CODAGE DE REED SOLOMON

P. GUERINI, D'APRÈS [HJ]

1. Éléments sur les corps finis

Pour la théorie générale, on pourra se référer à [E] ou à [S] ; voir aussi [C-L].

On travaille dans un corps fini de caractérisrique 2, c.-à-d. dans $\mathbb{F}_q$, où $q = 2^m$ ($m \in \mathbb{N}^\star$).
Pour $m = 1$, $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Et pour $m = 4$, $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$, où $(X^4 + X + 1)$ est l'idéal de $\mathbb{F}_2[X]$ engendré par le polynôme $X^4 + X + 1$. On montre que $\mathbb{F}_{16}$ est un anneau, comme on le fait pour $\mathbb{Z}/n\mathbb{Z}$. Et de même que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier, $\mathbb{F}_{16}$ est un corps car $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Preuve de l'irréductibilité. Le polynôme $X^4 + X + 1$ n'est pas le produit d'un polynôme de degré 1 et d'un polynôme de degré 3 car il n'a pas de racines dans $\mathbb{F}_2$.
S'il est le produit de deux polynômes de degré 2, il s'écrit $(X^2 + bX + \dot{1})(X^2 + \beta X + \dot{1})$. Le coefficient de X^3 est alors $b + \beta$ et celui de X est aussi $b + \beta$. On doit donc avoir $b + \beta = 0$ et $b + \beta = \dot{1}$, ce qui est impossible. □

Le corps $\mathbb{F}_{16}$ est bien de cardinal 16, engendré par la classe de X, notée $\overline{X}$. Ses éléments sont donnés par le tableau suivant :

$\mathbb{F}_{16}$	$\dot{0}$	$\dot{1}$	$\overline{X}$	$\overline{X} + \dot{1}$	$\overline{X}^2$	$\overline{X}^2 + \dot{1}$	$\overline{X}^2 + \overline{X}$	$\overline{X}^2 + \overline{X} + \dot{1}$	$\overline{X}^3$	$\overline{X}^3 + \dot{1}$
Indexation pyfinite	0	1	2	3	4	5	6	7	8	9

$\overline{X}^3 + \overline{X}$	$\overline{X}^3 + \overline{X} + \dot{1}$	$\overline{X}^3 + \overline{X}^2$	$\overline{X}^3 + \overline{X}^2 + \dot{1}$	$\overline{X}^3 + \overline{X}^2 + \overline{X}$	$\overline{X}^3 + \overline{X}^2 + \overline{X} + \dot{1}$
10	11	12	13	14	15

Pour effectuer un produit, on procède par division euclidienne.
Par exemple, dans $\mathbb{F}_2$, $(X^2 + \dot{1})(X^2 + X + \dot{1}) = X^4 + X^3 + X + \dot{1} = X^4 + X + \dot{1} + X^3$. Donc dans $\mathbb{F}_{16}$, le produit de $\overline{X}^2 + \dot{1}$ et de $\overline{X}^2 + \overline{X} + \dot{1}$ est $\overline{X}^3$. Pour Python, cela se traduit par $5 \times 7 = 8$.
Et pour l'inverse, on utilise l'algorithme d'Euclide étendu. Par exemple, $X^4 + X + \dot{1} + (X^2 + X)(X^2 + X + \dot{1}) = \dot{1}$. En réduisant modulo $X^4 + X + \dot{1}$, $(\overline{X}^2 + \overline{X} + \dot{1})^{-1} = \overline{X}^2 + \overline{X}$. En Python, $7^{-1} = 6$.

On note enfin que $(\mathbb{F}_{16}^\star, \times)$ est cyclique, engendré par $\overline{X}$ (c'est un fait général : si $\mathbb{F}_q$ est un corps fini, alors le groupe $(\mathbb{F}_q^\star, \times)$ est cyclique). En particulier, $\overline{X}^{q-1} = \overline{X}^{15} = \dot{1}$ (15 étant l'ordre de $\overline{X}$).

2. Codage de Reed Solomon

Dans toute la suite, on notera $\alpha = \overline{X}$ (élément primitif), $q = 2^p$, $n = q - 1$ et, pour tout $i \in \{1, \dots, n\}$, $x_i = \alpha^{i-1}$. On a $\alpha^n = 1$ et $\mathbb{F}_q = \left\{\dot{0}, \dot{1}, \alpha, \dots, \alpha^{n-1}\right\} = \left\{\dot{0}, x_1, x_2, \dots, x_n\right\}$.
On pose, pour $k \leqslant n$,

$$G = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{k-1} \\ & & & \vdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{k-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{k-1} \\ & & & \vdots & \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \cdots & \alpha^{(k-1)(n-1)} \end{bmatrix} = \left(\alpha^{(i-1)(j-1)}\right)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant k}} \in \mathcal{M}_{n,k}\left(\mathbb{F}_{16}\right).$$

Le message à coder est un vecteur $U = \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{k-1} \end{bmatrix}$, c.-à-d. un polynôme $u(x) = u_0 + u_1 x + \cdots + u_{k-1}x^{k-1} \in \mathbb{F}_{16}[x]$. Son codage est le n-uplet $(u(x_1), \dots, u(x_n))$ c.-à-d. , vectoriellement, $C = GU$.

On définit aussi la matrice de contrôle

$$H = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ & & \vdots & \\ x_1^{n-k} & x_2^{n-k} & \cdots & x_n^{n-k} \end{bmatrix} = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ & & \vdots & \\ 1 & \alpha^{n-k} & \cdots & \alpha^{(n-k)(n-1)} \end{bmatrix} = \left(\alpha^{i(j-1)}\right)_{\substack{1 \leqslant i \leqslant n-k \\ 1 \leqslant j \leqslant n}} \in \mathcal{M}_{n-k,n}\left(\mathbb{F}_{16}\right).$$

On remarque que le produit HG est nul :

Preuve. Pour $1 \leqslant i \leqslant n-k$ et $1 \leqslant j \leqslant k$,

$$\begin{aligned} (HG)_{i,j} &= \sum_{l=1}^{n} h_{i,l}\, g_{l,j} \\ &= \sum_{l=1}^{n} \alpha^{(i-1)(l-1)} \alpha^{j(l-1)} \\ &= \sum_{l=1}^{n} (\alpha^{i+j-1})^{(l-1)} \\ &= \sum_{l=0}^{n-1} (\alpha^{i+j-1})^{l} \\ &= (1 - \alpha^{i+j-1})^{-1}(1 - \alpha^{n(i+j-1)}) \text{ car } 1 \leqslant i+j-1 \leqslant n-1 \text{ et donc } \alpha^{i+j-1} \neq 1 \\ &= 0 \text{ car } \alpha^n = 1. \end{aligned}$$

□

On a donc le résultat important

$$HC = 0.$$

3. Correction d'erreurs par l'arithmétique des polynômes

Le message codé C est transmis (sur CD, par WIFI, etc.) mais peut subir des erreurs. Notons R, le message reçu. On pose $R = C + E$, où E est le vecteur correspondant aux erreurs. On suppose que le nombre maximal d'erreurs, c.-à-d. de coordonnées non nulles de E est au plus $t = \left\lfloor \frac{n-k}{2} \right\rfloor$.

On va voir que dans ce cas, on peut identifier et corriger les erreurs.
On définit le polynôme

$$Q(x, y) = Q_0(x) + yQ_1(x),$$

où $Q_0 \in \mathbb{F}_{16}[x]$ est de degré au plus $l_0 = n - 1 - t$ et $Q_1 \in \mathbb{F}_{16}[x]$ est de degré au plus $l_1 = n - 1 - t - (k - 1) = n - k - t$.
Notons que

- si $n - k$ est pair, $2t = n - k$, $l_1 = t$ et $l_0 + l_1 = n - 1$;
- si $n - k$ est impair, $2t = n - k - 1$, $l_1 = n - k - 1 - (t - 1) = t + 1$ et $l_0 + l_1 = n$.

On montre que l'on peut choisir Q_0 et Q_1 de sorte que pour tout $i \in \{1, \dots, n\}$ $Q(x_i, r_i) = 0$.

Preuve. En notant $a_0, \dots, a_{l_0}$ les coefficients de Q_0 et $b_0, \dots, b_{l_1}$ ceux de Q_1, il s'agit de résoudre

$$\begin{bmatrix} 1 & x_1 & \cdots & x_1^{l_0} & \vdots & r_1 & r_1x_1 & \cdots & r_1x_1^{l_1} \\ & & \vdots & & \vdots & & & \vdots & \\ 1 & x_n & \cdots & x_n^{l_0} & \vdots & r_n & r_nx_n & \cdots & r_nx_n^{l_1} \end{bmatrix} \begin{bmatrix} a_0 \\ \vdots \\ a_{l_0} \\ b_0 \\ \vdots \\ b_{l_1} \end{bmatrix} = 0, \tag{3.1}$$

c.-à-d. de trouver un élément du noyau d'une matrice de taille $n \times l_0 + l_1 + 2$. Comme $l_0 + l_1 + 2 \geqslant n - 1$, il existe bien un élément non nul dans le noyau.
Noter que Q_1 ne peut être le polynôme nul. En effet si c'était le cas, il existerait un élément non nul dans la noyau de la matrice $\begin{bmatrix} 1 & x_1 & \cdots & x_1^{l_0} \\ & & \vdots & \\ 1 & x_n & \cdots & x_n^{l_0} \end{bmatrix}$. Or celle-ci est de rang $l_0 + 1 < n$. □

On considère alors le polynôme $P(x) = Q_0(x) + u(x)Q_1(x)$, de degré $\leqslant n - 1 - t$. Comme le nombre maximal d'erreurs est t, parmi les nombres $x_1, \dots, x_n$, il y en a au moins $n - t$ tels que $r_i = u(x_i)$ et donc $P(x_i) = 0$. Donc P admet plus de racines que son degré maximal et est donc nul. On en déduit que

$$u(x) = -\frac{Q_0(x)}{Q_1(x)},$$

ce qui permet de retrouver C.

4. Décodage par syndromes

On suppose dans cette section que $n - k$ est *pair*.
Le polynôme Q_1 déterminé ci-dessus est appelé *polynôme localisateur des erreurs*. En effet, on a pour tout i,

$$\begin{cases} Q_0(x_i) + r_iQ_1(x_i) = 0 \text{ par définition de } Q_0 \text{ et } Q_1 \\ Q_0(x_i) + c_iQ_1(x_i) = 0 \text{ car } u(x_i) = c_i \end{cases}$$

et si i est un indice tel que $e_i \neq 0$, c.-à-d. $r_i \neq c_i$, on a donc $Q_1(x_i) = 0$. Les indices des erreurs sont donc parmi les indices des racines de Q_1.
Noter que puisque $n - k$ est pair, $l_1 = t$ et donc les t erreurs sont données exactement par les racines de Q_1.

On remarque que, puisque $HC = HGU = 0$, $HR = HE$. On définit alors le vecteur des *syndromes* par la formule

$$S = \begin{bmatrix} S_1 \\ \vdots \\ S_{n-k} \end{bmatrix} = HR,$$

dont la non nullité traduit l'apparition d'erreurs. On a ainsi, pour tout $i \in \{1, \dots, n-k\}$,

$$S_i = \sum_{l=1}^{n} \alpha^{i(l-1)}\, r_l = \sum_{l=1}^{n} r_l\, x_l^i.$$

Le système (3.1) se réécrit $MA+NB = 0$, où $M = \begin{bmatrix} 1 & x_1 & \cdots & x_1^{l_0} \\ & & \vdots & \\ 1 & x_n & \cdots & x_n^{l_0} \end{bmatrix}$ et $N = \begin{bmatrix} r_1 & r_1x_1 & \cdots & r_1x_1^{l_1} \\ & & \vdots & \\ r_n & r_nx_n & \cdots & r_nx_n^{l_1} \end{bmatrix}$.

Soit $K = \begin{bmatrix} x_1 & \cdots & x_n \\ & \vdots & \\ x_1^{l_1} & \cdots & x_n^{l_1} \end{bmatrix} \in \mathcal{M}_{l_1,n}(\mathbb{F}_{16})$ dont on vérifie, comme pour le produit HG de la section 2, que $KM = 0$. On obtient alors $KNB = 0$. Or KN est une matrice de taille $l_1 \times l_1 + 1$ et de terme général

$$(KN)_{i,j} = \sum_{l=1}^{n} x_l^i\, r_l\, x_l^{j-1} = \sum_{l=1}^{n} r_l\, x_l^{i+j-1} = S_{i+j-1}.$$

On a ainsi

$$\begin{bmatrix} S_1 & \cdots & S_{l_1+1} \\ & \vdots & \\ S_{l_1} & \cdots & S_{2l_1} \end{bmatrix} \begin{bmatrix} b_0 \\ \vdots \\ b_{l_1} \end{bmatrix} = 0$$

(noter que puisque $n-k$ est pair, on a $2l_1 = n-k$).
Si B résout ce système, On a $NB \in \operatorname{Ker} K$. Mais comme $KM = 0$, $\operatorname{Im} M \subset \operatorname{Ker} K$. Et de plus, K est de rang l_1, donc $\dim \operatorname{Ker} K = n - l_1$ et M est de rang $l_0 + 1 \underset{n-k \text{ pair}}{=} n - l_1$. Donc $\operatorname{Ker} K = \operatorname{Im} M$. Il existe donc bien un vecteur A tel que $MA = -NB$. Le vecteur B trouvé donne donc bien les coefficients d'un polynôme Q_1.

Grâce aux syndromes, on détermine donc Q_1. Ses racines donnent les indices $i_1, \dots, i_t$ d'apparition des erreurs. On extrait alors du système $HE = S$ le système

$$\begin{bmatrix} x_{i_1} & \cdots & x_{i_t} \\ & \vdots & \\ x_{i_1}^t & \cdots & x_{i_t}^t \end{bmatrix} \begin{bmatrix} e_{i_1} \\ \vdots \\ e_{i_t} \end{bmatrix} = \begin{bmatrix} S_1 \\ \vdots \\ S_t \end{bmatrix}.$$

On détermine ainsi les coordonnées non nulles de E et on retrouve alors C par la formule $C = R + E$.

On peut aussi, en théorie, travailler dans $\mathbb{C}$ en choisissant α égal à une racine primitive $n^{\text{ième}}$ de l'unité.

Références

[C-L] Chambert-Loir A. *De Galois aux corps finis*, Gazette des mathématiciens, 131, 59-68 (janvier 2012).

[E] J-P. Escofier, *Théorie de Galois*, Masson, 1997.

[HJ] T. Høholdt, J. Justesen, *A Course In Error-Correcting Codes*, second edition, EMS Textbooks in Mathematics, 2017.

[S] I. Stewart, *Galois Theory*, Chapman & Hall Mathematics, 1989.