TD 2 - Codes Cycliques

Exercice 1 - Généralités sur les codes cycliques

On se fixe un corps $\mathbb{F}_q$ où q est la puissance d'un nombre premier, et n un entier non nul.

On dit qu'un code $\mathcal{C}$ de longueur n est *cyclique* si toute permutation cyclique d'un mot de code de $\mathcal{C}$ est dans $\mathcal{C}$. De façon équivalente, $\mathcal{C}$ est cyclique si

$$\forall c = (c_0, \ldots, c_{n-1}) \in \mathcal{C}, \sigma(c) = (c_1, \ldots, c_{n-1}, c_0) \in \mathcal{C}$$

où σ est l'opérateur de décalage vers la gauche.

(a) Soit $\mathcal{D}$ le code linéaire de matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Montrer que ce code est cyclique.

Pour toute la suite de l'exercice, on identifie bijectivement les espaces vectoriels $(\mathbb{F}_q)^n$, $\mathbb{F}_q[X]_{<n}$ et $\mathbb{F}_q[X]/(X^n-1)$, en associant à un mot $c = (c_0, \ldots, c_{n-1})$ respectivement le polynôme $c(X) = c_0 + c_1 X + \ldots + c_{n-1}X^{n-1}$ et la classe $\overline{c(X)}$ de ce polynôme (modulo $X^n - 1$).

On appelle $\overline{\mathcal{C}}(X)$ le sous-ensemble de $\mathbb{F}_q[X]/(X^n-1)$ dont les éléments sont les $\overline{c(X)}$ pour $c \in \mathcal{C}$.

(b) Démontrer qu'un code $\mathcal{C}$ est cyclique si et seulement si pour tout $\overline{c}(X) \in \overline{\mathcal{C}}(X)$, $\overline{Xc(X)}$ est dans $\overline{\mathcal{C}}(X)$.

(c) Démontrer qu'un code $\mathcal{C}$ est cyclique si et seulement si $\overline{\mathcal{C}}(X)$ est un idéal de l'anneau $\mathbb{F}_q[X]/(X^n-1)$.

On admet pour la suite de l'exercice que l'anneau $\mathbb{F}_q[X]/(X^n-1)$ est principal.

(d) Pour les 3 sous-questions suivantes, on se fixe un code cyclique $\mathcal{C}$, l'idéal associé $\overline{\mathcal{C}}(X)$ et $\overline{g(X)}$ un polynôme de $\overline{\mathcal{C}}(X)$ de plus petit degré et unitaire. Soit r son degré.

(d.1) Montrer que $\overline{g(X)}$ engendre l'idéal $\overline{\mathcal{C}}(X)$.

(d.2) Montrer que $g(X) \in \mathbb{F}_q[X]_{<n}$ est l'unique polynôme unitaire de degré r tel que $\overline{g(X)} \in \overline{\mathcal{C}}(X)$.

(d.3) Montrer que $g(X)$ divise $X^n - 1$ dans $\mathbb{F}_q[X]$.

(d.4) Montrer que $g(X)$ a un terme constant g_0 non nul.

Exercice 2 - Un exemple de code cyclique

1. Montrer que dans $\mathbb{F}_5[X]$, le polynôme $g = (X^2 - 1)^2$ divise le polynôme $X^{10} - 1$.

   Soit C le code cyclique de longueur 10 sur $\mathbb{F}_5$, engendré par le polynôme g.

2. Quelle est la dimension k de C ? Quel est le nombre de mots de C ?

3. Donner une matrice génératrice de C.

4. Déterminer le polynôme de contrôle de C et donner une matrice de contrôle de C.

5. Montrer que la distance minimum d de C est égale à 3. Quelle est la capacité de correction t de C ?

6. Le mot $\gamma = \big(1111131111\big)$ est reçu.

   (a) (a) Quel est le mot de code c émis ?

   (b) (b) Quel est le message m envoyé, sachant qu'il a été encodé par le polynôme g ?

Exercice 3 - Code de Golay

Le but de cet exercice est l'étude de certains résultats sur le code de Golay binaire $\mathcal{G}_{23}$ et le code de Golay binaire étendu $\mathcal{G}_{24}$.

Commençons par deux petits résultats généraux qui serviront ensuite à déterminer la distance des codes de Golay binaires (c-à-d sur $\mathbb{F}_2$). On se fixe un code binaire C, de paramètres $[n, k, d]$, et G une matrice génératrice de C. On suppose pour toute la suite que les lignes de G sont orthogonales entre elles.

(a) Montrer que C est inclus dans $C^{\perp}$.

On s'intéresse maintenant aux poids des vecteurs d'un tel code.

(b.1) Soient L et K deux lignes de G.
Montrer que $w(L + K) = w(L) + w(K) - 2\#\{i\,;\, L_i = K_i = 1\}$ (où $\#$ désigne le cardinal d'un ensemble et L_i désigne le $i$ème coefficient de L).

(b.2) On suppose que le poids des lignes de G est multiple de 4. Montrer que la somme de deux lignes a un poids multiple de 4.

(b.3) En déduire que, sous la même hypothèse qu'en (b.2), tout élément du code a un poids multiple de 4.

On définit maintenant le code de Golay binaire étendu $\mathcal{G}_{24}$ par sa matrice génératrice $G = (I_{12}\vdots A)$ obtenue en mettant côte à côte deux matrices 12×12 où

$$A = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & B & \\ 1 & & & \end{pmatrix}$$

et B est la matrice circulante de taille 11×11 définie par sa première ligne

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Précisément $B_{i,j}$ vaut 1 lorsque $i+j-2$ est un carré modulo 11 (c-à-d $0, 1, 3, 4, 5, 9$) et vaut 0 sinon.

On admet que les lignes de G sont orthogonales entre elles.

(c.1) Vérifier que le poids des lignes de G est multiple de 4.

(c.2) En déduire que la distance du code est 4 ou 8, et que $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

(c.3) Montrer que $A = {}^{\mathrm{t}}A$.

(c.4) En déduire que $H = (A\vdots I_{12})$ est à la fois une matrice de contrôle et une matrice génératrice de $\mathcal{G}_{24}$.

Il se trouve que la distance minimale du code de Golay étendu est en fait 8.

(c.5) En déduire la capacité de correction du code de Golay étendu.