TD 4

Le but de cet exercice est l'étude d'une famille de codes, dits *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 $c(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1}$ 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.

(e) On s'intéresse dans cette question à l'exemple de code cyclique engendré par le polynôme défini par $g(X) = X + 1$ pour $q = 2$. Soit c dans $\mathbb{F}_2^n$.
(e.1) Montrer que c est dans $\mathcal{C}$ si et seulement si

$$c = (c_0, \ldots, c_{n-2}) \cdot \begin{pmatrix} & & 1 \\ & I_{n-1} & \vdots \\ & & 1 \end{pmatrix}.$$

(e.2) Comment appelle-t-on un tel code ? Quels sont ses paramètres ?

(f) On s'intéresse dans cette question à l'exemple de code cyclique engendré par le polynôme défini par $g(X) = X^3 + X + 1$ pour $q = 2$ et $n = 7$. Le polynôme g étant irréductible, on définit $\mathbb{F}_8$ par $\mathbb{F}_2[X]/(g)$ et il existe donc α dans $\mathbb{F}_8$ vérifiant $g(\alpha) = 0$.
Soit c dans $\mathbb{F}_2^n$.
(f.1) Vérifier que $X^3 + X + 1 = (X - \alpha)(X - \alpha^2)(X - \alpha^4)$.
(f.2) En déduire l'équivalence

$$c \in \mathcal{C} \iff c(\alpha) = 0.$$

(f.3) Montrer que $c(\alpha) = 0$ est équivalent à

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_6 \end{pmatrix} = 0.$$

(f.4) Comment appelle-t-on un tel code ? Quels sont ses paramètres ?

Soit $\mathcal{C}$ un code cyclique de longueur n sur $\mathbb{F}_q$, de polynôme générateur $g(X) = g_0 + g_1 X + \dots g_r X^r$ de degré r. On note $k = n - r$.

(g) Montrer que les mots associés $g(X), Xg(X), X^2 g(X), \dots, X^{k-1} g(X)$ sont des mots de $\mathcal{C}$ et en forment une base. En déduire une matrice génératrice du code.

On appelle polynôme de contrôle le polynôme $h(X) \in \mathbb{F}_q[X]$ défini par la relation $h(X)g(X) = X^n - 1$.
Soit $c \in \mathcal{C}$.
(h.1) Montrer que $c(X)h(X)$ est de degré maximal $n + k - 1$ et est un multiple de $X^n - 1$.
(h.2) Ecrire les coefficients de $c(X)h(X)$ en fonction de ceux de $c(X)$ et de $h(X)$, puis montrer la relation $H \cdot {}^t c = 0$, où

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & \dots & 0 & 0 & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & \dots & 0 & 0 \\ 0 & 0 & h_k & h_{k-1} & \dots & h_0 & \dots & 0 \\ & & & & & & & \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \end{pmatrix}.$$

(h.3) Montrer que H est bien une matrice de contrôle pour le code $\mathcal{C}$.
(h.4) Montrer que le code dual de $\mathcal{C}$ est cyclique et donner son polynôme générateur.

On appelle *burst* de longueur ℓ un mot de $\mathbb{F}_2^n$ dont les composantes non nulles sont concentrées dans ℓ positions consécutives. Par exemple, $e = (00110101000000)$ est un burst de longueur 6.
(i) Montrer qu'un code cyclique peut détecter les erreurs qui sont de type burst et dont la longueur est inférieure ou égale au degré de g.