Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Codes correcteurs

1 Codes correcteurs

1.1 Généralités

On considère un corps fini $\mathbb{F}_q$. Le *poids* $w(x)$ d'un vecteur [1] $x \in \mathbb{F}_q^n$ est le nombre de composantes non nulles de x. On a $0 \leq w(x) \leq n$. L'application :

$$\begin{array}{rcl} d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n & \longrightarrow & \mathbb{N} \\ (x, y) & \longrightarrow & w(x-y) \end{array}$$

est une distance (*distance de Hamming*) sur $\mathbb{F}_q^n$.
Un *code linéaire* C de *longueur* n est un sous-$\mathbb{F}_q$-espace vectoriel C de $\mathbb{F}_q^n$.
Les vecteurs $x = (x_1, \cdots, x_n) \in C$ sont les *mots* du code C. Si C est de dimension k sur $\mathbb{F}_q$ le code C possède q^k mots. La *distance minimale* du code C est définie par :

$$d = \min\{w(x)/x \in C \setminus \{0\}\}$$

On dit alors que C est un $[n, k, d]_q$-code [2].

Lemme 1
Soit C un $[n, k, d]_q$-code ; on a $d \leq n + 1 - k$.

$\triangledown$ Soit V le sous-espace vectoriel de $\mathbb{F}_q^n$ formé des vecteurs dont les $k-1$ dernières composantes sont nulles ; V est de dimension $n - k + 1$ et on a $\dim(C) + \dim(V) = n + 1$ de sorte que $C \cap V \neq \{0\}$; si $x \in C \cap V$ on a $w(x) \leq n - k + 1$. $\triangle$

Lemme 2
Soit C un $[n, k, d]_q$-code ; les boules de Hamming fermées centrées sur un mot du code C et de rayon $t = \left[\dfrac{d-1}{2}\right]$ sont deux à deux disjointes.

$\triangledown$ Supposons que $\overline{B}(x_1, t) \cap \overline{B}(x_2, t) \neq \emptyset$ avec $x_1, x_2 \in C$; il existerait $y \in \mathbb{F}_q^n$ tel que $d(x_1, y) \leq t$ et $d(x_2, y) \leq t$ de sorte que $d(x_1, x_2) < d$ d'où $x_1 = x_2$. $\triangle$
Remarque : Lors d'une transmission du mot $c \in C$, *supposons* que le mot reçu $x \in \mathbb{F}_q^n$ vérifie $x \in \overline{B}(c, t)$. Il s'agit d'une propriété du canal de transmission. Ainsi l'erreur de transmission $e = x - c$ vérifie $w(e) \leq t$. Comme c est l'unique mot de C contenu dans $\overline{B}(x, t)$, on peut retrouver c à partir de x.

Une matrice *génératrice* du code C est une matrice $G \in \mathbf{M}_{k,n}(\mathbb{F}_q)$ dont les *lignes* forment une base de C de sorte que C est l'*image* de l'application linéaire *injective* :

$$\begin{array}{rcl} (\mathbb{F}_q)^k & \longrightarrow & (\mathbb{F}_q)^n \\ c & \longrightarrow & c.G \end{array}$$

1. considéré comme vecteur *ligne*
2. ou un $[n, k, d]$-code q-aire.

On a donc [3] :

$$x \in C \Longleftrightarrow \text{ il existe } c \in (\mathbb{F}_q)^k \text{ tel que } x = c.G$$

En particulier la matrice $G \in \mathbf{M}_{k,n}(\mathbb{F}_q)$ est de rang k.
On considère la forme bilinéaire symétrique non dégénérée :

$$\begin{array}{ccc} (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \longrightarrow & \mathbb{F}_q \\ (x,y) & \longrightarrow & \langle x,y\rangle = \displaystyle\sum_{i=1}^{n} x_i y_i \end{array}$$

Le code *dual* d'un code C de dimension k de $(\mathbb{F}_q)^n$ est le code de dimension $n-k$:

$$\check{C} = \{y \in (\mathbb{F}_q)^n \,/\, \langle x,y\rangle = 0 \text{ pour tout } x \in \langle x,y\rangle\}$$

Une matrice de *contrôle* du code C est une matrice génératrice $H \in \mathbf{M}_{n-k,n}(\mathbb{F}_q)$ du code dual $\check{C}$ de sorte que :

$$C = \{x \in (\mathbb{F}_q)^n \,/\, H.{}^{\mathrm{t}}x = 0\}$$

En particulier la matrice $H \in \mathbf{M}_{n-k,n}(\mathbb{F}_q)$ est de rang $n-k$ et l'on a :

$$H.{}^{\mathrm{t}}G = 0$$

Lemme 3
On considère un code C de dimension k dans $\mathbb{F}_q^n$ et une matrice $H \in \boldsymbol{M}_{r,n}(K)$ où K est une $\mathbb{F}_q$-extension de degré fini de degré $m \geq 1$ [4] telle que $C = \{x \in (\mathbb{F}_q)^n \,/\, H.{}^{\mathrm{t}}x = 0\}$. Soit d la distance minimale de C ; pour tout entier $s \in \mathbb{N}$ on a $d > s$ si et seulement si tout ensemble de s colonnes de H est libre sur $\mathbb{F}_q$.

$\triangledown$ Supposons d'abord que tout ensemble de s colonnes de H est libre sur $\mathbb{F}_q$; pour tout mot *non nul* $x = (x_1, \cdots, x_n) \in C$ on a $H.{}^{\mathrm{t}}x = 0$ ce qui s'écrit encore $\displaystyle\sum_{j=1}^{n} x_j\, C_j(H) = 0$ de sorte que $w(x) > s$ et donc [5] $d > s$.
Réciproquement supposons qu'il existe un ensemble de s colonnes de H qui est linéairement dépendant sur $\mathbb{F}_q$. Il existe donc $x = (x_1, \cdots, x_n) \in \mathbb{F}_q^n \setminus \{0\}$ avec $w(x) \leq s$ et $\displaystyle\sum_{j=1}^{n} x_j\, C_j(H) = 0$ de sorte que $H.{}^{\mathrm{t}}x = 0$ et par suite $x \in C$. Il en résulte que $d \leq s$. $\triangle$

Lemme 4
Un $[n,k,d]_q$-code possède une matrice génératrice $G \in \boldsymbol{M}_{k,n}(\mathbb{F}_q)$ de la forme $G = \begin{pmatrix} \mathrm{I}_k & R \end{pmatrix}$ avec $R \in \boldsymbol{M}_{k,n-k}(\mathbb{F}_q)$. De plus $H = \begin{pmatrix} -{}^{\mathrm{t}}R & \mathrm{I}_{n-k} \end{pmatrix} \in \boldsymbol{M}_{n-k,n}(\mathbb{F}_q)$ est une matrice de contrôle de C.

$\triangledown$ Soit G' une matrice génératrice de C ; considérons la *forme échelonnée réduite en lignes* de la matrice $G' \in \mathbf{M}_{k,n}(\mathbb{F}_q)$, il existe $U \in \mathbf{GL}_k(\mathbb{F}_q)$ telle que :

$$G = U\,G' = \begin{pmatrix} \mathrm{I}_k & R \end{pmatrix} \text{ avec } R \in \mathbf{M}_{k,n-k}(\mathbb{F}_q)$$

Comme U est inversible, les applications linéaires :

$$\begin{array}{ccc} (\mathbb{F}_q)^k & \longrightarrow & (\mathbb{F}_q)^n \\ c & \longrightarrow & c.G \\ c' & \longrightarrow & c'.G' \end{array}$$

3. ce qui équivaut encore à ${}^{\mathrm{t}}x = {}^{\mathrm{t}}G.{}^{\mathrm{t}}c$ *ie.* que C est l'image de la matrice ${}^{\mathrm{t}}G \in \mathbf{M}_{n,k}(\mathbb{F}_q)$ de rang k dont les colonnes forment une base de C.
4. par exemple une matrice de contrôle $H \in \mathbf{M}_{n-k,n}(\mathbb{F}_q)$ de C.
5. puisque C est un ensemble fini.

ont la même image et G est une matrice génératrice du code C.
Enfin soit $H = \begin{pmatrix} -{}^tR & \mathrm{I}_{n-k} \end{pmatrix}$; comme G est de rang k, H de rang $n-k$ et que $H.{}^tG = 0$ on a $\mathrm{Im}({}^tG) = \mathrm{Ker}(H)$ donc H est une matrice de contrôle de C. $\triangle$

1.2 Codes cycliques

Un code linéaire $C \subset \mathbb{F}_q^n$ est *cyclique* s'il est stable par le *décalage* :

$$S : (x_1, \cdots, x_{n-1}, x_n) \longrightarrow (x_n, x_1, \cdots, x_{n-1})$$

Considérons l'algèbre (de rang n sur $\mathbb{F}_q$) :

$$\mathcal{R} = \mathbb{F}_q[X]/\langle X^n - 1\rangle$$

On a l'application $\mathbb{F}q$-linéaire bijective :

$$\begin{array}{rccc} \psi : & (\mathbb{F}_q)^n \simeq \mathbb{F}_q[X]_{\leq n-1} & \longrightarrow & \mathcal{R} \\ & x = (x_1 \cdots x_n) \simeq f = x_1 + x_2X + \cdots + x_nX^{n-1} & \longrightarrow \overline{f} = \overline{x_1 + x_2X + \cdots + x_nX^{n-1}} & \end{array}$$

Les codes linéaires C s'identifient donc aux sous-$\mathbb{F}_q$-espaces vectoriels $\psi(C)$ de $\mathcal{R}$.
De plus, on a, pour tout $x \in \mathbb{F}_q^n$:

$$\psi \circ S(x) = \overline{X}\,\psi(x)$$

de sorte que le code C est *cyclique* si et seulement si $\psi(C)$ est un *idéal* de la $\mathbb{F}_q$-algèbre $\mathcal{R}$.
Il existe alors un unique polynôme unitaire $g \in \mathbb{F}_q[X]$, de degré $\leq n-1$, divisant $X^n - 1$ et tel que l'idéal principal $\psi(C)$ de $\mathcal{R}$ soit engendré par $\overline{g}$ (*le polynôme générateur du code*).
Dans l'isomorphisme :

$$\begin{array}{rcc} \mathbb{F}_q[X]_{\leq n-1} & \longrightarrow & \mathcal{R} \\ f = x_1 + x_2X + \cdots + x_nX^{n-1} & \longrightarrow & \overline{f} = \overline{x_1 + x_2X + \cdots + x_nX^{n-1}} \end{array}$$

le sous-espace vectoriel $\psi(C)$ de $\mathcal{R}$ correspond au sous-espace $\langle g\rangle \cap \mathbb{F}_q[X]_{\leq n-1}$ de $\mathbb{F}_q[X]_{\leq n-1}$ de base $(X^i\,g)_{0\leq i\leq n-\deg(g)-1}$ de sorte que C est de dimension $k = n - \deg(g)$. On a ainsi l'application $\mathbb{F}_q$-linéaire *injective* :

$$\begin{array}{rcc} (\mathbb{F}_q)^k \simeq \mathbb{F}_q[X]_{\leq k-1} & \overset{m_g}{\longrightarrow} & \mathbb{F}_q[X]_{\leq n-1} \simeq (\mathbb{F}_q)^n \\ (c_1, \cdots, c_k) \simeq h = \sum_{i=0}^{k-1} c_{i+1}X^i & \longrightarrow f = h\,g = \sum_{j=0}^{n-1} x_{j+1}X^j & \simeq (x_1, \cdots, x_n) \end{array}$$

d'*image* C. Si l'on pose [6] $g = \sum_{i=0}^{n-k} g_iX^i$, on obtient la matrice génératrice suivante du code C :

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & & g_{n-k} & 0 & 0 \\ \vdots & \cdots & & & & & \cdots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & & g_{n-k} \end{pmatrix}$$

Prenons [7] $q = p$. Supposons de plus que p *ne divise pas* n, le polynôme $X^n - 1 \in \mathbb{F}_p[X]$ est alors sans facteurs multiples. Soit m l'ordre de $\overline{p}$ dans $(\mathbb{Z}/\mathbb{Z}n)^\times$; si K est un corps ayant p^m

6. on a $g_{n-k} = 1$ et, puisque $g|X^n - 1$, $g_o \neq 0$.

7. c'est encore vrai pour q puissance quelconque de p, en utilisant la factorisation de $\overline{\Phi_n}$ dans $\mathbb{F}_q[X]$. Les résultats sont analogues à ceux que l'on a établis.

éléments, K contient le groupe (cyclique d'ordre n) $\mu_n(p)$ des racines $n^{\text{ièmes}}$ de l'unité. Si α est un générateur de ce groupe on a alors :

$$g = \prod_{i \in I} (X - \alpha^i)$$

avec $I \subset \{0, 1, \cdots, n-1\}$; les α^i pour $i \in I$ sont appelés les *racines du code* C et l'on a :

$$\psi(C) = \{\overline{f} \,/\, f \in \mathbb{F}_p[X]_{\leq n-1} \text{ et } f(\alpha^i) = 0 \text{ pour tout } i \in I\}$$

Le fait que g soit à coefficients dans $\mathbb{F}_p$ équivaut à ce que $\{\alpha^i / i \in I\}$ soit stable par l'automorphisme de Frobenius $\mathcal{F}_{K/\mathbb{F}_p} : x \longrightarrow x^p$ de K *i.e.* que I soit stable par l'application [8]

$$\begin{array}{ccc} \mathrm{F} : \{0, 1, , \cdots, n-1\} & \longrightarrow & \{0, 1, \cdots, n-1\} \\ i & \longrightarrow & p\,i \bmod n \end{array}$$

Les facteurs irréductibles de $X^n - 1$ dans $\mathbb{F}_p[X]$ correspondent aux parties stables minimales *ie.* aux orbites de l'action de F dans l'ensemble $\{0, 1, \cdots, n-1\}$ (*classes cyclotomiques*) [9].

1.3 Codes BCH - Bose-Chaudhuri-Hocquenghem

On prend $n = p^m - 1$ (avec $m \geq 1$) et K corps fini ayant p^m éléments. On a $K = \mathbb{F}_p[\alpha]$ où $p_{\alpha,\mathbb{F}_p}$ (de degré m) est l'un des facteurs irréductibles de $\overline{\Phi_n}$ dans $\mathbb{F}_p[X]$ de sorte que K^* est le groupe cyclique d'ordre $n = p^m - 1$ engendré par α.
On fixe un entier δ tel que $2 \leq \delta \leq n$, le code *BCH* C de *distance apparente* [10] est le code cyclique de polynôme générateur :

$$g = \prod_{j \in J} (X - \alpha^j)$$

où J est la plus petite partie de $\{0, 1, \cdots, n-1\}$ stable par $F : i \longrightarrow p\,i \bmod n$ et contenant $\{1, \cdots, \delta - 1\}$.
Le code C est de dimension $k = n - \mathrm{Card}(J)$. *Via* l'isomorphisme *canonique* :

$$\begin{array}{ccc} (\mathbb{F}_p)^n & \longrightarrow & \mathbb{F}_p[X]_{\leq n-1} \\ (x_1, \cdots, x_n) & \longrightarrow & f = \displaystyle\sum_{j=0}^{n-1} x_{j+1} X^j \end{array}$$

le code C s'identifie à l'ensemble des polynômes $f \in \mathbb{F}_p[X]$, de degré $\leq n-1$, tels que $f(\alpha^i) = 0$ pour [11] $1 \leq i \leq \delta - 1$. On a ainsi :

$$C = \{x \in (\mathbb{F}_p)^n \,/\, H.{}^{\mathrm{t}}x = 0\} \text{ où } H = (\alpha^{i(j-1)})_{1 \leq i \leq \delta-1,\ 1 \leq j \leq n} \in \mathbf{M}_{\delta-1,n}(K)$$

Lemme 5
Soit d la distance minimale du code C ; on a $d \geq \delta$.

8. on a $\mathcal{F}_{K/\mathbb{F}_p}(\alpha^i) = \alpha^{F(i)}$ pour $0 \leq i \leq n-1$
9. Le polynôme minimal $p_{\alpha,\mathbb{F}_p}$ est l'un de ces facteurs ; c'est l'un des facteurs irréductibles de $\overline{\Phi_n}$ dans $\mathbb{F}_p[X]$
10. ou *distance assignée*.
11. puisque $\mathcal{F}_{K/\mathbb{F}_p}(f(\alpha^i)) = f(\mathcal{F}_{K/\mathbb{F}_p}(\alpha^i))$ la condition est équivalente à $f(\alpha^i) = 0$ pour tout $i \in I$ et donc à $g | f$ puisque les racines de g sont simples.

$\triangledown$ On a $d \geq \delta$ si et seulement si tout ensemble de $\delta - 1$ colonnes de H est libre sur $\mathbb{F}_p$.
Considérons donc $\delta - 1$ colonnes d'indices : $1 \leq d_1 + 1 < \cdots < d_{\delta-1} + 1 \leq n$.
et la matrice $M = (\alpha^{id_j})_{1 \leq i,j \leq \delta-1}$ *extraite* de H. On a :

$$\begin{aligned} \det(M) &= (\alpha^{d_1} \cdots \alpha^{d_{\delta-1}}) \det((\alpha^{(i-1)d_j})_{1 \leq i,j \leq \delta-1}) \\ &= (\alpha^{d_1} \cdots \alpha^{d_{\delta-1}}) \prod_{i<j} (\alpha^{d_i} - \alpha^{d_j}) \neq 0 \end{aligned}$$

puisque α est d'ordre n. $\triangle$
Il s'agit maintenant de décrire l'opération de *correction*. Considérons un mot du code représenté par $f = g\,h \in \mathbb{F}_p[X]_{\leq n-1}$ tel que $f(\alpha^i) = 0$ pour $1 \leq i \leq \delta - 1$; ce mot est brouillé par une erreur représentée par un polynôme $e = \sum_{j=1}^{t} e_j X^{d_j} \in \mathbb{F}_p[X]$ avec $e_j \neq 0$ pour $1 \leq j \leq t$ et $0 \leq d_1 < \cdots < d_t \leq n-1$. On *suppose que* $2t + 1 \leq \delta$. Ainsi le mot *reçu* est représenté par le polynôme $\widetilde{f} = f + e$; il s'agit de retrouver f à partir de $\widetilde{f}$.
Le *syndrôme* de $\widetilde{f}$ est la suite $(S_i)_{1 \leq i \leq \delta-1}$ définie par :

$$S_i = \widetilde{f}(\alpha^i) = e(\alpha^i) = \sum_{j=1}^{t} e_j \alpha_j^i,\ 1 \leq i \leq \delta - 1, \text{ avec } \alpha_j = \alpha^{d_j} \text{ pour } 1 \leq j \leq t$$

On définit alors le *polynôme syndrôme* :

$$S = \sum_{i=1}^{\delta-1} S_i X^{i-1} \in K[X]$$

le *polynôme localisateur d'erreurs*[12] :

$$\sigma = \prod_{j=1}^{t} (1 - \alpha_j X) \in K[X]$$

et le *polynôme évaluateur d'erreurs* :

$$\omega = \sigma \sum_{i=1}^{t} \frac{e_i \alpha_i}{1 - \alpha_i X} \in K[X]$$

Lemme 6 (équation clé)
On a $\deg(\sigma) \leq \frac{\delta-1}{2}$, $\deg(\omega) < \frac{\delta-1}{2}$, *les polynômes* σ *et* ω *sont premiers entre eux et vérifient l'équation clé :*

$$S\sigma \equiv \omega \bmod X^{\delta-1}$$

$\triangledown$ Par définition on $\deg(\sigma) = t \leq \frac{\delta-1}{2}$ et $\deg(\omega) < t \leq \frac{\delta-1}{2}$.
Les racines de σ sont $\dfrac{1}{\alpha_j}$, $1 \leq j \leq t$. Par ailleurs on a :

$$\frac{\sigma}{1 - \alpha_i X} = \prod_{k \neq i} (1 - \alpha_k X) \text{ pour } 1 \leq i \leq t$$

d'où

$$\omega(\frac{1}{\alpha_j}) = c_j x_j (\prod_{k \neq j} (1 - \frac{\alpha_k}{\alpha_j}) \neq 0$$

12. σ est donc le *polynôme réciproque* du polynôme unitaire ayant $\alpha_1, \cdots, \alpha_t$ pour racines.

de sorte que σ et ω sont premiers entre eux. On a enfin :

$$\begin{aligned} S &= \sum_{i=1}^{\delta-1}(\sum_{j=1}^{t} e_j\alpha_j^i)X^{i-1} \\ &= \sum_{j=1}^{t} e_j\alpha_j(\sum_{i=1}^{\delta-1}(\alpha_j X)^{i-1} \\ &= \sum_{j=1}^{t} e_j\alpha_j\frac{1-\alpha_j^{\delta-1}X^{\delta-1}}{1-\alpha_j X} \\ &= \sum_{j=1}^{t}\frac{e_j\alpha_j}{1-\alpha_j X} - \left(\sum_{j=1}^{t}\frac{e_j\alpha_j^{\delta}}{1-\alpha_j X}\right)X^{\delta-1} \end{aligned}$$

de sorte que :

$$\begin{aligned} S\sigma &= \sigma\sum_{j=1}^{t}\frac{e_j\alpha_j}{1-\alpha_j X} - \sigma\left(\sum_{j=1}^{t}\frac{e_j\alpha_j^{\delta}}{1-\alpha_j X}\right)X^{\delta-1} \\ &\equiv \omega \bmod X^{\delta-1} \end{aligned}$$

$\triangle$

Lemme 7
Soient $\widetilde{\sigma}$ et $\widetilde{\omega}$ deux polynômes tel que $\deg(\widetilde{\sigma}) \leq \frac{\delta-1}{2}$, $\deg(\widetilde{\omega}) < \frac{\delta-1}{2}$ *et vérifiant l'équation clé :*

$$S\widetilde{\sigma} \equiv \widetilde{\omega} \bmod X^{\delta-1}$$

il existe $c \in K[X]$ tel que $\widetilde{\sigma} = c\sigma$ et $\widetilde{\omega} = c\omega$. Si, de plus, $\widetilde{\sigma}$ et $\widetilde{\omega}$ sont premiers entre eux, c est une constante non nulle.

$\triangledown$ On a $\omega\widetilde{\sigma} \equiv \widetilde{\omega}\sigma \bmod X^{\delta-1}$ mais $\deg(\omega\widetilde{\sigma} - \widetilde{\omega}\sigma) < \delta - 1$ donc $\omega\widetilde{\sigma} = \widetilde{\omega}\sigma$.
Ainsi ω divise $\widetilde{\omega}\sigma$ mais ω et σ sont premiers entre eux donc ω divise $\widetilde{\omega}$ et l'on a $\widetilde{\omega} = c\omega$ avec $c \in K[X]$. On a alors $\omega\widetilde{\sigma} = \widetilde{\omega}\sigma = c\omega\sigma$ d'où $\widetilde{\sigma} = c\sigma$. $\triangle$

On résout alors l'*équation clé* au moyen de l'*algorithme d'Euclide-Sugiyama* : une variante de l'algorithme d'Euclide étendu appliquée aux polynômes $R_0 = X^{\delta-1}$ et $R_1 = S$.
Soient $(R_k)_{k\geq 0}$ la suite des restes successifs *non nuls* dans l'algorithme d'Euclide étendu ; Δ le *pgcd* de $X^{\delta-1}$ et S, $(U_k)_{i\geq 0}$ et $(V_k)_{i\geq 0}$ les suites telles que

$$R_k = U_k X^{\delta-1} + V_k S$$

Supposons que $\deg(\Delta) \geq t$; on aurait alors $X = X^s|S$ avec $s \geq t$ et par suite $X^t|S = \sum_{i=1}^{\delta-1} S_i X^{i-1}$ d'où $S_1 = \cdots = S_t = 0$ et finalement on aurait :

$$e(\alpha^i) = \sum_{j=1}^{t} e_j\alpha^{id_j} = 0 \text{ pour } 1 \leq i \leq t$$

Les coefficients $e_1, \cdots, e_t$ seraient ainsi les *solutions du système linéaire* de matrice $M' = (\alpha^{id_j})_{1\leq i,j\leq t}$. Mais on a :

$$\begin{aligned} \det(M') &= (\alpha^{d_1}\cdots\alpha^{d_t})\det((\alpha^{(i-1)d_j})_{1\leq i,j\leq t}) \\ &= (\alpha^{d_1}\cdots\alpha^{d_t})\prod_{i<j}(\alpha^{d_i} - \alpha^{d_j}) \neq 0 \end{aligned}$$

puisque α est d'ordre n. On aurait donc $e_1 = \cdots = e_t = 0$ *ie.* $e = 0$.
Ainsi $\deg(\Delta) < t \leq \frac{\delta-1}{2}$; il existe un *plus grand entier* k tel que :

$$\deg(R_{k-1}) \geq \frac{\delta - 1}{2}$$

et l'on a :

$$R_k = U_k X^{\delta-1} + V_k S$$

de sorte que $SV_k \equiv R_k \bmod X^{\delta-1}$. Mais on a :

$$\deg(R_k) < \frac{\delta-1}{2} \text{ et } \deg(V_k) = \delta - 1 - \deg(R_{k-1}) \leq \frac{\delta-1}{2}$$

Il existe donc $c \in K[X]$ tel que $V_k = c\,\sigma$ et $R_k = c\,\omega$ et l'on a :

$$\begin{aligned} R_k &= c\omega \\ &= c\left(S\,\sigma + W\,X^{\delta-1}\right) \\ &= U_k X^{\delta-1} + V_k\,S \\ &= U_k X^{\delta-1} + c\sigma\,S \end{aligned}$$

d'où :

$$U_k = c\,W$$

Ainsi c divise U_k et V_k qui sont *premiers entre eux* donc $c \in K^*$ et puisque $\sigma(0) = 1$ on a :

$$c = V_k(0)$$

et finalement on a :

$$\sigma = \frac{1}{V_k(0)} V_k \text{ et } \omega = \frac{1}{V_k(0)} R_k$$

On détermine alors (*eg.* par essais systématiques) les racines $\dfrac{1}{\alpha_j} = \alpha^{-d_j}$, $1 \leq j \leq t$, de σ. On en déduit, par un calcul de *logarithme discret*, les *positions* d_j, $1 \leq j \leq t$, des erreurs.
On détermine alors ces erreurs à l'aide du polynôme *évaluateur* ω en utilisant les formules de Forney.

Lemme 8 (formules de Forney)
On a $e_j = -\dfrac{\omega(\alpha^{-d_j})}{\sigma'(\alpha^{-d_j})}$ *pour* $1 \leq j \leq t$.

$\triangledown$ Rappelons que :

$$\sigma = \prod_{j=1}^{t}(1 - \alpha_j X) \quad \text{et} \quad \omega = \sigma \sum_{i=1}^{t} \frac{e_i \alpha_i}{1 - \alpha_i X}$$

On a, en considérant la *dérivée logarithmique* de σ :

$$\sigma' = -\sigma \sum_{i=1}^{t} \frac{\alpha_i}{1 - \alpha_i X}$$

de sorte que :

$$\frac{\omega}{\sigma'} = -\frac{\displaystyle\sum_{i=1}^{t} \frac{e_i \alpha_i}{1 - \alpha_i X}}{\displaystyle\sum_{i=1}^{t} \frac{\alpha_i}{1 - \alpha_i X}}$$

Pour $1 \leq j \leq t$, on a alors :

$$\frac{\omega}{\sigma'} = -\frac{e_j\alpha_j + \sum_{i\neq j} e_i\alpha_i \dfrac{1-\alpha_j X}{1-\alpha_i X}}{\alpha_j + \sum_{i\neq j} \alpha_i \dfrac{1-\alpha_j X}{1-\alpha_i X}}$$

et en prenant la valeur en α^{-d_j} des deux membres on obtient :

$$-\frac{\omega(\alpha^{-d_j})}{\sigma'(\alpha^{-d_j})} = e_j$$

$\triangle$