Master CSI 1

Arithmétique 1

Feuille d'exercices n° 6.

1 Soit $F = \mathbb{F}_{2^L}$. On note $\sigma(x) = x^2$ le Frobenius. On pose, pour tout $a \in F$,

$$\mathrm{Tr}(a) = a + a^2 + a^4 + \cdots + a^{2^{L-1}} = a + \sigma(a) + \cdots + \sigma^{L-1}(a).$$

Soit $f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_L x^L$ un polynôme de $\mathbb{F}_2[x]$ de degré L que l'on suppose irréductible. On fixe une racine α de f dans F. On a donc $F = \mathbb{F}_2[\alpha]$.

On rappelle que l'on dit que f engendre la suite $s = (s_0, s_1, \dots)$ si pour tout $j \geq L$, on a :

$$s_j = \sum_{i=1}^{L} c_i s_{j-i} = c_1 s_{j-1} + c_2 s_{j-2} + \cdots + c_L s_{j-L}.$$

1. (a) Montrez que, si $\mathrm{Tr}(b) = 0$, alors b est racine d'un polynôme de degré 2^{L-1}. En déduire qu'il existe $b \in F$ tel que $\mathrm{Tr}(b) \neq 0$.
   (b) Montrez que, si $\mathrm{Tr}(au) = 0$ pour tout $u \in F$, alors $a = 0$.
2. (a) Montrez que, pour tout $\beta \in F$, la suite définie par $s_j = \mathrm{Tr}(\beta\alpha^{-j})$ pour $j \geq 0$ est engendrée par f.
   (b) En déduire que l'application de F dans l'espace vectoriel des suites engendrées par f qui à β associe la suite $s = s(\beta)$ définie par $s_j = \mathrm{Tr}(\beta\alpha^{-j})$ pour $j \geq 0$ est un isomorphisme d'espaces vectoriels.
   (c) Pour tout entier t, on note $s^{(t)}$ la suite définie par

$$(s^{(t)})_j = s_{tj}.$$

   i. Exemple : $f(x) = x^4 + x^3 + 1$. On sait que f est irréductible sur $\mathbb{F}_2$ et que ses racines engendrent $\mathbb{F}_{16}^*$. Soit $s = 100010011010111\ldots$.
   Quels sont les bits suivants de s ? Calculez le début de $s^{(2)}$, $s^{(3)}$, $s^{(5)}$, et le plus petit polynôme qui les engendre.
   ii. Retour au cas général : montrez que la suite $s^{(t)}$ est engendrée par le polynôme minimal de α^t sur $\mathbb{F}_2$.
   iii. Vérifiez sur l'exemple précédent.
   iv. Toujours l'exemple : d'après ce qui précède, si α est une racine de f, il existe $\beta \in F$ tel que $s = s(\beta)$. Calculez β.

2 Tous les codes de cet exercice sont cycliques, de longueur n sur $\mathbb{F}_q$.

1. Montrez que le code cyclique engendré par $1 + X + X^2 + \cdots + X^{n-1}$ est le code $C = \{(a, \dots, a) : a \in \mathbb{F}_q\}$. Quelle est sa dimension ?
2. Montrez que le code cyclique engendré par $X - 1$ est le code $C = \{(x_1, \dots, x_n) \in \mathbb{F}_q^n : \sum_{i=1}^n x_i = 0\}$. Quelle est sa dimension ?
3. Montrez que, si C_i est engendré par f_i avec f_i diviseur de $X^n - 1$, alors :
   (a) $C_1 \subset C_2 \iff f_2$ divise f_1
   (b) $C_1 + C_2$ est engendré par $\gcd(f_1, f_2)$
   (c) $C_1 \cap C_2$ est engendré par (f_1, f_2)