Théorie de l'information et codage **2010/2011**

Cours 11 — 10-17-24 mai 2011

Enseignant: Marc Lelarge *Scribe: Nicolas Daviaud - Marc Lelarge*

Pour information

- Page web du cours
  `http://www.di.ens.fr/~lelarge/info11.html`

11.1 Code de Hamming cycliques

Rappel : la matrice de parité d'un code de Hamming de longueur $n = 2^m - 1$ a pour colonnes les $2^m - 1$ m-uplets distincts et non nuls.

Si $\alpha \in \mathbb{F}(2^m)$ est un élément primitif, alors $1, \alpha, \dots \alpha^{2^m-2}$ sont distincts et non nuls, et peuvent être représentés par des m-ulpets. On définit le code de Hamming $\mathcal{H}_m$ avec paramètres $n = 2^m - 1, k = n - m, d_{\min} = 3$ par la matrice de parité $H = \left(1\ \alpha\ \cdots\ \alpha^{2^m-2}\right)$ où les α^i sont remplacés pas les m-uplets correspondants.

Exemple 11.1.1: Code de Hamming $\mathcal{H}_3$

On se place dans le cas $\mathbb{F}(2^3)$ et $\alpha^3 + \alpha + 1 = 0$

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

Un vecteur $c = (c_0 \cdots c_{n-1})$ appartient à $\mathcal{H}_m$ ssi $Hc^T = 0$ ssi $c(\alpha) = 0$ où $c(X) = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1}$. Par la propriété (M2), on a $c \in \mathcal{H}_m \Leftrightarrow M^{(1)}(X) | c(X)$ où $M^{(1)}(X)$ est le polynôme minimal de α.

Théorème 11.1.1 *Le code de Hamming $\mathcal{H}_m$ ci-dessus est un code cyclique de générateur le polynôme minimal de α.*

Un résultat précédent fournit la matrice générant $\mathcal{H}_m$:

$$G = \begin{pmatrix} M^{(1)}(X) & 0 & \cdots & 0 \\ 0 & XM^{(1)}(X) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & X^{n-m-1}M^{(1)}(X) \end{pmatrix}$$

Exemple 11.1.2: Code de Hamming $\mathcal{H}_3$ (suite)

Une matrice génératrice est

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & & & \\ & 1 & 1 & 0 & 1 & & \\ & & 1 & 1 & 0 & 1 & \\ & & & 1 & 1 & 0 & 1 \end{pmatrix}$$

De plus, on a $h(X) = \frac{X^7+1}{X^3+X+1} = X^4 + X^2 + X + 1$ et donc

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

On remarque que $\tilde{H} \neq H$ mais la dernière ligne de $\tilde{H}$ peut s'obtenir comme la somme des premières et dernières lignes de H.

11.2 Codes BCH (Bose-Chaudhuri-Hocquenghem)

On commence par un exemple en reprenant le code de Hamming cyclique de longueur $n = 15$, c'est à dire avec $m = 4$ et matrice de parité :

$$H = (1\ \alpha\ \cdots\ \alpha^{14}).$$

L'idée est de 'rajouter' des bits de parité grâce à une fonction f :

$$H' = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{14} \\ f(1) & f(\alpha) & \cdots & f(\alpha^{14}) \end{pmatrix}$$

S'il y a deux erreurs en $i \neq j$ alors le syndrome est :

$$s = H'_i + H'_j = \begin{pmatrix} \alpha^i + \alpha^j \\ f(\alpha^i) + f(\alpha^j) \end{pmatrix}$$

On est donc amené à résoudre $\alpha^i + \alpha^j = z_1$ et $f(\alpha^i) + f(\alpha^j) = z_2$.

Voici deux choix pour f qui ne sont pas judicieux :

– f linéaire -> mauvais car n'ajoute aucune information

– $f = X^2$ -> mauvais car en caractéristique 2 $x^2 + y^2 = (x + y)^2$.

Nous allons maintenant voir que le choix $f(x) = x^3$ permet de corriger deux erreurs. Avec $f(x) = x^3$, on obtient $\alpha^i + \alpha^j = z_1 \neq 0$ et $\alpha^{3i} + \alpha^{3j} = z_2 = (\alpha^i + \alpha^j)(\alpha^{2i} + \alpha^{i+j} + \alpha^{2j}) =$

$z_1(z_1^2 + \alpha^i\alpha^j)$ de telle sorte que : $\alpha^i\alpha^j = \frac{z_2}{z_1} + z_1^2$. Donc α^i et α^j sont solutions de l'équation du second degré :

$$X^2 + z_1X + (\frac{z_2}{z_1} + z_1^2) = 0 \tag{11.1}$$

Décodage du code BCH corrigeant deux erreurs : pour y recu, on calcule $s = Hy^T$ puis
- si $z_1 = z_2 = 0$, décider qu'il n'y a pas d'erreur
- si $z_1 \neq 0$ et $z_2 = z_1^3$, corriger une erreur en i tq $z_1 = \alpha^i$
- si $z_1 \neq 0$ et $z_2 \neq z_1^3$ corriger deux erreurs en i et j avec α^i et α^j racines de (11.1)
- sinon, détecter au moins 3 erreurs

S'il y a moins de deux erreurs, elles seront corrigées. On a donc démontré que $d_{\min} \geq 5$ pour ce code.

EXEMPLE 11.2.1:

Reprenons l'exemple ci-dessus avec $m = 4$, $F(2^4)$ et $\alpha^4 + \alpha + 1 = 0$

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{12} \end{pmatrix}$$

Remarque : α^3 n'est pas un élément primitif.

Supposons qu'on ait deux erreurs en 6 et 8. On trouve alors $z_1 = \alpha^6 + \alpha^8 = \alpha^{14} = 1001$ et $z_2 = \alpha^3 + \alpha^9 = \alpha = 0100$. On a donc $\frac{z_2}{z_1} + z_1^2 = \alpha^2 + \alpha^{13} = \alpha^{14}$ et on cherche donc les racines de $X^2 + \alpha^{14}X + \alpha^{14} = (X + \alpha^6)(X + \alpha^8)$ et on retrouve bien les deux erreurs correspondant à α^6 et α^8 (donc en position 7 et 9).

Plus généralement, un code de longueur $n = 2^m - 1$ corrigeant deux erreurs C est donné par la matrice de parité

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(2^m-2)} \end{pmatrix}.$$

On a alors

$$\begin{aligned} c \in C &\Leftrightarrow Hc^T = 0 \\ &\Leftrightarrow \textstyle\sum_{i=0}^{n-1} c_i\alpha^i = 0 \text{ et } \sum_{i=0}^{n-1} c_i\alpha^{3i} = 0 \\ &\Leftrightarrow \text{ppcm}\left(M^{(1)}(X), M^{(3)}(X)\right) | c(X) \\ &\Leftrightarrow M^{(1)}(X)M^{(3)}(X) | c(X) \end{aligned}$$

où dans la dernière équivalence, on utilise le fait que $M^{(1)}(X)$ et $M^{(3)}(X)$ sont irréductibles et distincts (cf exo) et donc premiers entre eux.

Théorème 11.2.1 *Le code binaire BCH C corrigeant deux erreurs a pour paramètres $n = 2^m - 1$, $k = n - 2m$ et $d_{\min} \geq 5$*

Démonstration. Le seul point à noter concerne la dimension :

$$k = n - 2m \Leftrightarrow \deg g(X) = 2m \text{ cf exo.}$$

□

11.3 Facteurs de $X^n - 1$

Nous avons vu que le polynôme générateur d'un code cyclique de longueur n sur $F(q)$ doit être un facteur $X^n - 1$.

On suppose que n et q sont premiers entre eux : $n \wedge q = 1$.

Il existe un plus petit entier m tel que $n|q^m - 1$ (ce résultat découle de l'exercice 11-1). m est appelé l'ordre multiplicatif de q modulo n.

On a alors (exercice 9-3) $X^n - 1|X^{q^m-1} - 1$ mais ne divise aucun des $X^{q^s-1} - 1$ pour $0 < s < m$.

Donc les racines de $X^n - 1$ qui sont appellées les racines n-ième de l'unité sont dans l'extension de corps $F(q^m)$ et ne sont inclus dans aucun corps plus petit.

Comme la dérivée de $X^n - 1$ est nX^{n-1} et que $n \wedge q = 1$, ces deux polynômes sont premiers entre eux. Donc $X^n - 1$ a n racines distinctes. En fait il découle de l'exercice 11-2(i) qu'il existe une racine n-ième de l'unité primitive notée α, telle que

$$X^n - 1 = \prod_{i=0}^{n-1} (X - \alpha^i).$$

Dans toute la suite, α est une racine $n$ième de l'untité primitive.

Nous avions défini les classes cyclotomiques modulo $p^m - 1$. Plus généralement, la classe cyclotomique modulo n sur $F(q)$ qui contient s est

$$C_s = \{s, sq, \ldots, sq^{m_s-1}\} \text{ avec } sq^{m_s} \equiv s \mod n.$$

On remarque que $m_1 = |C_1| = m$ est l'ordre multiplicatif de q modulo n. On obtient alors un partition

$$\{0, 1, \ldots, n-1\} = \cup_s C_s,$$

où s parcrout les représentants de classes mod n.

EXEMPLE 11.3.1:

Pour $n = 9, q = 2$, on obtient :

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8, 7, 5\} \\ C_3 &= \{3, 6\}. \end{aligned}$$

Donc $m = 6$ et $X^9 - 1$ se décompose sur $F(2^6)$.

Comme précédemment, on définit le polynôme minimal de α^s par :

$$M^{(s)}(X) = \prod_{i \in C_s} (X - \alpha^i).$$

C'est le polynôme unitaire de degré minimal à coefficients dans $F(q)$ ayant α^s comme racine.

On a alors

$$X^n - 1 = \prod_s M^{(s)}(X), \text{ où } s \text{ parcrout les représentants de classes.}$$

C'est la factorisation de $X^n - 1$ en polynômes irréductible sur $F(q)$.

EXEMPLE 11.3.2:

On continue l'exemple avec $n = 9$ et $q = 2$: on a donc $X^9 + 1 = M^{(0)}(X)M^{(1)}(X)M^{(3)}(X)$. Comme $M^{(0)}(X) = X + 1$, et que le seul polynôme irreductible de degré 2 sur $F(2)$ est $X^2 + X + 1$ donc $M^{(3)}(X) = X^2 + X + 1$ de telle sorte que $M^{(1)}(X) = X^6 + X^3 + 1$.

11.4 Codes BCH corrigeant t erreurs

Théorème 11.4.1 Borne BCH : *Soit C un code cyclique de polynome générateur $g(X)$ tel que pour des entiers $b \geq 0$ et $\delta \geq 1$, $g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0$. Alors $d_{\min} \geq \delta$.*

Démonstration. Si $c = (C_0, c_1, \ldots, c_{n-1}) \in C$ alors $c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+\delta-2}) = 0$ donc $H'c^T = 0$ avec

$$H' = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \ldots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix}.$$

La matrice H' n'est pas forcément la matrice de parité entière. Il suffit cependant de montrer que toute combinaison de $\leq \delta - 1$ colonnes de H' sont linéairement indépendantes sur $F(q^m)$. Soit donc c de poids $w \leq \delta - 1$ avec $c_i \neq 0$ ssi $i \in \{a_1, a_2, \ldots, a_w\}$. Alors $H'c^T = 0$ implique :

$$\begin{pmatrix} \alpha^{a_1 b} & \ldots & \alpha^{a_w b} \\ \alpha^{a_1(b+1)} & \ldots & \alpha^{a_w(b+1)} \\ \vdots & & \vdots \\ \alpha^{a_1(b+w-1)} & \ldots & \alpha^{a_w(b+w-1)} \end{pmatrix} \begin{pmatrix} c_{a_1} \\ \vdots \\ c_{a_w} \end{pmatrix} = 0.$$

Donc le déterminant de la matrice de gauche est nul, hors à un facteur $\alpha^{(a_1+\cdots+a_w)b}$, c'est

$$\det\begin{pmatrix} 1 & \dots & 1 \\ \alpha^{a_1} & & \alpha^{a_w} \\ \vdots & & \vdots \\ \alpha^{a_1(w-1)} & \dots & \alpha^{a_w(w-1)} \end{pmatrix},$$

qui est un determinant de Vandermonde donc $\prod_{i>j}(\alpha^{a_i} - \alpha^{a_j}) \neq 0$. □

Exemple 11.4.1:

Considérons les cas suivants :

- $\mathcal{H}_m$ a pour polynome générateur $M^{(1)}(X)$ dont α et α^2 sont racines (par la propriété (M6)). Donc $b = 1$ et $\delta = 3$. Ainsi $d_{\min} \geq 3$, en fait, on a égalité dans ce cas.
- le code C de générateur $M^{(1)}(X)M^{(3)}(X)$. On a alors $M^{(1)}(\alpha) = M^{(1)}(\alpha^2) = M^{(1)}(\alpha^4) = 0$ et $M^{(3)}(\alpha^3) = 0$ donc $d_{\min} \geq 5$.

Définition 11.4.1 Code BCH : *Un code cyclique de longueur n sur $\mathbb{F}_q$ est un code BCH(b, δ) si son polynôme générateur est :*

$$g(X) = ppcm\left\{M^{(b)}(X), \dots, M^{(b+\delta-2)}(X)\right\}$$

i.e. le polynôme unitaire de degré minimal admettant $\alpha^b, \dots, \alpha^{b+\delta-2}$ comme racines. Par défaut, un code BCH(δ) est un code BCH$(1, \delta)$.

Il découle du résultat précédent que $d_{\min} \geq \delta$.

On a : c est un mot code ssi $c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+\delta-2}) = 0$. En particulier, une matrice de parité pour le code est donnée par

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \vdots & & & & \vdots \\ 1 & \alpha^{b+\delta-2} & & \dots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix},$$

où chaque entrée est remplacée par la colonne correspondante de m éléments de $F(q)$. Une fois le remplacement effectué, il y a $m(\delta - 1)$ lignes dans la matrice qui ne sont pas nécessairement toutes indépendantes donc la dimension du code est au moins $n - m(\delta - 1)$. On a donc :

Théorème 11.4.2 *Un code BCH(b, δ) de longueur n sur $F(q)$ a une dimension $k \geq n - m(\delta - 1)$ (où m est l'ordre multiplicatif de q modulon n) et vérifie $d_{\min} \geq \delta$.*

Remarque 11.4.1 *Un code BCH est dit primitif si $n = q^m - 1$, c'est-à-dire si α est un élément primitif de $\mathbb{F}_{q^m}$*

Exemple 11.4.2: Code BCH binaires de longueur 15 ($b = 1$) :

δ	$g(X)$	exposant des racines	dim	d_{min}
1	1		15	1
3	$M^{(1)}$	$1, 2, 4, 8$	11	3
5	$M^{(1)}M^{(3)}$	$1, \ldots, 4, 6, 8, 9, 12$	7	5
7	$M^{(1)}M^{(3)}M^{(5)}$	$1, \ldots, 6, 8, 9, 10, 12$	5	7
$9, 11, 13, 15$	$M^{(1)}M^{(3)}M^{(5)}M^{(7)}$	$1, \ldots, 14$	1	15

On remarque que les distances minimales des codes $BCH(9)$ et $BCH(11)$ sont les mêmes.

11.5 Codes de Reed-Solomon

Définition 11.5.1 *Un code de Reed-Solomon sur $F(q)$ est un code $BCH(b, \delta)$ de longueur $n = q-1$ (i.e. $m = 1$).*

Comme $X^{q-1} - 1 = \prod_{\beta \in F(q)^*}(X - \beta)$, le polynôme minimal de α^i est simplement $M^{(i)}(X) = X - \alpha^i$. Donc le polynôme générateur du code est

$$g(X) = (X - \alpha^b)(X - \alpha^{b+1}) \ldots (X - \alpha^{b+\delta-2})$$

Exemple 11.5.1:

On considère $F(4) = \{0, 1, \alpha, \beta = \alpha^2\}$ avec $\alpha^2 + \alpha + 1 = 0$.Un code RS sur $F(4)$ de longueur $n = 3$ avec $\delta = 2$ et $b = 2$ a pour polynôme générateur $g(X) = X - \beta$.Les mots code sont : $000, 1\alpha 0, \beta 0\alpha, \beta\alpha 1, 01\alpha, \alpha\beta 0, 10\beta, 111, 0\alpha\beta, \beta 10, 1\beta\alpha, \alpha\alpha\alpha, 0\beta 1, \alpha 01, \alpha 01, \alpha 1\beta, \beta\beta\beta$.

La dimension d'un code RS est $k = n - \deg g(X) = n - \delta + 1$. Donc $d_{\min} \geq \delta = n - k + 1$, hors $n - k$ est égal au rang de la matrice de parité H donc $n - k \geq d_{\min} - 1$. Au final, pour un code RS

$$d_{\min} = \delta = n - k + 1.$$

11.6 Le polynôme de Mattson-Solomon

On considère toujours $\alpha \in F(q^m)$ qui est une racine n-ième de l'unité primitive. Le poynôme de Mattson-Solomon (MS) associé au veccteur $a = (a_0, \ldots, a_{n-1})$ avec $a_i \in F(q^m)$ est le polynôme dans $F(q^m)[Z]$:

$$A(Z) = \sum_{j=1}^{n} A_j Z^{n-j},$$

avec $A_j = a(\alpha^j) = \sum_{i=0}^{n-1} a_i \alpha^{ij}$.

Remarque 11.6.1 *On a :*

$$\begin{pmatrix} A_0 \\ A_1 \\ \vdots \\ A_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & & & & \vdots \\ 1 & \alpha^{n-1} & & \dots & \alpha^{(n-1)^2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

Pour un code BCH$(1, \delta)$*, tous les mots codes a sont tels que* $A_1 = A_2 = \cdots = A_{\delta-1} = 0$*.*

Théorème 11.6.1 Formule d'inversion : *Le vecteur a peut être retrouvé à partir de* $A(Z)$ *par :*

$$\begin{aligned} a_i &= \frac{1}{n} A(\alpha^i), \text{ pour } i = 0, 1, \dots, n-1 \\ a(X) &= \frac{1}{n} \sum_{i=0}^{n-1} A(\alpha^i) X^i \end{aligned}$$

La preuve découle des deux lemmes suivants :

Lemme 11.6.1 *Soit* $\xi \in F(q^m)$ *racine de* $X^n - 1$ *alors*

$$\sum_{i=0}^{n-1} \xi^i = \begin{cases} 0 & si\ \xi \neq 1, \\ n & si\ \xi = 1. \end{cases}$$

Démonstration. Si $\xi \neq 1$, on a $\sum_{i=0}^{n-1} \xi^i = \frac{1-\xi^n}{1-\xi} = 0$. □

Lemme 11.6.2 *Le vecteur* $c = (c_0, c_1, \dots, c_{n-1})$ *peut être retrouvé à partir de* $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ *par*

$$c_i = \frac{1}{n} \sum_{j=0}^{n-1} c(\alpha^j) \alpha^{-ij}.$$

Démonstration.

$$\begin{aligned} \sum_{j=0}^{n-1} c(\alpha^j) \alpha^{-ij} &= \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} c_k \alpha^{kj} \alpha^{-ij} \\ &= \sum_{k=0}^{n-1} c_k \sum_{j=0}^{n-1} \alpha^{j(k-i)} \\ &= n c_i. \end{aligned}$$

□

Polynôme locateur : soit un vecteur $a = (a_0, \dots a_{n-1})$ avec $a_i \in F(q)$ et ayant w composantes non nulles $a_{i_1}, \dots, a_{i_w}$. On associe au vecteur a les éléments de $F(q^m)$ définis par

$$X_1 = \alpha^{i_1}, \dots X_w = \alpha^{i_w},$$

qui sont appelés les locateurs de a et les éléments de $F(q)$:

$$Y_1 = a_{i_1}, \dots Y_w = a_{i_w}.$$

Le vecteur a est complétement déterminé par la liste $(X_1, Y_1), \dots (X_w, Y_w)$.

On a

$$a(\alpha^j) = A_j = \sum_{i=1}^{w} Y_i X_i^j.$$

Le polynôme locateur de a est donné par :

$$\sigma(Z) = \prod_{i=1}^{w}(1 - X_i Z) = \sum_{i=0}^{w} \sigma_i Z^i, \text{ avec } \sigma_0 = 1.$$

Les coefficients σ_i sont les fonctions symmétriques élémentairesdes X_i :

$$\begin{aligned} \sigma_1 &= -(X_1 + \cdots + X_w) \\ \sigma_2 &= X_1X_2 + X_1X_3 + \cdots + X_{w-1}X_w \\ &\vdots \\ \sigma_w &= (-1)^w X_1 \dots X_w. \end{aligned}$$

Théorème 11.6.2 Identités de Newton : *Pour tout j, les A_i satisfont la recurrence :*

$$A_{j+w} + \sigma_1 A_{j+w-1} + \cdots + \sigma_w A_j = 0. \tag{11.2}$$

En particulier, on a :

$$\begin{pmatrix} A_w & A_{w-1} & \dots & A_1 \\ A_{w+1} & A_w & \dots & A_2 \\ \vdots & & & \vdots \\ A_{2w-1} & A_{2w-2} & \dots & A_w \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_w \end{pmatrix} = \begin{pmatrix} A_{w+1} \\ A_{w+2} \\ \vdots \\ A_{2w} \end{pmatrix}$$

Démonstration. Dans l'équation :

$$\prod_{i=1}^{w}(1 - X_i Z) = 1 + \sigma_1 Z + \cdots + \sigma_w Z^w,$$

en prenant $Z = \frac{1}{X_i}$ et en multipliant par $Y_i X_i^{j+w}$, on obtient :

$$Y_i X_i^{j+w} + \sigma_1 Y_i X_i^{j+w-1} + \cdots + \sigma_w Y_i X_i^j = 0.$$

En sommant sur $i = 1, \dots, w$, on obtient (11.2). □

11.7 Décodage de codes BCH

On se restreint au cas binaire et $b = 1$ de telle sorte que la matrice de parité est :

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \vdots & & & & \vdots \\ 1 & \alpha^{\delta-2} & \dots & \dots & \alpha^{(\delta-2)(n-1)} \end{pmatrix}$$

Étape 1 : calcul du sydrome

Le mot code envoyé est $c = c_0 c_1 \dots c_{n-1}$ et le mot code reçu est $y = c + e$ où e est le motif d'erreur. Le syndrome est alors donné par :

$$s = Hy^T = \begin{pmatrix} \sum_i y_i \alpha^i \\ \sum_i y_i \alpha^{3i} \\ \vdots \\ \sum_i y_i \alpha^{(\delta-2)i} \end{pmatrix} = \begin{pmatrix} y(\alpha) \\ y(\alpha^3) \\ \vdots \\ y(\alpha^{\delta-2}) \end{pmatrix} = \begin{pmatrix} A_1 \\ A_3 \\ \vdots \\ A_{\delta-2} \end{pmatrix},$$

avec $A_\ell = y(\alpha^\ell)$.

Étape 2 : trouver le polynôme locateur $\sigma(z)$

On suppose que le motif d'erreur e a pour poids w et composantes non nulles $e_{i_1}, \dots, e_{i_w}$, donc que les erreurs ont eu lieu en $i_1, \dots i_w$. On définit $X_r = \alpha^{i_r}$ pour $r = 1, \dots, w$ et $\sigma(z) = \prod_{i=1}^{w}(1 - X_i z)$.

On a alors $A_\ell = y(\alpha^\ell) = c(\alpha^\ell) + e(\alpha^\ell) = e(\alpha^\ell)$ pour $1 \leq \ell \leq \delta - 1$ donc dans le cas binaire $A_\ell = \sum_{i=1}^{w} X_i^\ell$.

Le but est alors de trouver $\sigma(z)$ de plus petit degré satisfaisant les identités de Newton étant donné $A_1, A_2, \dots, A_{\delta-1}$.

Nous présentons un algorithme simple mais peu efficace ci-dessous.

Étape 3 : trouver les racines de $\sigma(z)$

La méthode la plus simple est de tester les différentes puissances de α. Il y a une erreur en i si $\sigma(\alpha^{-i}) = 0$.

11.8 Forme usuelle des identités de Newton et décodage de codes BCH

Soient $X_1, \dots X_w$ des indéterminées et

$$\sigma(z) = \prod_{i=1}^{w}(1 - X_i z)$$

Noter l'abus de notations qui prend sens par la suite...

On définit pour tout $i \geq 1$:

$$P_i = \sum_{r=1}^{w} X_r^i.$$

Lemme 11.8.1 *Si $P(z) = \sum_{i=1}^{\infty} P_i z^i$, on a $\sigma(z)P(z) + z\sigma'(z) = 0$*

Démonstration. On remarque que

$$P(z) = \sum_{r=1}^{w} \frac{X_r z}{1 - X_r z}, \text{ donc } \sigma(z)P(z) = \sum_{r=1}^{w} X_r z \prod_{i=1, i\neq r}^{w} (1 - X_i z),$$

or $\sigma'(z) = -\sum_{r=1}^{w} X_r \prod_{i=1,i\neq r}^{w}(1 - X_i z)$ donc le lemme est démontré. □

On a donc en regardant les coefficients du membre de gauche :

$$\begin{aligned} P_1 + \sigma_1 &= 0 \\ P_2 + P_1\sigma_1 + 2\sigma_2 &= 0 \\ &\vdots \\ P_w + \sigma_1 P_{w-1} + \cdots + \sigma_{w-1}P_1 + w\sigma_w &= 0, \end{aligned}$$

et pour $i > w$, on a :

$$P_i + \sigma_1 P_{i-1} + \cdots + \sigma_w P_{i-w} = 0.$$

Dans le cas binaire, c'est à dire si les X_i sont dans un corps de caractéristique 2, on remarque tout d'abord que $P_{2k} = P_k^2$. Donc les 2-ième, 4-ième... équations ci-dessus ne sont pas des containtes pour σ et on a alors :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ P_2 & P_1 & 1 & 0 & 0 & \dots & 0 \\ P_4 & P_3 & P_2 & P_1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ P_{2w-2} & P_{2w-3} & \dots & \dots & \dots & \dots & P_{w-1} \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \vdots \\ \sigma_w \end{pmatrix} = \begin{pmatrix} P_1 \\ P_3 \\ P_5 \\ \vdots \\ P_{2w-1} \end{pmatrix}. \tag{11.3}$$

Ceci permet de démontrer le théroème suivant :

Théorème 11.8.1 *Dans un corps de caractéristique 2 et si les $(X_i)_{i=1}^w$ sont deux à deux distincts et non nuls, la matrice de taille $\nu \times \nu$ donnée par*

$$M_\nu = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ P_2 & P_1 & 1 & 0 & 0 & \dots & 0 \\ P_4 & P_3 & P_2 & P_1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ P_{2\nu-4} & P_{2\nu-5} & \dots & \dots & \dots & \dots & P_{\nu-3} \\ P_{2\nu-2} & P_{2\nu-3} & \dots & \dots & \dots & \dots & P_{\nu-1} \end{pmatrix}$$

est non singulière si $w = \nu$ ou $w = \nu - 1$ et est singulière si $w < \nu - 1$.

Démonstration.

(i) Si $w < v-1$, alors

$$M_v \begin{pmatrix} 0 \\ 1 \\ \sigma_1 \\ \cdots \\ \sigma_{v-2} \end{pmatrix} = 0,$$

d'après (11.3).

(ii) Si $w = v$ alors

$$\det M_v = \prod_{1 \le i < j \le v} \left(X_i + X_j \right). \tag{11.4}$$

En effet, on a $P_i = \sum_{r=1}^{w} X_r^i$, donc si $X_i = X_j$ pour $i \neq j$, on a $P_i = \sum_{r \neq i,j} X_r^i$ et $\det M_v = 0$ par le point (i). Donc le membre de gauche doit être divisible par le membre de droite. Montrons maintenant que $\det M_v$ est homogène de degré $v(v-1)/2$. Soit $\gamma(j,k)$ l'indice de P correspondant au coefficient $M_v(j,k)$ de la matrice. Par exemple, $\gamma(2,1) = 2$, $\gamma(2,2) = 1$... On prend comme convention si le coefficient est 1 : $\gamma(1,1) = 0$ et si le coefficient est 0 : $\gamma(1,2) = -\infty$. On a alors $\gamma(v,k) = 2v-1-k$ et $\gamma(j,v) = 2j-1-v$ pour $2j \geq v+1$ et $\gamma(j,v) = -\infty$ pour $2j < v+1$. On a donc pour $k, j \leq v-1$ et $2j \geq v+1$:

$$\begin{aligned} \gamma(v,k) + \gamma(j,v) &= v - 2 + k - 2j \\ \gamma(j,k) &= 2j - k - 1 \text{ donc,} \\ \gamma(v,k) + \gamma(j,v) - \gamma(j,k) &= v - 1 \end{aligned}$$

On écrit maintenant : $\det M_v = \sum_{s \in \mathcal{S}_v} \prod_{i=1}^{v} M_v(i, s(i))$ et montrons par récurrence sur v que chacun des termes (non nul) de cette somme est homogène de degré $v(v-1)/2$. On observe que le terme associé à la permutation s est homogène de degré :

$$\sum_{i=1}^{v} \gamma(i, s(i)) = \gamma(v, s(v)) + \gamma(s^{-1}(v), v) + \sum_{i \neq v, s^{-1}(v)} \gamma(i, s(i)).$$

D'après l'hypothèse de récurrence, on a, si $\gamma(v, s^{-1}(v)) \neq -\infty$

$$\sum_{i \neq v, s^{-1}(v)} \gamma(i, s(i)) = \frac{(v-1)(v-2)}{2} - \gamma(v, s^{-1}(v))$$

Au final, on obtient :

$$\begin{aligned} \sum_{i=1}^{v} \gamma(i, s(i)) &= \gamma(v, s(v)) + \gamma(s^{-1}(v), v) - \gamma(v, s^{-1}(v)) + \frac{(v-1)(v-2)}{2} \\ &= v - 1 + \frac{(v-1)(v-2)}{2} = \frac{v(v-1)}{2} \end{aligned}$$

Donc $\det M_\nu$ est homogène de degré $\nu(\nu-1)/2$, ce qui implique que les deux termes de (11.4) ne diffèrent que d'une constante. Il reste à montrer que cette constante vaut 1 et non 0. Pour ceci, il suffit de calculer chaque terme pour des valeurs particulières des X_i. Si ν est impaire, on prend pour X_i les racines ν-ième de l'unité. On a alors

$$P_i = \sum_{r=1}^{\nu} X_r^i = \begin{cases} 0 & \text{si } i \not\equiv 0 \mod \nu \\ 1 & \text{si } i \equiv 0 \mod \nu \end{cases}$$

On vérifie alors qu'il y a exactement un 1 par ligne et par colonne dans M_ν donc $\det M_\nu = 1$. De même pour ν paire, en prenant les racines de $X^\nu - X = 0$, on aboutit aussi à $\det M_\nu = 1$. Donc dans les deux cas, on a bien (11.4).

(iii) Si $w = \nu - 1$, il suffit de prendre $X_1 = 0$ et d'utiliser (11.4).

□

En utilisant ce théorème, on a donc un algorithme itératif qui permet de trouver $\sigma(z)$ pour un code BCH($\delta = 2t+1$) si w erreurs ont lieu avec $w \leq t$ (et w inconnu).

On suppose que t erreurs ont eu lieu et on essaye de résoudre (11.3) avec w remplacé par t. D'après le théorème précédent, si t ou $t-1$ erreurs ont eu lieu, une unique solution existe et on va directement à l'étape 3. Si moins de $t-1$ erreurs ont eu lieu, les équations ne déterminent pas une solution. Dans ce cas, on suppose que $t-2$ erreurs ont eu lieu et on recommence la procédure...

Exemple 11.8.1: Cas $\nu = 2$. Le système est :

$$\begin{pmatrix} 1 & 0 \\ P_1^2 & P_1 \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \end{pmatrix} = \begin{pmatrix} P_1 \\ P_3 \end{pmatrix}$$

D'après le théorème précédent, ce système est inversible si $w = 2$ ou $w = 1$ mais pas si $w = 0$. En effet on a $P_1 \neq 0$ pour $w = 1, 2$ alors que $P_1 = 0$ pour $w = 0$. Dans le premier cas, on a donc $\sigma_1 = P_1$ et $\sigma_2 = \frac{P_3}{P_1} + P_1^2$. On trouve donc pour le polynome localisateur

$$\sigma(z) = 1 + P_1 z + \left(\frac{P_3}{P_1} + P_1^2\right) z^2 \tag{11.5}$$

On remarque que si $w = 1$ alors $P_3 = P_1^3$ et $\sigma(z) = 1 + P_1 z$. On retrouve bien la règle de décodage que l'on avait vue en Section 11.2 pour un code BCH binaire de paramètre $\delta = 5$.

Exemple 11.8.2: Cas $\nu = 3$. Le système à résoudre est :

$$\begin{pmatrix} 1 & 0 & 0 \\ P_1^2 & P_1 & 1 \\ P_1^4 & P_3 & P_1^2 \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} = \begin{pmatrix} P_1 \\ P_3 \\ P_5 \end{pmatrix}$$

De même, si $w = 0, 1$ alors le système n'est pas inversible. En effet si $w = 1$ alors $P_3 = P_1^3$ et les deux dernières lignes sont liées. Si $w = 2$ ou 3 alors le système est inversible. On calcule alors :

$$\begin{aligned} \sigma_1 &= P_1 \\ P_3 &= P_1^3 + P_1\sigma_2 + \sigma_3 \\ P_5 &= P_1^5 + P_3\sigma_2 + P_1^2\sigma_3 \end{aligned}$$

donc

$$\begin{aligned} \sigma_2 &= \frac{P_1^2 P_3 + P_5}{P_1^3 + P_3} \\ \sigma_3 &= \frac{P_1 P_5 + P_1^3 P_3 + P_6 + P_1^6}{P_1^3 + P_3} = \frac{P_1 P_5 + P_1^3 P_3}{P_1^3 + P_3} + P_1^3 + P_3 \end{aligned}$$

On peut vérifier facilement que si $w = 2$, on a bien $\sigma_3 = 0$ et on retrouve le polynôme locateur (11.5).