Université Mohammed V Agdal
Faculté des Sciences
Laboratoire de Mathématiques,
Informatique et Applications

Année 2009-10
Master 2 CSI
Théorie des codes 2
Contrôle Continu

Problème :

Soit C un code BCH strict sur $\mathbb{F}_q$ de longueur n et de distance prescrite δ. Soit α une racine primitive n^{eme} de l'unité dans l'extension $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$ (m le plus petit possible).

1) Montrer que le code C corrige au moins $t = [(\delta - 1)/2]$ erreurs.

Soit $y(x)$ un mot recçu. On suppose que $y(x)$ diffère d'un mot $c(x)$ de C au plus en t coordonnées. Par $e(x) = y(x) - c(x)$ on note l'erreur soit :

$$e(x) = e_{k_1}x^{k_1} + e_{k_2}x^{k_2} + \cdots + e_{k_\nu}x^{k_\nu}$$

où les e_{k_i} sont tous non nuls.

2) Comparer t et ν.

3) Montrer que $y(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i)$ pour tout $1 \leq i \leq 2t$.

Pour $1 \leq i \leq 2t$ on définit le syndrome S_i de $y(x)$ par $S_i = y(\alpha^i)$ dans F_{q^m}.

Soit la matrice $t \times n$

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ & & \vdots & & \\ 1 & \alpha^t & \alpha^{2t} & \cdots & \alpha^{t(n-1)} \end{pmatrix}$$

Si $y(x) = y_0 + y_1x + \cdots + y_{n-1}x^{n-1}$, on pose $\mathbf{y} = (y_0, y_1, \cdots, y_{n-1})$ et $S = (S_1, S_2, \cdots, S_t)$, où $S_i = y(\alpha^i)$.

4) Montrer que $H\mathbf{y}^T = S^T$.

5) Montrer que $S_{iq} = S_i^q$ pour tout $i \geq 1$ où on suppose que $S_i = y(\alpha^i)$ même pour $i > 2t$;

On pose $E_j = e_{k_j}$ et $X_j = \alpha^{k_j}$.

6) Montrer que la connaissance de X_j localise de façon unique l'erreur k_j.

7) Montrer que $S_i = \sum_{j=1}^{\nu} E_j X_j^i$ pour $1 \leq i \leq 2t$.

on pose $f(x) = (1 - xX_1)(1 - xX_2)\cdots(1 - xX_\nu) = 1 + \sum_{j=1}^{\nu} \sigma_i x^i$.

8) Montrer que $f(X_j^{-1}) = 1 + \sigma_1 X_j^{-1} + \sigma_2 X_j^{-2} + \cdots \sigma_\nu X_j^{-\nu} = 0$ pour $1 \leq j \leq \nu$.

9) Montrer que ,

$$\sum_{j=1}^{\nu} E_j X_j^{i+\nu} + \sigma_1 \sum_{j=1}^{\nu} E_j X_j^{i+\nu-1} + \cdots + \sigma_\nu \sum_{j=1}^{\nu} E_j X_j^i = 0$$

pour $1 \leq j \leq \nu$ et montrer que $\sigma_1 S_{i+\nu-1} + \sigma_2 S_{i+\nu-2} + \cdots + \sigma_\nu S_i = -S_{i+\nu}$ pour $1 \leq i \leq \nu$ et écrire ce système sous forme matricielle.

Pour $\mu \leq t$ on pose

$$M_\mu = \begin{pmatrix} S_1 & S_2 & \cdots & S_\mu \\ S_2 & S_3 & \cdots & S_{\mu+1} \\ & & \vdots & \\ S_\mu & S_{\mu+1} & \cdots & S_{2\mu-1} \end{pmatrix}, A_\mu = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_\mu \\ & & \vdots & \\ X_1^{\mu-1} & X_2^{\mu-1} & \cdots & X_\mu^{\mu-1} \end{pmatrix}, D_\mu = \begin{pmatrix} E_1X_1 & 0 & \cdots & 0 \\ 0 & E_2X_2 & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & E_\mu X_\mu \end{pmatrix}$$

10) Montrer que si $\mu > \nu$ alors $S_i = \sum_{j=1}^{\mu} E_j X_j^i$ pour $1 \leq i \leq 2t$.

11) Montrer que $M_\mu = A_\mu B_\mu A_\mu^T$.

12) Montrer que M_μ est inversible si $\mu = \nu$ et non inversible si $\mu > \nu$.

13) Expliquer en détail comment utiliser ce qui précède pour décoder les codes BCH.