TD n^o 4 - Codes cycliques

Solutions

Exercice 1 – Traité en TD.

Exercice 2 – C code cyclique dans $\mathbb{K} = \mathbb{F}_5[X]/(X^{10}-1)$ engendré par le polynôme g.

1. En effectuant la division euclidienne de $X^{10}-1$ par g dans $\mathbb{F}_5[X]$ on obtient :
$$X^{10} - 1 = g(X)(X^6 + 3X^4 + 2X^2 + 4).$$
2. Le code C a dimension $k = n - \deg(g) = 10 - 4 = 6$ et $M = |\mathbb{F}_5|^k = 5^6$ mots.
3. La premiere colonne de G correspond aux coefficients du polynôme g : $g_0 = 1, g_1 = 0, g_2 = 3, g_3 = 0, g^4 = 1$ suivis des zéros. Les colonnes suivantes sont obtenues en applicant un décalage sur la colonne précédente.
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 & 0 \\ 1 & 0 & 3 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 & 0 & 1 \\ 0 & 0 & 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
4. Le polynôme de contôle h de C est tel que $h(X)g(X) = X^{10} - 1$. On l'a calculé lors de la première question $h(X) = X^6 + 3X^4 + 2X^2 + 4$.

   La matrice de contôle H a sur la premiere ligne les coefficients du polynôme h : $h_6 = 1, h_5 = 0, h_4 = 3, h_3 = 0, h_2 = 2, h_1 = 0, h_0 = 4$, suivis des zéros. Ensuite on décale ces valeurs sur les lignes suivantes :
$$H = \begin{pmatrix} 1 & 0 & 3 & 0 & 2 & 0 & 4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 & 2 & 0 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 & 0 & 2 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 & 0 & 3 & 0 & 2 & 0 & 4 \end{pmatrix}$$
5. Toute colonne de H est non-nulle, donc $d > 1$. Deux colonnes de H qui comportent une seule valeur non-nulle sont distinctes et celles qui ont deux valeurs non-nulles sur les mêmes positions ne sont pas proportionnelles, donc $d > 2$. On trouve la dépéndence : $2C_1 - C_5 - C_7 = 0$, donc $d = 3$ et la capacité de correction est $t = 1$.

6. a) On calcule le syndrome $S(\gamma) = H \cdot \gamma = \begin{pmatrix} 4 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 2 \cdot C_5$.

On a que $S(\gamma) = S(2\varepsilon_5)$ où $\varepsilon_5 = (0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0)^\top$.
La capacité de correction etant $t = 1$, $S(\gamma) = S(2\varepsilon_5)$ et $wt(2\varepsilon_5) \leq 1$, alors $c = \gamma - 2\varepsilon_5$ est l'unique élément de C à distance ≤ 1 de γ.

$$c = (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)^\top.$$

b) On sait que $c(X) = m(X)g(X)$, donc $m(X)$ est le quotient de la division de $c(X)$ par $g(X)$ où :

$$c(X) = X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X^2 + X + 1.$$

Exercice 3 – C code linéaire sur $\mathbb{F}_7$ de matrice génératrice $G = \begin{pmatrix} 1 & 0 \\ 5 & 1 \\ 5 & 5 \\ 2 & 5 \\ 1 & 2 \\ 0 & 1 \end{pmatrix}$.

1. Le code C a longueur $n = 6$, dimension $k = 2$ et $M = |\mathbb{F}_7|^k = 7^2$ mots.
2. La matrice G nous permet de déduire le polynôme unitaire $g(X) \in \mathbb{F}_7[X]/(X^6 - 1)$ de degré $n - k = 4$ tel que tout $c(x) \in C_x$ peut s'écrire $c(x) = g(x)m(x)$ dans $\mathbb{K}[x] = \mathbb{F}_7[X]/(X^6 - 1)$.
   On pourra écrire une formule pour $c(x) = g(x)m(x)$ en utilisant les notations matricielles.
   (Voir Lemme 4.1.3 du cours pour la multiplication des polynômes dans l'anneau quotient $\mathbb{K}[x]$ en tenant compte que $x^n = 1$.)

   — Le polynôme générateur $g(X) = X^4 + 2X^3 + 5X^2 + 5X + 1$.
   — Le polynôme de contôle $h(X) = (X^6 - 1)/g(X) = X^2 + 5X + 6$.
3. $$H = \begin{pmatrix} 1 & 5 & 6 & 0 & 0 & 0 \\ 0 & 1 & 5 & 6 & 0 & 0 \\ 0 & 0 & 1 & 5 & 6 & 0 \\ 0 & 0 & 0 & 1 & 5 & 6 \end{pmatrix}$$
4. On cherche les éléments α de $\mathbb{F}_7$ pour lesquels $\mathbb{F}_7 = \{1, \alpha, \alpha^2 \dots \alpha^5\}$.
   On trouve $\alpha \in \{3, 5\}$.
   On vérifie que $g(X)$ a comme racines $1,\ \alpha = 3,\ \alpha^2 = 2,\ \alpha^3 = -1$.
   Cela nous donne une décomposition en facteurs pour g :

α	α^2	α^3	α^4	α^5	α^6
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

$$g(X) = (X-1)(X-\alpha)(X-\alpha^2)(X-\alpha^3).$$

Le code C est donc un code **Reed-Solomon** $RS(7,2)$ de longueur $q-1 = 7-1 = 6$, de dimension $k = 2$ et de polynôme générateur g de degré $\deg(g) = q-1-k = 4$.

Des résultats du cours nous donnent les paramètres du code $RS(7,2)$:
— La distance minimum $d = q - k = 5$.
— La capacité de correction $t = 2$.

5. a) On calcule le syndrome $S(\gamma) = H \times \gamma$.

Exercice 4 –

1. D'après la table on remarque que $-1 = 1$, donc on cherche les racines de $X^7 + 1$ parmi les éléments de $\mathbb{K}$ qui satisfont $X^7 = -1 = 1$. Dans le groupe multiplicatif $\mathbb{K}^*$ d'ordre $8 - 1 = 7$, d'après le théorème de Lagrange on a $\forall a \in \mathbb{K}^*\ a^7 = 1$.
   Donc les 7 racines de $X^7 + 1$ sont les éléments de $\mathbb{K}^*$.
2. $g = X^2 + (1+2)X + 1 \times 2 = X^2 + 3X + 2.$

$$\begin{aligned} h &= (X+3)(X+4)(X+5)(X+6)(X+7) \\ &= \big(X^2 + (3+4)X + 3\times 4\big)\big(X^2 + (5+6)X + 5\times 6\big)(X+7) \\ &= \big(X^2 + 7X + 7\big)\big(X^2 + 3X + 3\big)(X+7) \\ &= \big(X^4 + (3+7)X^3 + (3+7+3\times 7)X^2 + (3\times 7 + 3\times 7)X + 3\times 7\big)(X+7) \\ &= (X^4 + 4X^3 + 6X^2 + 2)(X+7) \\ &= X^5 + (4+7)X^4 + (6+4\times 7)X^3 + 6\times 7X^2 + 2X + 2\times 7 \\ &= X^5 + 3X^4 + 7X^3 + 4X^2 + 2X + 5 \end{aligned}$$

3. Le code C est donc un code *Reed-Solomon* $RS(8,4)$ de paramètres :
   — La longueur $n = q - 1 = |\mathbb{K}| - 1 = 7$,
   — La dimension $k = n - \deg(g) = 5$,
   — La distance minimum $d = q - k = 3$,
   — La capacité de correction $t = 1$.

   La matrice génératrice associée au polynôme générateur g :

$$G = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 3 & 2 & 0 & 0 & 0 \\ 1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

   La matrice de contôle associée au polynôme de contôle h :

$$H = \begin{pmatrix} 1 & 3 & 7 & 4 & 2 & 5 & 0 \\ 0 & 1 & 3 & 7 & 4 & 2 & 5 \end{pmatrix}$$

4. $c = G \times m$.