TP Maple Option Calcul Formel Agrégation
Codes correcteurs

15 janvier 2013

1 Codes de Reed-Solomon/BCH

1. Soit $\alpha \in \mathbb{F}_{2^6}$ défini par $\alpha^6 + \alpha + 1 = 0$. A l'aide de Maple vérifier que α engendre $(\mathbb{F}_{2^6})^*$.
   Pour la suite, on pourra définir α à l'aide de la commande RootOf :

   ```
   alias(alpha=RootOf(x^6+x+1));
   ```

   Afin d'écrire les éléments de $\mathbb{F}_{2^6}$ dans la base $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$, utiliser la commande `Normal` :

   ```
   Normal(alpha^8) mod 2;
   ```

2. Déterminer les polynômes minimaux sur $\mathbb{F}_2$ de α^3, α^5, α^7 et α^9.
3. Soit $H = (H_{i,j})_{1\leq i\leq 10, 1\leq j\leq 63} \in M_{10,63}(\mathbb{F}_{2^6})$ telle que pour tout $i \in \{1, \ldots, 10\}, j \in \{1, \ldots, 63\}$,

   $$H_{i,j} = \alpha^{i(j-1)}.$$

   Soit C le code de longueur 63 défini sur $\mathbb{F}_{2^6}$ par

   $$C = \{c \in (\mathbb{F}_{2^6})^{63}, H \cdot^t c = 0\}.$$

   Montrer que C est un code $[63, 53, 11]$ cyclique dont on déterminera le polynôme générateur.
   En déduire une matrice génératrice G pour C et vérifier à l'aide de Maple que $H \cdot^t G = 0$.
4. Soit $\mathcal{C}$ le code binaire défini par $\mathcal{C} = C \cap \mathbb{F}_2^{63}$. Construire une matrice de contrôle de $\mathcal{C}$ (matrice génératrice du dual de $\mathcal{C}$) et le polynôme générateur de $\mathcal{C}$. Que dire de la distance minimale de $\mathcal{C}$?
5. Soit $c \in C$. Soit $v \in (\mathbb{F}_{2^6})^{63}$ tel que

   $$v(X) - c(X) = \sum_{i=1}^{r} Y_i X^{e_i}$$

   avec $1 \leq r \leq 5$ et $Y_i \neq 0$.
   On note $X_i = \alpha^{e_i}$ pour $1 \leq i \leq r$.
   Soit $S = H \cdot^t v$ et notons $S_1, \ldots, S_{10}$ les coordonnées de S.
   (a) Montrer que

   $$\left\{\begin{array}{lcl} S_1 & = & Y_1X_1 + \cdots + Y_rX_r \\ S_2 & = & Y_1X_1^2 + \cdots + Y_rX_r^2 \\ \vdots & & \\ S_{10} & = & Y_1X_1^{10} + \cdots + Y_rX_r^{10} \end{array}\right. \tag{1}$$

   où $X_i = \alpha^{e_i}$ pour i entre 1 et r.

(b) Déterminer c connaissant v revient à déterminer les X_i et Y_i connaissant S. L'objectif de ce qui suit est d'éviter de résoudre le système polynomial (1) directement. Pour cela, on va se ramener à la résolution de systèmes linéaires. On peut aussi utiliser une autre méthode basée sur l'algorithme d'Euclide (voir texte plus tard).

On définit le *polynôme localisateur d'erreurs* $\sigma(z)$ par

$$\sigma(z) = \prod_{j=1}^{r}(1 - X_j\, z) = 1 + \sum_{i=1}^{r} s_i z^i \in \mathbb{F}_{2^6}[z] \tag{2}$$

Montrer que

$$\underbrace{\begin{pmatrix} S_1 & S_2 & S_3 & \cdots & S_r \\ S_2 & S_3 & S_4 & \cdots & S_{r+1} \\ S_3 & S_4 & S_5 & \cdots & S_{r+2} \\ & & & & \\ S_r & S_{r+1} & S_7 & \cdots & S_{2r-1} \end{pmatrix}}_{\mathcal{S}} \begin{pmatrix} s_r \\ \vdots \\ \\ s_2 \\ s_1 \end{pmatrix} = \begin{pmatrix} -S_{r+1} \\ -S_{r+2} \\ \\ \\ -S_{2r} \end{pmatrix} \tag{3}$$

et que la matrice $\mathcal{S}$ est inversible.

(c) Soit $v \in (\mathbb{F}_{2^6})^{63}$ défini par $v_i = \alpha^{i-1}$ pour $i \neq 1, 5, 12, 23, 45$ et $v_i = \alpha^{i-1} + \alpha^i$ pour $i = 1, 5, 12, 23, 45$. En utilisant (3), (2) et (1), déterminer, s'il existe, le mot le code le plus proche de v.

6. Plus généralement écrire un algorithme de décodage pour les codes de Reed-Solomon $[n = p^m - 1, n-d+1, d]$ définis sur $\mathbb{F}_{p^m}$ (p premier et $m \geq 2$) et engendrés par $g(x) = (x-\alpha)\cdots(x-\alpha^{d-1})$ où $\alpha \in \mathbb{F}_{p^m}$ est une racine primitive n-ième de 1.

2 Codes de Hamming (binaires)

1. Ecrire un programme qui prend en entrée un entier naturel $r \geq 2$ et qui calcule la matrice de contrôle H définissant le code de Hamming binaire $\mathcal{H}_r$ de longueur $n = 2^r - 1$.
2. Ecrire une procédure qui permet de calculer *une* matrice génératrice de $\mathcal{H}_r$.Les codes $\mathcal{H}_3$ et $\mathcal{H}_4$ possèdent-ils une matrice génératrice sous forme systématique ?
3. Ecrire un programme qui prend en entrée un entier naturel $r \geq 2$, une matrice génératrice G de $\mathcal{H}_r$ et un mot de l'espace ambiant v tel que $v = m \cdot G + e$, où $m \in \mathbb{F}_2^k$, $e \in \mathbb{F}_2^n$, $w(e) \leq 1$ avec $n = 2^r - 1$ et $k = n - r$. Ce programme rend c ainsi que m.
   Faire des tests.

3 Codes de Hamming sur $\mathbb{F}_q$

Soit r un entier ≥ 2. Un code de Hamming $\mathcal{H}_r(q)$ sur le corps fini $\mathbb{F}_q$ est défini à équivalence près par une matrice de parité dont les colonnes sont les r-uplets non nuls de $\mathbb{F}_q$ avec une première entrée non nulle égale à 1. Par exemple $\mathcal{H}_2(3)$ est, à équivalence près, le code sur $\mathbb{F}_3$ de matrice génératrice

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

1. Ecrire une procédure qui construit une matrice de contrôle d'un code de Hamming $\mathcal{H}_r(q)$ sur $\mathbb{F}_q$ pour $r \in \mathbb{N}$, $r \geq 2$. On demande de plus que la matrice formée des dernières colonnes de cette matrice de contrôle soit la matrice identité.
2. Ecrire un algorithme de décodage et faire des tests.