Université Pierre et Marie Curie LICENCE A Année 2005-2006

Devoir 4

Exercice 1. ***Codes linéaires cycliques*** *Un code linéaire cyclique est un code $\mathcal{C}$ linéaire de longueur n, stable par la permutation $T(a_1, \cdots, a_n) = (a_n, a_1, \cdots, a_{n-1})$.*

(1) En utilisant l'isomorphisme naturel d'espace vectoriel $\psi : \mathbb{F}_q^n \simeq \mathbb{F}_q[X]/Q(X)$ où $Q = X^n - 1$, montrer que $\mathcal{C} \subset \mathbb{F}_q^n$ est stable par T si et seulement si son image par ψ est un idéal. En déduire alors qu'il existe une bijection entre les codes cycliques de longueur n et les polynômes unitaires divisant $X^n - 1$.

(2) Rappeler la factorisation en irréductibles des polynômes cyclotomiques Φ_n dans $\mathbb{F}_q$, et en déduire une bijection entre les codes cycliques de longueur n et les parties $I \subset (\mathbb{Z}/n\mathbb{Z})^\times$ stables par la multiplication par q.

(3) Soit C un code linéaire cyclique de longueur n sur $\mathbb{F}_q$ associé à $I \subset (\mathbb{Z}/n\mathbb{Z})^\times$ et supposons qu'il existe i et s tels que $\{i+1, i+2, \cdots, i+s\} \subset I$. Montrer alors que $d(\mathcal{C}) \geq s+1$.

*(4) **Codes de Hamming**: soit $n = \frac{q^r-1}{q-1}$ et $I := \{1, q, q^2, \cdots, q^{r-1}\}$. Montrer que $d(\mathcal{C}) = 3$ ou 4 et qu'il est parfait 1-correcteur.*

Remarque: Pour $r = 3$, $q = 2$ et $n = 7$ on retrouve le code étudié précédemment.

En construisant une matrice vérificatrice montrer qu'en fait on a $d(\mathcal{C}) = 3$.

*(5) **Codes de Reed-Solomon**: ce code est utilisé dans les CD. Soit $n = q - 1$ et soit α un générateur de $\mathbb{F}_q^\times$. Pour k fixé on pose*

$$g(X) := \prod_{i=1}^{q-1-k} (X - \alpha^i)$$

Montrer que le code linéaire cyclique correspondant est MDS et que pour $q = 2^f$, on a $2t+1 \leq d(\mathcal{C}) = q - k$.

*(6) **Code ternaire de Golay**: on a $3^5 - 1 = 11.23$; on choisit $q = 3$, $n = 11$ et la partie de$(\mathbb{Z}/11\mathbb{Z})^\times$ engendrée par 3, i.e. $i = \{1, 3, 4, 5, 9\}$. On note $\mathcal{G}_{11}$ le code linéaire cyclique correspondant. Montrer que $d(\mathcal{G}_{11}) = 4, 5$ puis que $\mathcal{G}_{11}$ est 2-correcteur parfait (il n'est pas MDS).*

*(7) **Code binaire de Golay**: on a $2^{11} - 1 = 23.89$, on choisit $q = 2$, $n = 23$ et $I = (2) \subset (\mathbb{Z}/23\mathbb{Z})^\times$. On note $\mathcal{G}_{23}$ le code linéaire cyclique correspondant. Montrer que $d(\mathcal{G}_{2^n}) = 5, 6, 7$ puis que $\mathcal{G}_{23}$ est "-correcteur parfait.*

Preuve : (1) Dans $\mathbb{F}_q[X]/(Q)$, l'endomorphisme T a pour polynôme minimal $Q = X^n - 1$ de sorte que via $\psi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[X]/(X^n - 1)$ défini par $\psi(a_0, \cdots, a_{n-1}))a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} \mod (X^n - 1)$, on a

$$\psi \circ T(a_0, \cdots, a_{n-1}))X(a_0 + \cdots, a_{n-1}X^{n-1}) \mod (X^n - 1)$$

Ainsi $\mathcal{C}$ est stable par T si et seulement si son image par ψ est stable par la multiplication par X, i.e. est un idéal de $\mathbb{F}_q[X]/(X^n - 1)$. On conclut en notant que les idéaux de $\mathbb{F}_q[X]/(X^n - 1)$ correspondent aux idéaux de $\mathbb{F}_q[X]$ cotenant $X^n - 1$ et donc de la forme $P\mathbb{F}_q[X]$ avec P divisant $X^n - 1$.

(2) On rappelle que la décomposition en facteurs irréductibles du n-ième polynôme cyclotomique $\Phi_n(X)$ dans $\mathbb{F}_q[X]$ avec $q = p^f$ s'écrit comme suit:

- si $n = p^s m$ avec $p \wedge m = 1$ alors $\Phi_n(X) = \Phi_m(X)^{p^s - p^{s-1}}$;
- si $n \wedge p = 1$, soit r l'ordre de q modulo n dans $(\mathbb{Z}/n\mathbb{Z})^\times$; alors Φ_n se décompose en le produit de $\psi(n)/r$ facteurs irréductibles de degré r.

Les diviseurs P de $X^n - 1$ sont en bijection avec les parties $I \subset (\mathbb{Z}/n\mathbb{Z})^\times$ stable par la multiplication par q: en effet P est un produit de facteurs irréductibles, chacun étant associé à l'orbite d'une racine primitive n-ième de l'unité sous l'action du Frobenius, i.e. à l'orbite d'un élément $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ sous l'action de la multiplication par q.

(3) Soit ξ une racine primitive n-ième dans une extension de $\mathbb{F}_q$. Soit Q un polynôme modulo $X^n - 1$, il appartient à $\mathcal{C}$ si et seulement si $Q(\xi^{i+j}) = 0$ pour $j = 1, \cdots, s$. Supposons que le poids ω de$Q$ soit inférieur ou

égal à s, i.e. $Q = a_1 X^{i_1} + \cdots + a_\omega X^{i_\omega}$ avec disons $0 \leq a_1 < a_2 < \cdots < a_\omega < n$. Il faut montrer qu'en fait Q doit être nul. On dispose des équations

$$a_1 \xi^{i_1(i+j)} + \cdots + a_\omega \xi^{i_\omega(i+j)} = 0$$

pour $j = 1, \cdots, s$. Posons $a'_1 = a_1 \xi^{i_\omega i}$, les équations se réécrivent:

$$\xi^{i_1 j} a'_1 + \cdots + \xi^{i_\omega j} a'_\omega = 0, \qquad \textit{pour } j = 1, \cdots, s.$$

Mais la matrice des $\xi^{i_r j}$ est extraite d'une matrice de Vandermonde avec $\xi^{i_r} \neq \xi^{i_{r'}}$, puisque ξ est d'ordre n; elle est donc de rang $\min\{\omega, s\}$ ce qui impose $a'_1 =) \cdots = a'_\omega = 0$ et donc $a_1 = \cdots = a_\omega = 0$.

(4) Montrons tout d'abord que $d(\mathcal{C}) \geq 3$: en effet un polynôme de poids 2 s'écrit $P = aX^i + bX^j$ avec disons $0 \leq i < j \leq n-1$ et la condition qu'il s'annule en ξ^{q^l} pour $0 \leq l \leq r-1$ s'écrit donc $a + b\xi^{j-i)q^l} = 0$ et comme ξ est d'ordre n, on voit que ceci est impossible sauf si $a = b = 0$. Ainsi le code est 1-correcteur et comme $\mathrm{card} B(x,1) = 1 + n(q-1) = q^r$, on voit que $\mathcal{C}$ est parfait 1-correcteur et ainsi $d(\mathcal{C}) = 3$ ou 4.

Choisissons des représentants $e_1, \cdots, e_n$ des vecteurs non nuls de $\mathbb{F}_q^r$ à colinéarité près: $n = (q^r - 1)/(q-1)$. Notons A la matrice dont les colonnes sont les vecteurs e_i et appelons L_i ses lignes. Alors A est la matrice vérificatrice du code

$$\mathcal{C} := \{x \in \mathbb{F}_q^n \ / \ < L_i, x >= 0, \text{ pour } 1 \leq i \leq r\}.$$

Ce code est isomorphe au code de Hamming: comme deux vecteurs e_i distincts ne sont jamais liés par construction mais qu'il existe bien sûr des triplets linéairement indépendants, on vérifie bien que $d(\mathcal{C}) = 3$.

(5) On a $\dim \mathcal{C} = k$ et comme $I = \{1, 2, \cdots, q-1-k\}$, on a $d(\mathcal{C}) \geq q - k$. Or comme pour tout code linéaire on a $d(\mathcal{C}) \leq n + 1 - k$, on a donc $d(\mathcal{C}) = q - k$ et le code est MDS.
Remarque: Supposons $q = 2^f$, on peut voir $\mathcal{C}$ comme un code binaire $\mathcal{C}'$ de paramètre $n' = (2^f - 1)f$, $k' = kf$ et distance $d(\mathcal{C}') \geq 2^f - k$. Une particularité de ce code est de corriger de large bouffées d'erreurs si celles-ci se répartissent par parquets! Cette particularité explique pourquoi ce type de code est utilisé dans la technologie des CD.

(6) D'après le théorème sur la distance d'un code cyclique, on voit que $d(\mathcal{G}_{11}) \geq 4$ et en considérant la factorisation de Φ_{11} dans $\mathbb{F}_3[X]$, on voit que $\mathcal{G}_{11}$ contient un polynôme de poids 5 et donc $d(\mathcal{G}_{11}) \leq 5$.
Remarque: On peut montrer que $d(\mathcal{G}_{11}) = 5$.

Ainsi $\mathcal{G}_{11}$ est 2-correcteur et comme $\mathrm{card} B(x,2) = 1 + 2C_{11}^1 + 2^2 C_{11}^2 = 3^5$, on voit que le code est 2-correcteur parfait, mais il n'est pas MDS.

(7) D'après le théorème sur la distance d'un code cyclique, on voit que $d(\mathcal{G}_{23}) \geq 5$ et en considérant la factorisation de Φ_{23} dans $\mathbb{F}_2[X]$, on voit que $\mathcal{G}_{23}$ contient un polynôme de poids 7 et donc $d(\mathcal{G}_{11}) \leq 7$.
Remarque: On peut montrer que $d(\mathcal{G}_{23}) = 7$.

Ainsi $\mathcal{G}_{23}$ est 3-correcteur et comme $\mathrm{card} B(x,3) = 1 + 2C_{23}^1 + C_{23}^2 + C_{23}^3 = 2^{11}$, on voit que le code est 3-correcteur parfait, mais il n'est pas MDS.