( c + d \in \mathcal{C} + \mathcal{D} \), then \( \sigma(c + d) = \sigma(c) + \sigma(d) \) which is in \( \mathcal{C} + \mathcal{D} \) by cyclicity of the two codes.

(b) Let \( g \) be a greatest common divisor of \( \mathcal{C} + \mathcal{D} \) and denote by \( g_{\mathcal{C} + \mathcal{D}} \) the generating polynomial of \( \mathcal{C} + \mathcal{D} \) dividing \( X^n - 1 \). One sees easily that \( g \) divides any word in \( \mathcal{C} + \mathcal{D} \). Hence \( g | g_{\mathcal{C} + \mathcal{D}} \). Moreover, by Bézout Theorem, there exist \( u, v \) such that

\[
ug_{\mathcal{C}} + vg_{\mathcal{D}} = g.
\]

Therefore, \( g \in \mathcal{C} + \mathcal{D} \) and hence \( g_{\mathcal{C} + \mathcal{D}} | g \). Consequently \( g_{\mathcal{C} + \mathcal{D}} = \gcd(g_{\mathcal{C}}, g_{\mathcal{D}}) \).

(c) \( I_{\mathcal{C}} \cap I_{\mathcal{D}} \).

3. (⋆) Consider the code

\[
\mathcal{E} \overset{\text{def}}{=} \text{Span}_{\mathbb{F}_q} \{(u(X)v(X)) \mid u \in \mathcal{C}, v \in \mathcal{D}\},
\]

where the product is performed in the ring \( \mathbb{F}_q[X]/(X^n - 1) \), and the code

\[
\mathcal{F} \overset{\text{def}}{=} \{(g_{\mathcal{D}}(X)u(X)) \mid u(X) \in \mathcal{C}\}.
\]

Prove that both \( \mathcal{E} \) and \( \mathcal{F} \) equal \( \mathcal{C} \cap \mathcal{D} \).

**Hint.** One can first suppose that \( g_{\mathcal{C}} \) and \( g_{\mathcal{D}} \) are prime to each other.

**Answer:** Clearly, both \( \mathcal{E} \) and \( \mathcal{F} \) are contained in \( \mathcal{C} \cap \mathcal{D} \). Therefore, there remains to prove that the generating polynomial \( g = \text{lcm}(g_{\mathcal{C}}, g_{\mathcal{D}}) \) of \( \mathcal{C} \cap \mathcal{D} \) is in \( \mathcal{E} \) (resp. \( \mathcal{F} \)).

If \( g_{\mathcal{C}} \) and \( g_{\mathcal{D}} \) are prime to each other, one sees easily that both codes contain the product \( g_{\mathcal{C}}g_{\mathcal{D}} \) is in \( \mathcal{E} \) (resp. \( \mathcal{F} \)).

If the two generating polynomials are not prime to each other, then, one can observe that, since both \( g_{\mathcal{C}}, g_{\mathcal{D}} \) divide \( X^n - 1 \) and \( X^n - 1 \) is squarefree (we assumed \( n \) to be prime with \( q \)), then

\[
\gcd(g_{\mathcal{C}}g_{\mathcal{D}}, X^n - 1) = \text{lcm}(g_{\mathcal{C}}, g_{\mathcal{D}}) = g.
\]

Next, by Bézout’s Theorem, there exist polynomials \( u, v \) such that

\[
u(X)(X^n - 1) + v(X)g_{\mathcal{C}}g_{\mathcal{D}} = g,
\]

which proves that \( g \in \mathcal{E} \) (resp. \( \mathcal{F} \)).

**Exercise 3.** For a vector \( c \in \mathbb{F}_q^n \) denote by \( \text{Supp}(c) \) the set \( \text{Supp}(c) \overset{\text{def}}{=} \{i \in \{1, \ldots, n\} \mid c_i \neq 0\} \). Given a linear code \( \mathcal{C} \subseteq \mathbb{F}_q^n \) and \( I \subseteq \{1, \ldots, n\} \), we denote by

\[
\mathcal{C}_{|I} \overset{\text{def}}{=} \{c \in \mathcal{C} \mid \text{Supp}(c) \subseteq I\}.
\]

For a positive integer \( r \leq n \), the \( r \)-th generalised Hamming weight of \( \mathcal{C} \) is defined as

\[
d_r(\mathcal{C}) \overset{\text{def}}{=} \min \{\sharp I \mid I \subseteq \{1, \ldots, n\} \text{ and } \dim \mathcal{C}_{|I} = r\}.
\]
1. Prove that $d_1(\mathcal{C})$ is nothing but the minimum distance.

**Answer:** Let $d$ be the minimum distance and $c$ be a minimum weight codeword with support $I$, i.e., $\sharp I = d$. Then, $\dim \mathcal{C}_I \geq 1$. If $\dim \mathcal{C}_I \geq 2$, then, by elimination, one could construct a nonzero codeword whose support would be a proper subset of $I$, which contradicts the fact that $d$ is the minimum distance. Thus, $\dim \mathcal{C}_I = 1$ and $\dim \mathcal{C}_J = 0$ for any $J$ with cardinality $< d$. Hence the result.

2. Let $k$ be the dimension of $\mathcal{C}$, prove that

$$1 \leq d_1(\mathcal{C}) < d_2(\mathcal{C}) < \cdots < d_k(\mathcal{C}) \leq n.$$

**Answer:** Clearly, there is no weight above $d_k(\mathcal{C})$. Let $1 \leq t \leq k$ and $I \subseteq \{1, \ldots, n\}$ such that $\sharp I = d_t(\mathcal{C})$ and $\dim \mathcal{C}_I = t$. Let $i \in I$, by definition of $d_t(\mathcal{C})$ the subspace $\mathcal{C}_{I \setminus \{i\}}$ of codewords of $\mathcal{C}_I$ whose $i$-th entry vanishes is a proper subspace of $\mathcal{C}_I$ of codimension 1. Therefore

$$d_t(\mathcal{C}) > \sharp I \setminus \{a\} \geq d_{t-1}(\mathcal{C}).$$

This proves that the sequence is strictly increasing.

3. Prove that for an $[n, k]$ code and any $r \leq k$, we have

$$d_r(\mathcal{C}) \leq n - k + r.$$

**Answer:** This a direct consequence of Singleton bound together with Question 2.

4. Deduce the sequence of generalised Hamming weights for a code achieving Singleton bound.

**Answer:** Due to Question 1, we have $d = d_1(\mathcal{C})$. Then, from Question 2, we deduce that the sequence of generalised Hamming weights cannot be something else but

$$n - k + 1, n - k + 2, \ldots, n - 1, n.$$