Master CSI 1 — 2006-2007

Arithmétique 1

Feuille d'exercices n° 7.

$\boxed{1}$ Soit C le code de Reed-Solomon de dimension 2 sur $\mathbb{F}_4$. Soit α, avec $\alpha^2+\alpha+1$ tel que $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$.

1. Soit $y = (0, 0, \alpha^2, \alpha) \in \mathbb{F}_4^4$. Trouvez le mot de C le plus proche de y par l'algorithme des fractions continues. Quelle est la distance de y à C ?
2. En calculant card$(\cup_{x\in C} B(x,1)$, montrez que $\cup_{x\in C} B(x,1)$ n'est pas égal à $\mathbb{F}_4^4$ tout entier.
3. Trouvez explicitement un élément $z \in \mathbb{F}_4^4$ tel que $z \notin \cup_{x\in C} B(x,1)$ (indication : on pourra le chercher avec $z_1 = 0$).
4. Calculez $d(z, C)$ et $\{x \in C : d(z,x) = d(z,C)$.
5. Que se passe-t-il si on applique l'algorithme de décodage par fractions continues à z ?

$\boxed{2}$ Soit C un code BCH binaire de longueur 15 et de distance minimale construite 5. On pose $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ avec $\alpha^4+\alpha+1 = 0$.

1. Déterminez un polynôme générateur de C et montrez que C a pour paramètres $[15, 7, 5]$.
2. Déterminez une matrice H de taille 2×15 à coefficients dans $\mathbb{F}_4$ telle que
$$x \in C \iff Hx^t = 0.$$
3. Notre but est de décoder le mot binaire y dont le syndrome par rapport à la matrice H est
$$s = \begin{pmatrix} 1+\alpha^2+\alpha^3 \\ 1+\alpha \end{pmatrix}.$$
   (a) Si i et j sont les indices des erreurs, montrez que s permet de calculer $S = \alpha^i + \alpha^j$ et $P = \alpha^i\alpha^j$. Et faites-le.. En déduire un polynôme de degré 2 dont les racines sont α^i et α^j.

   (b) Écrire la matrice de l'application linéaire sur $\mathbb{F}_2$:
$$\begin{aligned} \mathbb{F}_{16} &\to \mathbb{F}_{16} \\ x &\mapsto x^2 \end{aligned}$$
   dans la base $(1, \alpha, \alpha^2, \alpha^3)$. En déduire par un calcul matriciel les racines du polynôme défini ci-dessus.

   (c) Conclure.
4. Montrez qu'en remplaçant chaque coefficient de H par le vecteur colonne des coordonnées de ce coefficient sur $(1, \alpha, \alpha^2, \alpha^3)$, on trouve une matrice de contrôle de parité de C. Vérifiez.