MPRI **Year 2022–23**

Module 2.13.2 : Error correcting codes and applications to cryptography

---

Mid-term exam, December 1st, 2022

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

Note. *In both exercises, any code is linear.*

Exercise 1. Let $C \subseteq \mathbb{F}_q^n$ be a code of length n. The *support* of C is the subset

$$\mathrm{Supp}(C) \stackrel{\text{def}}{=} \{i \in \{1, \ldots, n\} \mid \exists c \in C,\ c_i \neq 0\}.$$

1°) Prove that $j \notin \mathrm{Supp}(C)$ if and only if for any generator matrix G of C, the j-th column of G is zero.

Answer : Suppose that some generator matrix G of C has a nonzero j–th column, then, for some row index i we have $G_{ij} \neq 0$. Then the i–th row of this generator matrix is a codeword with a nonzero j–th entry. A contradiction.
The converse statement is straightforward.

2°) Prove that $\mathrm{Supp}(C) = \{1, \ldots, n\}$ if and only if the minimum distance $C^\perp$ satisfies $d(C^\perp) > 1$.

Answer : A generator matrix of C is a parity–check matrix of $C^\perp$. Using the previous question, a code has support $\{1, \ldots, n\}$ if and only if any generator matrix has a zero column, which is equivalent to having weight 1 vectors in its kernel.

A code is said to be *degenerated* if there exist nonempty sets $I, J \subseteq \{1, \ldots, n\}$ such that $I \cap J = \emptyset$ and there exist two codes C_I, C_J of length n, with respective supports I and J such that

$$C = C_I + C_J. \tag{1}$$

3°) Prove that the sum (1) is a direct sum.

Answer : It suffices to prove that $C_I \cap C_J = \{0\}$. This is obvious since a vector in this intersection has support contained in $I \cap J$ which is empty.

4°) Prove that the minimum distance of a degenerated code C is the minimum of the minimum distances of the codes C_I, C_J in (1).

Answer : C contains C_I and C_J and hence contains their minimum weight codewords. Thus its minimum distance is at most the minimum of those of C_I, C_J. Conversely, any $c \in C$ has a unique decomposition $c = c_I + c_J$ relative to the aforementioned direct sum and, for support reasons, the weight of c is the sum of the weights of c_I and c_J, thus, for a nonzero c, its weight is larger than the minimum of the minimum distances of C_I, C_J. This yields the result.

5°) If C is degenerated with $I = \{1, \ldots, s\}$ and $J = \{s+1, \ldots, n\}$, give the shape of any generator matrix of C.

Answer : The matrix is block–diagonal

$$G \begin{pmatrix} G_I & (0) \\ (0) & G_J \end{pmatrix}$$

with a $k_I \times s$ block G_I on the top–left–hand corner and a $k_J \times (n-s)$ one G_J on the bottom–right–hand corner.

6°) If C is degenerated, prove that there exists a diagonal matrix D whose diagonal entries are **not** all equal and such that

$$\forall c \in C, \ c \cdot D \in C.$$

Answer : Since C is degenerated, then $C = C_I \oplus C_J$ for some non trivial partition I, J of $\{1, \ldots, n\}$. Let D be the diagonal matrix with diagonal entries $d_1, \ldots, d_n$ such that $d_i = 1$ if $i \in I$ and 0 if $i \in J$. Then, the right multiplication by D sends a codeword $c = c_I + c_J$ onto c_I which is in C too.

7°) Suppose now that there exists a diagonal matrix D whose diagonal entries are not all equal and such that $cD \in C$ for any $c \in C$. We aim to prove that C is degenerated.

(a) Prove first that for any polynomial P and any $c \in C$, $c \cdot P(D) \in C$.

Answer : Let $c \in C$, clearly $cD \in C$ and $cD^s \in C$ for any non-negative integer s. Since C is linear, then any linear combination of the cD^s for $s \geqslant 0$ is in C.

(b) Since the diagonal entries of D are not all equal, prove the existence of two polynomials P_1, P_2 such that $P_1(D), P_2(D)$ are nonzero, have only 0's and 1's on their diagonals and satisfying $P_1(D) + P_2(D) = I_n$, where I_n denotes the $n \times n$ identity matrix.

Answer : Denote by $d_1, \ldots, d_n$ the diagonal entries of D. Denote by $A \subseteq \mathbb{F}_q$ the set $\{d_1, \ldots, d_n\}$ (here we mean the *set* and not the list, *i.e.* we remove repeated entries). By assumption A has cardinal at least 2 and hence one can split A in the disjoint union of two nonempty sets $A = U \cup V$.
Then, by Lagrange interpolation, there exist polynomials P_1, P_2 such that P_1 sends U onto 1 and V onto 0 and P_2 sends U onto 0 and V onto 1. These polynomials satisfy the requested properties.

(c) Use the previous result to prove that C is degenerated.

Answer : Let $C_I = CP_1(D)$ and $C_J = CP_2(D)$. Since $P_1(D) + P_2(D) = I_n$, we deduce that $C_I + C_J = C$, moreover, the supports of the codes are disjoint and correspond to the sets I, J on which the diagonal entries of $P_1(D)$ respectively equal 0 and 1.

8°) Propose a polynomial time algorithm taking as input a code C (represented with a generator matrix G) and deciding whether a code is degenerated.

Answer : Compute the space of diagonal matrices D such that $CD \subseteq C$. This can be done by solving the following linear system. Consider the formal matrix D whose diagonal entries are variables $x_1, \ldots, x_n$ and denote by G, H a generator and a parity–check matrix of C. Then, solve the system :

$$GDH^\top = 0.$$

The space of solutions contains the space of scalar matrices λI_n. This space has dimension 1. If the code is degenerated then this space contains other matrices and hence has dimension $\geqslant 2$. This yields our algorithm :

- compute the space of solutions of $GDH^\top = 0$ whose unknown is a diagonal matrix D.
- if the solution space has dimension 1 return "Non degenerated", else return "degenerated".

Exercise 2.

1°) Give the list of minimal binary cyclotomic classes of $\mathbb{Z}/17\mathbb{Z}$ (*i.e.* the subsets $A \subseteq \mathbb{Z}/17\mathbb{Z}$ such that $x \in A \Rightarrow 2x \in A$).

Answer : $\{0\}$, $\{1, 2, 4, 8, 16, 15, 13, 9\}$, $\{3, 6, 12, 7, 14, 11, 5, 10\}$.

2°) Deduce the number of possible cyclic codes in $\mathbb{F}_2^{17}$.

Answer : 8.

In the sequel, we wish to study codes of length n over $\mathbb{F}_q$ where n is an odd **prime** number such that $\gcd(n, q) = 1$. We recall that $\mathbb{Z}/n\mathbb{Z}$ is a field and that its group of nonzero elements splits in two disjoint parts

$$(\mathbb{Z}/n\mathbb{Z})^\times = S \cup \overline{S},$$

where S is the set of (nonzero) squares and $\overline{S}$ the set of non-squares. It is well–known (and admitted) that $|S| = |\overline{S}| = \frac{n-1}{2}$. We also suppose that 2 is a square in $\mathbb{Z}/n\mathbb{Z}$.

3°) Prove that both S and $\overline{S}$ are cyclotomic classes.

Answer : Since 2 is a square in $\mathbb{Z}/n\mathbb{Z}$, then both S and $\overline{S}$ are stable by multiplication by 2.

4°) Deduce the sets $S, \overline{S}$ for $n = 17$ and $q = 2$.

Answer : $S = \{1, 2, 4, 8, 16, 15, 13, 9\}$, $\overline{S} = \{3, 6, 12, 7, 14, 11, 5, 10\}$.

5°) Give the dimension of the cyclic code associated to the cyclotomic class S.

Answer : 9.

From now on, we suppose that $q = 2$ and that -1 is **not** a square in $\mathbb{Z}/n\mathbb{Z}$. We still assume that 2 is a square in $\mathbb{Z}/n\mathbb{Z}$.

6°) (a) Prove that the map $\left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & -x \end{array} \right.$ sends S onto $\overline{S}$ and conversely.

Answer : Since -1 is not a square, for any square a, the number $-a$ is a non-square. Since $S, \overline{S}$ form a partition of $\mathbb{Z}/n\mathbb{Z}^\times$ and the map $x \mapsto -x$ is an involution of $\mathbb{Z}/n\mathbb{Z}^\times$ sending S onto $\overline{S}$, it should send $\overline{S}$ onto S.

(b) Let α be a primitive n–th root of the unity in an algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$. Let

$$g_S(X) \stackrel{\text{def}}{=} \prod_{i \in S} (X - \alpha^i) \quad \text{and} \quad g_{\overline{S}}(X) \stackrel{\text{def}}{=} \prod_{j \in \overline{S}} (X - \alpha^j).$$

We admit that that $\sum_{j \in S} j = 0$. Prove that

$$g_{\overline{S}}(X) = X^{\frac{n-1}{2}} g_S(1/X).$$

Answer :

$$\begin{aligned} X^{\frac{n-1}{2}} g_S(1/X) &= \prod_{j \in S} (1 - \alpha^j X) \\ &= \prod_{j \in S} \alpha^j (X - \alpha^{-j}) \\ &= \alpha^{\sum_{j \in S} j} \prod_{j \in \overline{S}} (X - \alpha^j) \end{aligned}$$

The result is a consequence of the assumption $\sum_{j \in S} j = 0$. Note that the assumption can be proved as follows : squares in $\mathbb{Z}/n\mathbb{Z}^\times$ for the group of $\frac{n-1}{2}$–th roots of unity in $\mathbb{Z}/n\mathbb{Z}$ and hence their sum is zero.

The objective of the end of the exercise is to get a lower bound for the minimum distance of the code C associated to $g_S(X)$. Denote by d its minimum distance and we assume from now on that d is **odd**. Let $a(X) = \sum_{i=0}^{n-1} a_i X^i \in C$ (hence g_S divides a) with weight d.

7°) Let $a'(X) \stackrel{\text{def}}{=} X^{n-1} a(1/X) = \sum_{j=0}^{n-1} a_j X^{n-1-j}$. Prove that the polynomial $a(X)a'(X)$ when regarded as an element of $\mathbb{F}_2[X]$ (**not** in $\mathbb{F}_2[X]/(X^n - 1)$) has at most $d^2 - d + 1$ monomials.
Hint. Compute the number of pairs of a monomial of a and a monomial of a' whose product is a monomial of degree $n-1$.

Answer : Computing the product consists in computing d^2 products of monomials. However, d pairs of monomials yield a product of the same degree. Namely the pairs $(a_i X^i, a_i X^{n-1-i})$ all give a multiple of X^{n-1}. Therefore, the resulting product has at most $d^2 - d + 1$ distinct monomials.

8°) Prove that $g_S g_{\overline{S}}$ divides aa'.

Answer : $g_S(X)$ divides $a(X)$, which means that $a(X) = g_S(X)u(X)$ for some polynomial u of degree $\deg(a) - |S|$. Then,

$$\begin{aligned} X^{n-1} a(1/X) &= X^{n-1-\deg(a)} X^{|S|} g_S(1/X) X^{\deg(a)-|S|} u(1/X) \\ &= X^{n-1-\deg(a)} g_{\overline{S}}(X) X^{\deg(a)-|S|} u(1/X). \end{aligned}$$

Therefore, $g_{\overline{S}}$ divides a' and hence $g_S g_{\overline{S}}$ divides aa'.

9°) Prove that for any $P(X) \in \mathbb{F}_2[X]$,

$$P(X)g_S(X)g_{\overline{S}}(X) \equiv P(1)g_S(X)g_{\overline{S}}(X) \mod X^n - 1.$$

Answer : Note first that

$$g_S(X)g_{\overline{S}}(X) = \prod_{i \in \mathbb{Z}/n\mathbb{Z}^\times} (X - \alpha^i) = \frac{X^n - 1}{X - 1}$$

.

Next, for $P \in \mathbb{F}_2[X]$ decomposed as, $P(X) = P(1) + (X - 1)Q(X)$ for some polynomial Q, we have

$$P(X)g_S(X)g_{\overline{S}}(X) = P(1)\frac{X^n - 1}{X - 1} + (X^n - 1)Q(X) \equiv P(1)g_S(X)g_{\overline{S}}(X) \mod X^n - 1.$$

10°) Recall that d is assumed to be odd. Prove that $a(1) = a'(1) = 1$.

Answer : $a(1)$ is the sum of the coefficients of a, which is 1 (modulo 2) since a has odd weight. The same holds for a'.

11°) Deduce that $aa' \equiv g_S g_{\overline{S}} \mod X^n - 1$.

Answer : This is a direct consequence of the two previous questions.

12°) What is the weight of $aa' \in \mathbb{F}_2[X]/(X^n - 1)$?

Answer : From the previous question, its weight is n since

$$a(X)a'(X) \equiv \frac{X^n - 1}{X - 1} = 1 + X + \cdots + X^{n-1}.$$

13°) Prove that $d^2 - d + 1 \geqslant n$.

Answer : We proved in question 7 that aa' has weight at most $d^2 - d + 1$ when regarded in $\mathbb{F}_2[X]$, thus its weight modulo $X^n - 1$ is bounded from above by $d^2 - d + 1$. From the previous question we deduce that $d^2 - d + 1 \geqslant n$.