MPRI **Year 2023–24**

Module 2.13.2 : Error-correcting codes and applications to cryptography

---

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 ($\star$) are harder than the other ones.*

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

$$\left(\mathbf{I}_k \quad | \quad \mathbf{R} \right),$$

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

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

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

   $$\mathbf{G}' = \left(\mathbf{I}_k \quad | \quad \mathbf{R} \right).$$

   Since $\mathbf{G}$ and $\mathbf{G}'$ are generator matrices of the same code, there exists an invertible matrix $\mathbf{S}$ such that $\mathbf{G} = \mathbf{S}\mathbf{G}'$. Hence $\mathbf{G} = (\mathbf{S} \mid \mathbf{S}\mathbf{R})$. Thus, the k leftmost columns of $\mathbf{G}$ are those of $\mathbf{S}$ which are independent since $\mathbf{S}$ is invertible.

2. Prove that $(-\mathbf{R}^\top \mid \mathbf{I}_{n-k})$ is a parity check matrix of $\mathscr{C}$.

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

   $$\left(\mathbf{I}_k \quad | \quad \mathbf{R} \right)\left(-\mathbf{R}^\top \quad | \quad \mathbf{I}_{n-k} \right)^\perp = \left(\mathbf{I}_k \quad | \quad \mathbf{R} \right)\begin{pmatrix} -\mathbf{R} \\ \mathbf{I}_{n-k} \end{pmatrix} = -\mathbf{R} + \mathbf{R} = 0.$$

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 $\mathbf{P}_\sigma$ the corresponding permutation matrix. Then, for a code $\mathscr{C}$, denote by $\mathscr{C}\mathbf{P}_\sigma$ the *permuted code* defined by

$$\mathscr{C}\mathbf{P}_\sigma \stackrel{\text{def}}{=} \{\mathbf{c}\mathbf{P}_\sigma \mid \mathbf{c} \in \mathscr{C}\}.$$

4. Prove that for any linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$, there exists $\sigma \in \mathfrak{S}_n$ such that $\mathscr{C}\mathbf{P}_\sigma$ is systematic.

   Answer : Let $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ be a generator matrix of $\mathscr{C}$. It has rank k and hence has k linearly independent columns with indexes $i_1, \dots, i_k$. Let $\sigma \in \mathfrak{S}_n$ be a permutation sending $i_1, \dots, i_k$ on $1, \dots, k$. Then, the k leftmost columns of $\mathbf{G}\mathbf{P}_\sigma$ 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 $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ be a generator matrix of such a code $\mathscr{C}$. Denote by $\mathbf{S} \in \mathbb{F}_q^{k\times k}$ the submatrix formed by these k leftmost columns of $\mathbf{G}$. Suppose that the k leftmost columns of $\mathbf{G}$ of the code are not independent. Then, $\mathbf{S}$ has not full rank and hence, there exists $\mathbf{T} \in \mathbf{GL}_k(\mathbb{F}_q)$ such that the last row of $\mathbf{TS}$ is zero. Since $\mathbf{TG}$ is another generator matrix of $\mathscr{C}$ with independent rows, the last row of $\mathbf{TG}$ is a nonzero codeword of $\mathscr{C}$ with at least k zero entries, *i.e.*, with Hamming weight $\leqslant n-k$. A contradiction.

6. Prove that a cyclic code is systematic.

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

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

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 :

$$\left(\begin{array}{ccccc|ccccc} f_0 & f_1 & \cdots & \cdots & f_{n_0-1} & g_0 & g_1 & \cdots & \cdots & g_{n_0-1} \\ f_{n_0-1} & f_0 & f_1 & \cdots & f_{n_0-2} & g_{n_0-1} & g_0 & g_1 & \cdots & g_{n_0-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & f_1 & \vdots & & \ddots & \ddots & g_1 \\ f_1 & f_2 & \cdots & f_{n_0-1} & f_0 & g_1 & g_2 & \cdots & g_{n_0-1} & g_0 \end{array}\right).$$

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. ($\star$) 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 $\gcd(f, g, X^{n_0}-1) = 1$.

   Hint. One could consider the map

$$\left\{ \begin{array}{ccc} \mathbb{F}_q[X]/(X^{n_0}-1) & \longrightarrow & \mathscr{C} \\ u(X) & \longmapsto & (u(X)f(X)) \mid u(X)g(X)) \end{array} \right.$$

   which turns out to be injective if and only if the code has dimension n_0.

Answer : Suppose that the map

$$\begin{cases} \mathbb{F}_q[X]/(X^{n_0}-1) & \longrightarrow & \mathscr{C} \\ u(X) & \longmapsto & (u(X)f(X)) \mid u(X)g(X)) \end{cases}$$

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, then this factor divides both f and g. 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. ($\star$) 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 $\mathscr{C}, \mathscr{D} \subseteq \mathbb{F}_q^n$ be cyclic codes with generating polynomials $g_{\mathscr{C}}, g_{\mathscr{D}}$ which both divide (X^n-1) and cyclotomic classes $I_C, I_D \subseteq \mathbb{Z}/n\mathbb{Z}$.

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

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

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

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

   (c) express its cyclotomic classes in terms of I_C, I_D.

   Answer : $I_{\mathscr{C}} \cup I_{\mathscr{D}}$.

2. Same questions ((a), (b), (c)) for $\mathscr{C} + \mathscr{D}$.

Answer :

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

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

$$ug_{\mathscr{C}} + vg_{\mathscr{D}} = g.$$

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

(c) $I_{\mathscr{C}} \cap I_{\mathscr{D}}$.

3. ($\star$) Consider the code

$$\mathscr{E} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{(u(X)v(X)) \mid u \in \mathscr{C},\ v \in \mathscr{D}\},$$

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

$$\mathscr{F} \stackrel{\text{def}}{=} \{(g_{\mathscr{D}}(X)u(X)) \mid u(X) \in \mathscr{C}\}.$$

Prove that both $\mathscr{E}$ and $\mathscr{F}$ equal $\mathscr{C} \cap \mathscr{D}$.
Hint. One can first suppose that $g_{\mathscr{C}}$ and $g_{\mathscr{D}}$ are prime to each other.

Answer : Clearly, both $\mathscr{E}$ and $\mathscr{F}$ are contained in $\mathscr{C} \cap \mathscr{D}$. Therefore, there remains to prove that the generating polynomial $g = \mathrm{lcm}(g_{\mathscr{C}}, g_{\mathscr{D}})$ of $\mathscr{C} \cap \mathscr{D}$ is in $\mathscr{E}$ (resp. $\mathscr{F}$).
If $g_{\mathscr{C}}$ and $g_{\mathscr{D}}$ are prime to each other, one sees easily that both codes contain the product $g_{\mathscr{C}}g_{\mathscr{D}}$ is in $\mathscr{E}$ (resp. $\mathscr{F}$).
If the two generating polynomials are not prime to each other, then, one can observe that, since both $g_{\mathscr{C}}, g_{\mathscr{D}}$ divide $X^n - 1$ and $X^n - 1$ is squarefree (we assumed n to be prime with q), then

$$\gcd(g_{\mathscr{C}}g_{\mathscr{D}}, X^n - 1) = \mathrm{lcm}(g_{\mathscr{C}}, g_{\mathscr{D}}) = g.$$

Next, by Bézout's Theorem, there exist polynomials u, v such that

$$u(X)(X^n - 1) + v(X)g_{\mathscr{C}}g_{\mathscr{D}} = g,$$

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

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

$$\mathscr{C}_{|I} \stackrel{\text{def}}{=} \{\mathbf{c} \in \mathscr{C} \mid \mathrm{Supp}(\mathbf{c}) \subseteq I\}.$$

For a positive integer $r \leqslant n$, the r–*th generalised Hamming weight* of $\mathscr{C}$ is defined as

$$d_r(\mathscr{C}) \stackrel{\text{def}}{=} \min\{\sharp I \mid I \subseteq \{1, \ldots, n\} \quad \text{and} \quad \dim \mathscr{C}_{|I} = r\}.$$

1. Prove that $d_1(\mathscr{C})$ is nothing but the minimum distance.

   Answer : Let d be the minimum distance and $\mathbf{c}$ be a minimum weight codeword with support I, *i.e.*, $\sharp I = d$. Then, $\dim \mathscr{C}_{|I} \geqslant 1$. If $\dim \mathscr{C}_{|I} \geqslant 2$, 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, $\dim \mathscr{C}_{|I} = 1$ and $\dim \mathscr{C}_{|J} = 0$ for any J with cardinality $< d$. Hence the result.

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

$$1 \leqslant d_1(\mathscr{C}) < d_2(\mathscr{C}) < \cdots < d_k(\mathscr{C}) \leqslant n.$$

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

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

   This proves that the sequence is strictly increasing.

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

$$d_r(\mathscr{C}) \leqslant n - k + r.$$

   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 $d = d_1(\mathscr{C})$. Then, from Question 2, we deduce that the sequence of generalised Hamming weights cannot be something else but

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