Université de Bordeaux

Master 1 CSI
4TCY703U - Arithmétique
Feuille 7

Exercice 1. Soient K un corps fini, C_1 et C_2 deux codes cycliques de longueur n sur K de polynômes générateurs respectifs $P_1(X)$ et $P_2(X)$. Vérifier que le code $C_1 + C_2$ est cyclique et exprimer son polynôme générateur en fonction de $P_1(X)$ et $P_2(X)$.

Exercice 2. On pose $K = \mathbf{F}_2[Y]/\langle Y^4 + Y + 1\rangle$ et on note α la classe de Y dans K. On sait que K est un corps. On désigne par C le code cyclique de longueur 15 engendré par le polynôme $P(Y) = Y^4 + Y + 1$.
(1) Montrer que C est un code de Hamming. Quels sont ses paramètres ?
(2) Trouver une matrice de contrôle de C.
(3) Déterminer le polynôme minimal $Q(Y)$ de α^3 sur $\mathbf{F}_2$.
(4) Notons C' le code cyclique de longueur 15 engendré par $P(Y)Q(Y)$. L'ordre de la condition de décodage de C' est-il meilleur que celui de C ?

Exercice 3. On note $(u_n)_{n\geqslant 0}$ la suite d'éléments de $\mathbf{F}_2$ définie par $u_0 = u_1 = u_2 = u_3 = 0$, $u_4 = 1$, et $u_{n+5} = u_{n+2} + u_n$ pour tout $n \in \mathbf{N}$.
(1) Déterminer la période de la suite $(u_n)_{n\geqslant 0}$.
(2) Le polynôme $P(X) = X^5 + X^2 + 1$ est-il irréductible dans $\mathbf{F}_2[X]$?
(3) Posons $K = \mathbf{F}_2[X]/\langle P(X)\rangle$ et désignons par α la classe de X dans K. Calculer $\mathsf{Tr}(\alpha^n)$ pour tout $n \in \{0, 1, 2, 3, 4\}$.
(4) Trouver l'élément $b \in K$ tel que $u_n = \mathsf{Tr}(b\alpha^n)$ pour tout $n \in \mathbf{N}$.

Exercice 4. Posons $K = \mathbf{F}_2[X]/\langle X^4 + X^3 + X^2 + X + 1\rangle$ et notons a la classe de X dans K. On sait que K est un corps. On désigne par C le code linéaire de matrice génératrice

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & a & a^2 & a^3 & a^4 \\ 1 & a^2 & a^4 & a & a^3 \end{bmatrix}$$

(1) Prouver que C est un code cyclique.
(2) Montrer que C est un code de Reed-Solomon. Quels sont ses paramètres ?
(3) Déterminer le polynôme générateur du dual de C.
(4) En déduire le polynôme générateur de C.

Exercice 5. On note C le code $\mathbf{F}_5$-linéaire de matrice génératrice

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{bmatrix}$$

(1) Vérifier que C est un code de Reed-Solomon. Quelle est sa distance minimale ?
(2) Posons $r = (4, 2, 0, 0)$. Trouver le mot de C le plus proche de r.