Codes correcteurs

Cours Bachelor HEIG-VD

Semestre printemps 2023

Laboratoire 3 : Codes cycliques

Le but de ce laboratoire est d'étudier l'algorithme d'Euclide appliqué à des polynômes, les règles de calcul dans un corps fini et les codes cycliques et en particulier les codes BCH et Reed-Solomon.

Problème 1
Soient $a(x)$ et $b(x)$ deux polynômes dans $\mathbb{F}_q[x]$. L'algorithme d'Euclide étendu permet non seulement d'obtenir le pgdc($a(x)$, $b(x)$), mais aussi de fournir les polynômes $u_i(x)$ et $v_i(x)$ tels que $r_i(x) = a(x)\,u_i(x) + b(x)\,v_i(x)$ (voir la section 7.10 du polycopié). En utilisant les mêmes notations de la section7.10 (pages 46-47) du polycopié et étant donné deux polynômes $a(x) = x^8$ et $b(x) = x^6 + x^4 + x^2 + x + 1$ dans $\mathbb{F}_2[x]$, écrire un programme qui permet de

1) calculer les polynômes $u_i(x)$, $v_i(x)$, , $r_i(x)$ et $q_i(x)$ pour $-1 \leq i \leq n$,
2) donner le pgdc($a(x)$, $b(x)$),
3) vérifier les formules $r_i(x) = a(x)\,u_i(x) + b(x)\,v_i(x)$ pour $-1 \leq i \leq n$

Problème 2
Écrire un programme qui permet de trouver la représentation exponentielle, polynomiale et vectorielle du corps fini $\mathbb{F}_{2^5}$ défini à partir du polynôme primitif $m(x) = x^5 + x^2 + 1$ et de donner le polynôme minimal de chaque élément de $\mathbb{F}_{2^5}$.

Problème 3
Construire le polynôme générateur $g(x)$ d'un code BCH de longueur 63, qui corrige toutes les erreurs de poids inférieur ou égal à 3 en utilisant la représentation de $\mathbb{F}_{2^6}$ défini à partir du polynôme primitif $m(x) = x^6 + x + 1$.
Écrire le polynôme générateur $g(x)$ sous forme

$$g(x) = \sum_{i=0}^{r} P_i(\alpha)\, x^i$$

où r est le degré du polynôme $g(x)$, $P_i(x)$ est un polynôme dans $\mathbb{F}_2[x]$ de degré inférieur ou égal à 5 et où $\alpha \equiv \bar{x}$ modulo le polynôme $m(x)$.

Problème 4
Pour construire un code de Reed-Solomon $\mathcal{C}$ sur le corps $\mathbb{F}_q$ il est commode, en pratique de prendre q de la forme $q = 2^m$. Les éléments de $\mathbb{F}_{2^m}$ sont des suites de m bits. Si on ramène tout à $\mathbb{F}_2$ on peut voir alors $\mathcal{C}$ comme un code binaire $\mathcal{C}'$, de longueur $n' = (2^m - 1)m$, de dimension $k' = k\,m$ et de distance minimale $d' \geq d = 2^m - k$ (car cette opération augmente les poids des mots du code $\mathcal{C}$).
Le code $\mathcal{C}'$ est bien adapté aux corrections faites par paquets : si t vérifie $2t + 1 \leq d(\mathcal{C}) = q - k$, le code corrige t éléments de $\mathbb{F}_{2^m}$, donc $t\,m$ erreurs binaires si celles-ci sont consécutives.

Le satellite d'exploration de Jupiter Galileo utilise le code de Reed-Solomon (255,223) sur le corps $\mathbb{F}_{2^8}$(corps des octets) où ce corps est construit modulo le polynôme primitif
$m(x) = x^8 + x^7 + x^2 + x + 1$ de $\mathbb{F}_2[x]$

a) Calculer la distance minimale et la capacité de correction de ce code.

b) Le polynôme générateur choisi est $g(x) = \prod_{j=12}^{43} (x - (\alpha^{11})^j)$ et où $\alpha \equiv \bar{x}$ modulo le polynôme $m(x)$.
Écrire un programme fournissant $g(x)$ sous la forme

$$g(x) = \sum_{i=0}^{32} P_i(\alpha)\, x^i$$

avec $P_i(x) \in \mathbb{F}_2[x]$ et de degré inférieur ou égal à 7.

Ce code de $(\mathbb{F}_{256})^{255}$ est alors 16-correcteur ; via ce que nous avons dit est un code linéaire sur $(\mathbb{F}_2)^{2040}$, de dimension 1784 qui peut corriger au moins 128 erreurs portant sur les bits dès qu'elles sont consécutives (erreurs par paquets).