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

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

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.

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

A code is said to be *degenerated* if there exist nonempty sets $I, J \subseteq \{1, \dots, n\}$ 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.

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).

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

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

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

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 $c \in C$, $c \cdot P(D) \in C$.

(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.

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

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.

Turn the page please ⟶

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 $x \in A \Rightarrow 2x \in A$).

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

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.

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

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

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.

(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

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

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 $n - 1$.

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

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

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

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

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

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

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