Cours : Codes correcteurs

Emily Clement
Enseignant : Delphine Boucher

Master 1 de Mathématiques
Semestre 2
2015-2016

Table des matières

Chapitre 1

Généralités sur les codes correcteurs

Ce cours comportera trois notes : un contrôle au retour des vacances de février, un TP noté et un contrôle à la fin de l'année, tous affecté du même coefficient.
Bibliographie :

- Mathématiques appliquées, L3, Pearson, chapitre 7. (On a un chapitre aussi de cryptographie dedans)
- Introduction to Coding Theory, Ronald Roth.

Exemple 1.1.
On utilise des turbo-codes pour la mission Rosetta (ESA, Europear Space Agency), concurrent des turbo-codes : codes LDPC.
Disques compacts : Codes de ***Reed-Solomon****.*
Télévision à satellite : DVC. S2 (Digital Vidéa Broadcasting) : on utilise des codes LDPC + ***BCH****.*
Billet de banque, code ISBN, code sécurité sociale etc.
Les codes en gras seront ceux que l'on va étudier.

I Codes correcteurs : principe

Soit A un alphabet fini, et soit q son cardinal.

Définition 1.1 (Codes)**.**

Un **code** $(n, M)_q$ défini sur A est un ensemble non vide de A^n ayant M éléments.
On appelle n la longueur du code.
et M sa taille, ou son cardinal.
On peut avoir un autre paramètre : le log cardinal.
On appelle **log cardinal** la quantité, qui n'est pas forcément un entier :

$$k \overset{\text{def}}{=} \log_q(M)$$

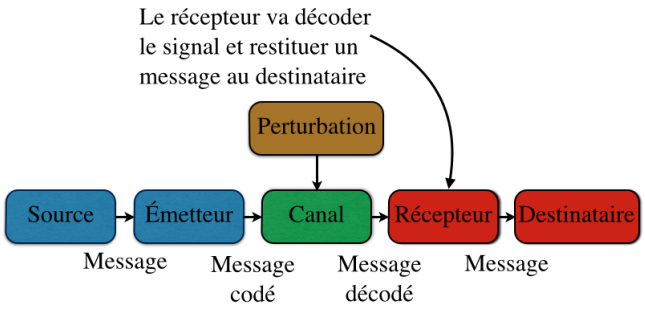
Autre notation pour un tel code : $[n, k]_q$

Définition 1.2 (Rendement, ou taux d'information du code)**.**

Le **rendement** ou taux d'information du code est $R = \dfrac{k}{n}$.

Quand k n'est pas un entier on trouve parfois l'écriture $R = \dfrac{\lceil k \rceil}{n}$.

Principe :



Soit C un code $[n, k]_q$.
On suppose que k est un **entier** si bien que C possède q^k éléments.
On considère un message que l'on couple en "morceau"de longueur k, et on considère chaque "morceau"individuellement.
On construit une application injective $\phi : A^k \rightarrow A^n$ telle que $\phi\left(A^k\right) = C$
On considère $c = \phi(m)$, et on envoie c.

$$\text{Source} \quad m \underset{\text{encodage}}{\mapsto} c = \phi(m) \underset{\text{bruit}}{\rightarrow} y \underset{\text{décodage}}{\rightarrow} c' \overset{?}{=} c, m?$$

On reçoit un mot y et on cherche c' dans C, le plus "proche"de y.
La quantité $n \cdot k$ est appelé **redondance**.

Exemple 1.2.
Si on reçoit 1101 *au lieu de* 1001.
On peut faire que de redondance :

$$1001 \quad \mapsto \quad 10011001 \quad \underset{\textit{Réception}}{\rightarrow} \quad 10001001$$

On ne peut pas corriger l'erreur là : est-ce un 1 *ou un* 0 *?*

On doit définir pour cela la notion de distance entre les mots de A^n.
Dans la suite on supposera que A est un **corps fini**, qu'on notera F

Définition 1.3 (Distance de Hamming – 1940)**.**

Soit $n \in \mathbb{N}^*$, soit $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ dans F^n.
Le **poids** de x est $w(x) = \text{Card } (\{i \in [\![1, n]\!], x_i \neq 0\})$
La **distance de Hamming** de x à y est $d_H(x, y) = w(x - y)$

Proposition 1.1.

La distance de Hamming est une distance, *ie.* elle vérifie :

1. $\forall x, y \in F^n$, $d_H(x, y) \geqslant 0$
2. $\forall x, y \in F^n$, $d_H(x, y) = 0 \Leftrightarrow y = x$
3. $\forall x, y \in F^n$ $d_H(x, y) = d_H(y, x)$
4. Inégalité triangulaire : $\forall x, y, z \in F^n$, $d_H(x, y) \leqslant d_N(x, z) + d_H(z, y)$

Démonstration.
Montrons le quatrième point : $\forall a, b \in F^n$ $w(a + b) \leqslant w(a) + w(b)$
Soient $a, b \in F^n$ $w(a + b) = \#\{i \in [\![1, \ldots, n]\!], a_i + b_i \neq 0\}$
Or $\forall i \in [\![1, n]\!]$ $a_i + b_i \neq 0 \Rightarrow a_i \neq 0$ ou $b_i \neq 0$
Donc $\{i | a_i + b_i \neq 0\} \subset \{i | a_i \neq 0\} \bigcup \{a | b_i \neq 0\}$
Donc $w(a + b) \leqslant w(a) + w(b)$
Soient $x, y, z \in F^n$:

$$w((y - z) - (x - z)) \leqslant w(x - z) + w(z - y)$$

□

Définition 1.4 (Distance minimale).

La **distance minimale** d'un code C est :

$$d = \min_{c,c' \in C, c \neq c'} d_H(c, c')$$

Nouvelle notation du code C :

$$(n, M, d)_q \quad [n, M, d]_q$$

Définition 1.5 (Taux de correction).

Le taux de correction est $r_0 = \frac{d}{n}$

Proposition 1.2.

Soit C un code $[n, k, d]_q$
Soit $c \in C$ et soit $Y \in F^n$ tel que :

$$d_H(y, c) \leqslant \lfloor \frac{d-1}{2} \rfloor$$

on dit que $t = \lfloor \frac{d-1}{2} \rfloor$ est la capacité de correction du code.

Démonstration.
Soit $c' \in C$ tel que $d_H(y, c') \leqslant \lfloor \frac{d-1}{2} \rfloor$
Par l'inégalité triangulaire :

$$d_H(c, c') \leqslant d(c, y) + d(y, c') < d$$

Or d est la distance minimale de C donc $d_H(c, c') = 0$ donc $c = c'$ □

Proposition 1.3.

Soit C un code $[n, k, d]_q$ soit $c \in C$ et soit $y \in F^n$ tel que $d_H(c, y) \leqslant d - 1$.
Alors $y = c$ ou $y \notin C$.

Démonstration.
Si $y \in C$ et $y \neq c$ alors par définition de d :

$$d_H(y, c) \geqslant d$$

□

Exemple 1.3.
$A = F = \mathbb{F}_2$

1. $\phi : \begin{array}{ccc} A^k & \to & A^{2k} \\ m & \mapsto & (m|m) \end{array}$, $C = \phi\left(A^k\right)$
   rendement : $\dfrac{1}{2}$
   Taux de correction ?
   Si on prend $c_1 = (10\ldots0|10\ldots0) \in C$ *et* $c_2 = (0\ldots0|0\ldots0) \in C$
   $d_H(c_1, c_2) = 2$
   Soient $m, m' \in A^k$, $c = (m|m)$ *et* $c' = (m'|m')$

$$\begin{aligned} w(c - c') &= w((m - m'|m - m')) \\ &= 2 \cdot w(m - m') \\ &\equiv 0\,[2] \end{aligned}$$

   donc $d = 2$, $r = \dfrac{2}{n}$
   Exemple :

$$10011001 \mapsto 10001001$$

   on ne peut pas corriger...
2. *Un exemple plus fort mais avec un moins bon rendement :*

$$\phi : \begin{array}{ccc} A^k & \to & A^{3k} \\ m & \mapsto & (m|m|m) \end{array}$$

   , $C = \phi\left(A^k\right)$
   Rendement : $\dfrac{1}{3}$
   Si on prend $c_1 = (10\ldots0|10\ldots0) \in C$ *et* $c_2 = (0\ldots9|0\ldots0) \in C$
   $d_H(c_1, c_2) = 3$
   Soient $m, m' \in A^k$, $c = \phi(m)$ *et* $c' = \phi(m')$
   $w(c - c') = 3w(m - m') = 0\,[3]$ *don* $d = 3$
   On peut corriger 1 *erreurs, et* ***détecter*** 2 *erreurs.*
   $r = \dfrac{3}{n}$ *le taux de correction n'a pas bougé, c'est* t *qui a changé.*

3. $\phi : \begin{array}{ccc} A^k & \to & A^{k+1} \\ m & \mapsto & (m|m_1 + \cdots + m_k) \end{array}$

$C = \phi\left(A^k\right)$ *code de parité.*

$R = \dfrac{k}{k+1}$

Si on prend $(0 \ldots 0|0) \in C$ *et* $(1\,0 \ldots 0|1) \in C$ *donc* $d \leqslant 2$.

Soient $m, m' \in F^k$

$c = (m|t)$ *avec* $t = m_1 + \cdots + m_k$ *et* $c' = (m'|t')$ *avec* $t' = \sum_{i=1}^{k} m'_i$

$$c - c' = (m - m'|t - t')$$

On a plusieurs cas :

si $m = m'$ *alors* $t = t'$ *et* $c = c'$

si $m \neq m'$ $w(m - m') \geqslant 1$

— *Si* $w(m - m') \geqslant 2$ *alors* $w(c - c') \geqslant 2$

— $w(m - m') = 1$ *alors* $t \neq t'$ *donc* $w(c - c') = 2$

Objectif :

1. Construire des codes de longueurs arbitrairement grande avec un taux d'information et un taux de correction élevé.
2. Construire des algorithmes de corrections d'erreurs qui soient efficaces (complexité en temps polynomial.)

On a besoin de plus de structures : on va introduire les codes linéaires.

II Codes linéaires.

Définition 1.6 (Codes linéaires)**.**

Soit k, n des entiers tels que $k \leqslant n$
Un code linéaire sur F de longueur n et de dimension k est un sous-espace vectoriel de F^n de dimension k sur F.
Dit autrement, $C = \phi\left(F^k\right)$ où ϕ est injective et linéaire.
La matrice de ϕ par rapport aux bases canoniques de F^k et F^n (notées en colonnes) est une matrice $n \times k$ de rang k.
La transposée de cette matrice est une matrice génératrice de C.
Ses lignes forment une base de C.

$$C = \left\{m \cdot G | m \in F^k\right\}$$

m est une matrice $1 \times k$ et G une matrice $k \times n$.
où G est la matrice génératrice de C.
$G \in \mathcal{M}_{k,n}(F)$,$\mathrm{Rg}(G) = k$
G possède un sous-déterminant d'ordre k non nul.

Remarque 1.1.

Si C possède une matrice génératrice sous la forme $G = \left(I_k | \underbrace{A}_{n-k}\right)$, on dit que G est sous forme systématique.

Propriétés 1.1.

Soit C un code linéaire $[n, k, d]_q$, $d = \min\limits_{c \in C, c \neq 0} w(c)$

Démonstration.
Soit $c \in C$ $c \neq 0$ $w(c) = d_H(c, 0) \geqslant d$ car $0 \in C$ car C est un espace-vectoriel.
Soit $c_1, c_2 \in C$ tel que $d_H(c_1, c_2) = d$ (ces deux mots existent par définition de la distance minimale)
Soit $c = c_1 - c_2$, $c \in C$ car C est linéaire.

$$w(c) = d$$

□

Théorème 1.1 (Borne de Singleton)**.**

Pour un code linéaire $[n,k,d]_q$ on a

$$d \leqslant n-k+1$$

C'est vrai aussi pour les codes **non-linéaires** (on verra la preuve en TD)

Démonstration.

Preuve longue matricielle Soit G une matrice génératrice de C.
$G \in \mathcal{M}_{n,k}(F)$ et $\mathrm{Rg}(G) = k$
Soient $G_1, \dots, G_n$ les colonnes de G.
Soient $j_1, \dots, j_k \in [\![1,n]\!]$ distincts 2 à 2, tels que : $\Delta = (G_{i_1}|\dots|g_{i_k})$ est inversible (possible car $\mathrm{Rg}(G) = k$.) la matrice $\Delta^{-1} \cdot G = (C_1, \dots, C_i \dots)$
a ses colonnes : $C_{j_i} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ avec 1 en position i.
Soit

$$\begin{aligned} c &= \underbrace{(1,0,\dots,0) \cdot \Delta^{-1} \cdot G}_{\in C} \\ &= \left(?\dots?, \underset{\uparrow}{1}_{j_1}, ?, \dots, ?, \underset{\uparrow}{0}_{j_2}, 0 \dots, \underset{\uparrow}{0}_{j_k}, ?, \dots, ? \right) \end{aligned}$$

On a : $\begin{cases} w(c) \geqslant 1 \\ w(c) \leqslant n-k+1 \end{cases}$
Donc c est un mot de code non nul de poids inférieur à $n-k+1$.
donc :

$$d \leqslant n-k+1$$

Preuve plus rapide et élégante On regarde pour E un espace vectoriel des éléments de F^n ont les $k-1$ premières coordonnées sont nulles.

$$\dim E = n - (k-1) = n - k + 1$$

donc $\dim(E) + \dim(C) = n + 1 > \dim F^n$ donc $E \bigcap C \neq \varnothing$ donc E Et C ne sont pas en somme directe, d'où le résultat : C possède un mot non nul de poids inférieur ou égal à $n - k + 1$.

□

Remarque 1.2.
*Les codes tels que $d = n - k + 1$ sont des codes **MDS** : Maximum Distance Separable, ce sont des codes optimaux.*
Par exemple les codes de Reed-Solomon (1960) sont MDS.

Attention, on écrit plus les vecteur en colonne mais en ligne ! $C\left\{m \cdot G, m \in \mathbb{F}_q^k\right\}$ $G \in \mathcal{M}_{k,n}(\mathbb{F}_q)$, de rang k.

Définition 1.7 (Code dual)**.**

Soit C un code linéaire $[n,k]_q$, le **dual** de C est :

$$C^\perp \overset{\text{def}}{=} \left\{x \in \mathbb{F}_q^n \, \forall c \in C, \langle x, c\rangle = 0\right\}$$

où $\forall x, y \in \mathbb{F}_q^n, \langle x, y\rangle \overset{\text{def}}{=} \sum_{i=1}^{n} x_i y_i$ (produit scalaire euclidien).
Une **matrice de contrôle** de C est une matrice génératrice de $C^\perp$.

Remarque 1.3.

$$\begin{aligned} C^\perp &= \left\{x \in \mathbb{F}_q^n, \forall c \in C, c \cdot {}^t x = 0\right\} \\ &= \left\{x \in \mathbb{F}_q^n, G^t x = 0\right\} \end{aligned}$$

Or $Rg(G) = k$ car $\dim C = k$ donc d'après le théorème du rang, $\dim(\ker(G)) = n - k$ *donc* $\dim\left(C^\perp\right) = n - k$.
Notons H une matrice de contrôle de C, $H \in \mathcal{M}_{n-k,n}(\mathbb{F}_q)$ et $Rg(H) = n - k$
$G \cdot {}^t H = 0$ *et* $H \cdot {}^t G = 0$

Définition 1.8.

Un code linéaire C est auto-dual si $C = C^\perp$

Propriétés 1.2.

Soit C un code linéaire $[nk]_q$ et soit H une matrice de contrôle de C.

$$C = \left\{x \in \mathbb{F}_q^n | H \cdot^t x = 0\right\}$$

La quantité $H \cdot^t x$ est appelée **syndrome** de c, **Notation :** $S(x) = H \cdot^t x$

Démonstration.
On a que :

$$\mathrm{Rg}(H) = n - k \text{ et } \dim(\ker(H)) = k$$

Donc $\dim(C) = \dim\left(\left\{x \in \mathbb{F}_q^n | H \cdot^t x = 0\right\}\right)$ Soit G une matrice génératrice de C telle que $H \cdot^t G = 0$, on a $\forall x \in C, \exists m \in (\mathbb{F}_q)^k \; x = m \cdot G$
Soit $x \in C$ soit $m \in \mathbb{F}_q^k$ tel que $x = mG$ alors $H \cdot^t x = H \cdot \left({}^t \cdot^t m\right) = 0$ car $H \cdot^t G = 0$
Donc $C \subset \left\{x \in \mathbb{F}_q^n | \, H \cdot^t x = 0\right\}$ l'autre inclusion vient par égalité de dimension des espaces. □

Remarque 1.4.

Si $G = \left(I_k | \underset{n-k}{\underset{\leftrightarrow}{M}}\right)$ *est une matrice génératrice de* C.
Alors $H = \left(-\left({}^t M\right) | \, I_{n-k}\right)$ *est une matrice de contrôle de* C :
En effet :

- $H \in \mathcal{M}_{n-k,n}(\mathbb{F}_q)$
- $Rg(H) = n - k$
- $H \cdot^t G = \left(-{}^t M \quad | \quad I_{n-k}\right) \cdot \left(\begin{array}{c} I_k \\ \hline {}^t H \end{array}\right) = -{}^t M \cdot I_k + I_{n-k} \cdot^t M = 0$

Théorème 1.2.

Soit C un code linéaire $[n, k, d]_q$ et soit H une matrice de contrôle de C.
H possède d colonnes linéairement dépendantes et tout ensemble de $w < d$ colonnes de H sont linéairement **indépendantes**

Démonstration.
$d = \min_{c\neq 0, c\in C} w(c)$.
Soit c un mot de C de poids $w \neq 0$, on a :

$$H \cdot^t c = 0$$

donc $\sum_{j=1}^{w} c_{i_j} H_{i_j} = 0$ où H_i désigne le i-ème colonne de H et $c = \left(0, \ldots, 0, \underset{\shortparallel}{c_{i_1}}, 0 \ldots, \underset{\shortparallel}{c_{i_w}}, \ldots 0 \right)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad 0 \qquad\qquad\quad 0$
L'indépendance linéaire vient avec le caractère minimal de d ! □

Exemple 1.4.

1. $\phi : \begin{array}{ccc} \mathbb{F}_2^k & \to & \mathbb{F}_2^{2k} \\ m & \mapsto & (m|m) \end{array}$ $C = \phi\left(\mathbb{F}_2^k\right)$
   Matrice génératrice $G = (I_k|I_k)$
   Matrice de contrôle $H = (I_k|I_k)$
   $G = \left(\underset{k}{\overset{\leftrightarrow}{A}} | \underset{n-k}{\overset{\leftrightarrow}{B}}\right)$
   $mG = (mA|mB)$
   $$A = I \Leftrightarrow mA = m$$

   H n'a pas de colonne nulle donc pas de mot de poids 1.
   $H_1 = H_{k+1}$ *donc* $(1, 0 \ldots 0, 1, 0 \ldots 0) \in C$
   donc $d = 2$
2. $\phi : \begin{array}{ccc} \mathbb{F}_2^k & \to & \mathbb{F}_2^{2k} \\ m & \mapsto & (m|m|m) \end{array}$
   $G = (I_k|I_k|I_k)$ *et* $H = \begin{pmatrix} I_k & | & I_{2k} \\ I_k & | & \end{pmatrix}$
   Pas de colonne nulle : pas de mot de poids 1
   Colonnes distinctes : pas de mot de poids 2.
   $H_1 + H_{k+1} + H_{2k} = 0$ *donc* $d = 3$
3. $\phi : \begin{array}{ccc} \mathbb{F}_2^k & \to & \mathbb{F}_2^k \\ m & \mapsto & (m|m_1 + \cdots + m_k) \end{array}$
   $C = \phi\left(\mathbb{F}_2^k\right)$ *code de parité.*

$$G = \begin{pmatrix} & & 1 \\ & & 1 \\ & I_k & \vdots \\ & & 1 \end{pmatrix} \text{ et } H = (1 \cdots 1|1)$$

donc $d = 2$ donc c'est un code MDS.
*$C^\perp$ est appelé **code de répétition**, c'est aussi un code MDS (borne de singleton appliquée sur $C^\perp$.*

4. $C = \left\{mG | m \in \mathbb{F}_2^k\right\}$ *où* $G = \begin{pmatrix} & & 1 & 0 & 0 & 1 \\ & & 0 & 1 & 0 & 1 \\ & I_4 & 1 & 0 & 1 & 0 \\ & & 0 & 1 & 1 & 0 \end{pmatrix}$

Une matrice de contrôle est $H = \begin{pmatrix} 1 & 0 & 1 & 0 & & \\ 0 & 1 & 0 & 1 & & \\ 0 & 0 & 1 & 1 & & I_4 \\ 1 & 1 & 0 & 0 & & \end{pmatrix}$

$d = 3$
$\begin{cases} \forall i, H_i \neq 0 \\ \forall i \neq j, H_i + H_j \neq 0 \\ H_1 + H_5 + H_8 = 0 \end{cases}$

5. $C = \left\{mG | m \in \mathbb{F}_2^4\right\}$ $R = 4/7$

$G = \begin{pmatrix} & & 0 & 1 & 1 \\ & I_4 & 1 & 0 & 1 \\ & & 1 & 1 & 0 \\ & & 1 & 1 & 1 \end{pmatrix}$ $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

$$\begin{cases} \forall i, H_i \neq 0 \\ \forall i \neq j, H_i \neq H_j \\ H_1 + H_4 + H_5 = 0 \end{cases}$$

donc $d = 3$

III Décodage des codes linéaires (premières techniques)

Soit C un code linéaire $[n, kd]_q$
La question que l'on se pose est la suivante :

$$\text{soit } y \in \mathbb{F}_q^n \text{ on veut trouver } c \in C \text{ tel que } d_H(c, y) = \min_{x \in C} d(y, x)$$

Il est possible de trouver plusieurs $c \in C$ vérifiant cette propriété (décodage par liste)
Autre formulation : soit $y \in \mathbb{F}_q^n$ trouver $e \in \mathbb{F}_q^n$ de poids minimum tel que $y - e \in C$
Moyen :

— décodage par tableau standard.
— Amélioration en terme de complexité : Décodage par syndrome.

1 Décodage par tableau standard

Soit $\mathcal{R}$ la relation définie sur $\mathbb{F}_q^n$ par :

$$\forall x, y \in \mathbb{F}_q^n, x\mathcal{R}y \Leftrightarrow y - c \in C$$

$\mathcal{R}$ est une relation d'équivalence, on appelle **coset** de $c \in \mathbb{F}_q^n$ la quantité $x + c$
Un **coset leader** est un mot de plus petit poids dans un **coset**
Un **tableau standard** est un tableau qui a q^{n-k} ligne et q^k colonnes construit comme suit :

1. La première ligne est formée par les mots de C en commençant par 0.
2. Chaque ligne commence par un mot e de $\mathbb{F}_q^n$ de poids minimum qui n'apparaît pas sur les lignes précédentes, on complète la ligne par les $e + c$ où c décrit $C - \{0\}$ **dans le même ordre que celui imposée par la première ligne.**

Exemple 1.5 (Exemple de calcul de tableau standard)**.**
Soit C le code $[5, 2]_2$ de matrice génératrice $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

00000	10110	01011	11101
10000	00110	11011	01101
01000	11110	00011	10101
00100	10010	01111	11001
00010	10100	01001	11111
00001	10111	01010	11100
11000	01110	10011	00101
01100	11010	00111	10001
10001	00111	11010	01100

On a bien 8 lignes, et 2^2 colonnes, on peut s'arrêter.
On cherche dans ce tableau le mot y reçu, et on cherche le coset leader correspondant et la différence entre les deux est le mot de code le plus proche.

Algorithme 1.1 (Décodage par tableau standard)**.**

Principe :
Soit $y \in \mathbb{F}_q^n$ on cherche la ligne (ou coset) qui contienne y.
Soit e le premier élément de la ligne (coset leader), *ie* c'est un mot de plus petit poids tel que $y - e \in C$.
Alors $c = y - e$ est **un** mot de code le plus proche de y. (on a pas nécessairement unicité)

Propriétés 1.3 (Unicité du décodage)**.**

Il existe au plus **un** coset leader de poids $\leqslant \lfloor \frac{d-1}{2} \rfloor$ dans un coset.

Démonstration.
Soient x_1, x_2 tels que $w(x_1) \leqslant \lfloor \frac{d-1}{2} \rfloor$ et $w(x_2) \leqslant \lfloor \frac{d-1}{2} \rfloor$ et $x_1 - x_2 \in C$
Alors $w(x_1 - x_2) \leqslant w(x_1) + w(-x_2) < d$ donc $x_1 = x_2$ □

2 Décodage par syndrome.

Soit H une matrice de contrôle de C.
Soient $x, y \in \mathbb{F}_q^n$ on a :

$$x \mathcal{R} y \Leftrightarrow H \cdot^t x = H \cdot^y$$

(On rappelle qu'on note le syndrome de x $H \cdot^t x =: S(x)$) En effet :

$$\begin{aligned} x \mathcal{R} y &\Leftrightarrow y - x \in C \\ &\Leftrightarrow H \cdot^t (y - x) = 0 \\ H \cdot^t x &= H \cdot^t y \end{aligned}$$

Construction du tableau :

1. Sur la première ligne on a le mot nul et son syndrome. (vecteur nul)
2. Chaque ligne suivante commence par un mot de plus petits poids dont le syndrome n'apparaît pas dans le tableau.

Exemple avec : $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ et $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

e, coset leader	${}^tS(e)$
00000	000
10000	110
01000	011
00100	100
00010	010
00001	001
11000	101

on calcule le syndrome de 11000, on trouve 101 comme syndrome, il n'est pas dans le tableau, on l'ajoute.
idem avec 10100, on trouve 010, il est dans le tableau, on ne l'ajoute pas...

Algorithme 1.2 (Décodage par syndrome)**.**

Soit $y \in \mathbb{F}_q^n$. on calcule $S = H \cdot {}^t y$, on cherche dans le talbeau un coset leader e de syndrome S.
Alors $y - e$ est un mort le plus proche de y.

Exemple 1.6.
Soit $y = (1, 1, 0, 0, 1) \in \mathbb{F}_2^5$.
Le syndrome de y *est :*

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Le coset leader du tableau ayant le même syndrome est $(0, 0, 1, 0, 0)$ *donc un mot de code le plus proche est* $c = (1, 1, 1, 0, 1)$
Il y a unicité de ce mot de code le plus proche car $w(e) \leqslant \lfloor \frac{3-1}{2} \rfloor$

IV Codes de Hamming

But : Construire une famille infinie de codes linéaire $1-$correcteurs d'erreurs.

Idée : on prend $2^r - 1$ colonnes, et r lignes, les vecteurs sont de $(\mathbb{F}_2)^r \setminus \{0\}$
Soit r un entier non nul, soit $n = 2^r - 1$
Le codes de Hamming H_r de longueur n et le code binaire linéaire de matrice de contrôle $H \in \mathcal{M}_{r,n}(\mathbb{F}_2)$ dont les n colonnes sont les n vecteurs non nuls de $(\mathbb{F}_2)^r$ rangés dans un certain ordre.
$C = \left\{mG, m \in \mathbb{F}_2^k\right\} = \left\{c \in \mathbb{F}_2^n | H \cdot {}^t x = 0\right\}$ Soit $j \in [\![1, n]\!]$ la $j-$ème colonne de H est $\begin{pmatrix} \overline{\varepsilon_1^{(j)}} \\ \vdots \\ \overline{\varepsilon_r^{(j)}} \end{pmatrix}$
où les $\varepsilon_1^{(j)}$ sont définis à l'aide de la décomposition en base 2 de j.

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

$j = \sum_{i=0}^{r-1} \underbrace{\varepsilon_{r-i}^{(j)}}_{\in\{0,1\}} 2^i$.
Les colonnes de H sont non nulles et distinctes 2 à 2. ($i \neq j \Rightarrow \left(\varepsilon_1^{(j)} \cdots \varepsilon_r^{(j)}\right) \neq \left(\varepsilon_1^{(i)} \cdots \varepsilon_r^{(i)}\right)$)
De plus $(1, 1, 1, 0 \cdots, 0) \in \mathcal{H}_r$ donc la distance minimale de $\mathcal{H}_r$ est 3.

$$\mathrm{Rg}(H) = r$$

Donc $\mathcal{H}_r$ est un code $[2^r - 1, 2^r - 1 - r, 3]$.

$$M = 2^k$$

$(n, M, d) = [n, k, d]$ avec $k = \log_q(M)$

Exemple 1.7.

$\mathcal{H}_3$ est définie par $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

Décodage :
Soit $c \in C$ soit $y \in \mathbb{F}_2^n$ tel que $d(y, c) \leqslant 1$.

On veut retrouver c connaissant y.
Soit $S = H \cdot^t y$.
Si $S = 0$ alors $y \in C$ et $c = y$.
Si $S \neq 0$ alors c est tel que $d(y, c) = 1$.
Donc $y = c + e$ où $e \in \mathbb{F}_2^n$ et $w(e) = 1$

$$\underset{\substack{\uparrow \\ \text{connu}}}{S} = H \cdot^t y = \underbrace{H \cdot^t c}_{=0} + \underbrace{H \cdot^t e}_{H_i}$$

H_i $j-$ème colonne de H où i est tel que :

$$\begin{cases} e_i = 1 \\ \forall j \in [\![1, n]\!] \setminus \{i\}, e_j = 0 \end{cases}$$

Algorithme 1.3.

Entrée : H, y où y est tel que $y = c + e$ avec $c \in C$ et $w(e) = 0$ ou 1, (c et e inconnus)

Sortie : c

1. $S \leftarrow H \cdot^t y$
2. Si $S = 0$, alors rendre y
3. Parcourir les colonnes de H jusqu'à trouver $i \in [\![1, n]\!]$ tel que $H_i = S$.
4. Rendre $(y - e)$ où $e = \left(0, \cdots, \underset{\substack{\uparrow \\ i-\text{ème} \\ \text{posititon}}}{1}, 0 \cdots, 0\right)$

On peut améliorer le point 3 de l'algorithme par les codes de Hamming :
Si $S \neq 0$, $\exists i \in [\![1, n]\!]$ $S - H_i$.
De plus, par construction, $i = \sum_{l=0}^{r-1} \varepsilon^{(i)} \times 2^l$

où $H_i = \begin{pmatrix} \varepsilon_1^{(i)} \\ \vdots \\ \varepsilon_r^{(i)} \end{pmatrix}$

Pour retrouver i,il suffit donc de calculer :

$$\sum_{l=0}^{r-1} \underbrace{S_{r-l}}_{\in\{0,1\}} \times 2^l$$

où $S = \begin{pmatrix} S_1 \\ \vdots \\ S_r \end{pmatrix}$ avec $S_i \in \mathbb{F}_2$ Correction de l'algorithme (point 3) pour l'améliorer :

$$i \leftarrow \sum_{l=0}^{r-1} S_{r-l} \cdot 2^l$$

Exemple 1.8.

1. $y = (1,1,1,0,0,0,0)$

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

$r = 3$

$$S = H \cdot^t y = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

donc $y \in C$.

2. $y = (1,1,1,0,0,1,0)$

$$S = H \cdot^t y = \begin{pmatrix} 1(\in \mathbb{F}_2) \\ 1 \\ 0 \end{pmatrix}$$

donc $i = 0 \cdot 2^0 + \underbrace{2}_{\in \mathbb{N}} \cdot 2^1 + 1 \cdot 2^2 = 6$

Donc $e = (0,0,0,0,0,1,0)$ *et* $c = (1,1,1,0,0,0,0)$

Exercice 1.1.

1. *Montrer que la code de Hamming est parfait.*
   $n = 2^r - 1$, $k = 2^r - 1 - r$ *et* $t = 1$.

$$\sum_{i=0}^{t} C_n^i (2-1)^i \stackrel{?}{=} 2^{n-k}$$

$$\sum_{i=0}^{t} C_n^i = 1 + n = 2^r = 2^{n-k}$$

2.

Remarque 1.5 (Tableau standard)**.**

$(0,\cdots,0)$	$(0,\cdots,0)$
$(1,0,\cdots,0)$	H_1
$(0,1,0,\cdots,0)$	H_2
$\vdots$	$\vdots$
$(0,\cdots,0,1)$	H_n

3. Soit α dans $\mathbb{F}_{2^r}$ racine primitive $(2^r-1)-$ième de 1.
On définit le code C par :

$$C = \{c \in \mathbb{F}_2^n | c(\alpha) = 0\}$$

où $c-(c_0,\cdots,c_n)$ où $c(\alpha) = \sum_{i=0}^{r-1} c_i\alpha^i$ Montrer que C est un code $[n, n-r, 3]_2$

V Codes de Golay

Le code de Golay linéaire étendue $\mathcal{G}_{24}$ a été utilisé par les sondes Voyager I et II $(1979-81)$ pour la transmission de photos de Jupiter et Saturne.
Il a pour matrice génératrice $G = (I_{12}|A)$ où :

$$A = \left(\begin{array}{c|ccc} 0 & 1 & \cdots & 1 \\ \hline 1 & & & \\ \vdots & & B & \\ 1 & & & \end{array}\right)$$

et $B \in \mathcal{M}_{11,11}(\mathbb{F}_2)$ est une matrice dite circulante définie par sa première ligne :

$$B = \begin{pmatrix} \overset{(1)}{1} & \overset{(2)}{1} & \overset{(3)}{0} & \overset{(4)}{1} & \overset{(5)}{1} & \overset{(6)}{1} & \overset{(7)}{0} & \overset{(8)}{0} & \overset{(9)}{0} & \overset{(10)}{1} & \overset{(11)}{0} \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ & & & & & & & & & & \\ & & & & & & & & & & \\ & & & & & \cdots & & & & & \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

où les carrés modulo 11 sont : $1, 4, 9, 5, 3$.
$\forall j \in \{1, \cdots, 11\}$

$$B_{ij} = \begin{cases} 1 & \text{si } (j-1=0) \text{ ou } (j-1 \text{ carré modulo } 11) \\ 0 & \text{sinon} \end{cases}$$

$$\text{donc } B_{ij} = \begin{cases} 1 & \text{si } i+j-2=0 \text{ ou } i+j-2 \text{ est un carré modulo } 11 \\ 0 & \text{sinon} \end{cases}$$

Théorème 1.3.

Soit C un code binaire $[n,k,d]_2$ et soit G une matrice génératrice de C.
Si les lignes de G sont orthogonales entre elles, et si les poids des lignes de G sont multiples de 4 alors les poids des mots de C sont multiples de 4 et $C \subset C^{\perp}$ (le code est inclus dans son dual)

Démonstration.

1. Soient deux lignes u et v de G alors $\langle u, v \rangle = 0$.
   Tout mot de C est une combinaison linéaire des lignes de G.
   Donc $\forall x, y \in C$
   $$\langle x, y \rangle = 0$$
   donc $\forall x \in C \; c \in C^{\perp}$
   $C^{\perp} = \{x \; in \mathbb{F}_2^n | \forall y \in C, \langle x, y \rangle = 0\}$
2. Montrons que le poids de la somme de deux lignes de G est multiple de 4 :
   Soient u, v deux lignes distinctes de G :

   $$\begin{aligned} w(u+v) &= \#\{i | u_i + v_i = 1\} \\ &= \#\{i | u_i = 1, v_i = 0\} + \#\{i | u_i = 0, v_i = 1\} \\ &= \#\{i | u_i = 1\} - \#\{i | u_i = 1, v_i = 1\} \\ &\quad + \#\{i | v_i = 1\} - \#\{i | u_i = 1, v_i = 1\} \end{aligned}$$

   $$w(u+v) = w(u) + w(v) - 2u * v$$

   où $u * v = \#\{i | u_i = v_i = 1\}$
   Or $\langle u, v \rangle = 0 = \sum_{i=1}^{n} u_i v_i = \sum_{u_i=1, v_i=1} 1$

Donc $\#\{i|u_i = 1 = v_i\} \equiv 0\,[2]$ donc $2u * v \equiv 0\,[4]$
De plus $w(u) \equiv 0\,[4]$ $w(v) \equiv 0\,[4]$ (par hypothèse car u et v sont des lignes de G)
Donc $w(u+v) \equiv 0\,[4]$ Par récurrence sur le nombre r de lignes, on obtient que le poids de la somme de r lignes de G est $\equiv 0\,[4]$.

□

On va utiliser ce théorème pour déterminer la distance minimale de $\mathcal{G}_{24}$ (sans faire la liste de 2^{12} mots de $\mathcal{G}_{24}$)
On remarque que le poids des lignes de G valent 12 ou 8 et que les lignes de G sont orthogonales entre elles.
Donc, d'après le théorème, $g \equiv 0\,[4]$ et $\underset{\dim 12}{\mathcal{G}_{24}} \subset \underset{\dim 24-12=\dim 12}{\mathcal{G}_{24}^{\perp}}$
Donc $g = 8$ ou 4 et $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$
Conséquences : soit $H = \left({}^tA|I_{12}\right)$, H est une matrice génératrice de $\mathcal{G}_{24}^{\perp}$ donc H est une matrice génératrice de $\mathcal{G}_{24}$
$G = (I_{12}|A)$ et $H = \left({}^tA|I_{12}\right) = (A|I_{12})$ sont des matrices génératrices de $\mathcal{G}_{24}$ donc

$$\mathcal{G}_{24} = \left\{ \underbrace{(x|xA)}_{x\cdot G} |x \in \mathbb{F}_2^{12} \right\}$$
$$= \left\{ \underbrace{(yA|y)}_{y\cdot H} |y \in \mathbb{F}_2^{12} \right\}$$

Supposons qu'il existe un mot de $\mathcal{G}_{24}$, c de poids 4. c est une somme de r lignes de G :

$$\exists x, c = \underbrace{(x|xA)}_{xG}$$

avec $w(x) = r$.
Nécessairement $r \leqslant 4$
Si $r = 4$ alors $w(x) = 4$ et $w(xA) = 0$ or c'est impossible car A est inversible ($A^2 = I$)
Si $r = 3$, alors $w(x) = 3$ donc $w(x^nA) = 1$
Or $\exists y \in \mathbb{F}_2^{12}$ tel que $c = (yA|a)$
Donc $\begin{cases} x = yA \\ xA = y \end{cases}$ donc $w(y) = 1$ et $w(yA) = 3$, yA est une ligne de A car $w(y) = 1$: impossible car les poids des lignes de A sont 11 ou 7.
Si $r = 1$: alors c est une ligne de G : impossible car les poids des lignes de

G sont 8 ou 12.
Si $r = 2$ alors :

$$c = g_1 + g_i$$

où g_i désigne la $i-$ème ligne de G et $i > 1$
ou $c = g_2 + g_i$ où $i > 2$
ou $c = g_i + g_j$ où $i \neq j$ $3 \leqslant i < j$ Matrice a finir voir feuille
$w(g_1 + g_2) = 8 \neq$ et $w(g_1 + g_i) = 8 \neq 4$ pour $i \geqslant 2$.
$w(g_2 + g_3) = 2 + 6 = 8$ et on vérifie $w(g_2 + h_i) = 8 \neq 4$ pour $i \geqslant 3$.
Conclusion : $\mathcal{G}_{24}$ ne possède pas de mot de poids 4.
Or $\begin{cases} d \leqslant 8 \\ d \equiv 0\,[4] \end{cases}$
Donc $d = 8$

Exercice 1.2.
On appelle $\mathcal{G}_{23}$ la code de Golay binaire, il est obtenu en ôtant une coordonnée (la dernière) aux mots de $\mathcal{G}_{24}$.
Montrons que $\mathcal{G}_{23}$ est un code $[23, 12, 7]_2$ parfait.

$$\begin{aligned}
\sum_{i=0}^{3} C_{23}^{i} &= 1 + 23 + C_{23}^{2} + C_{23}^{3} \\
&= 1 + 23 + \frac{23 \cdot 22}{2} + \frac{23 \cdot 22 \cdot 21}{3 \cdot 2} \\
&= 1 + 23 + 253 + 23 \times 11 \times 7 \\
&= 277 + 1771 \\
&= 2048 \\
&= 2^1 1
\end{aligned}$$

Décodage
$\mathcal{G}_{24}$ est un code binaire $[24, 12, 8]_2$ de matrices génératrices (et de contrôle car ce code est auto-dual) :

$$G = (I_{12}|A)\,, \text{ notons } A_j \text{ la j-ème colonne de } A$$

$$e_j = \left(0 \cdots, 0, \underset{\substack{\uparrow \\ j}}{1}, 0 \cdots, 0 \right)$$

et $H = (A|I_{12}) = \left({}^tA|I_{12}\right)$.
et $A =^t A$ et $A \cdot^t A = A^2 = I_{12}$ de plus sa distance minimale est 8.

Soit $c \in \mathcal{G}_{24}$ soit $e \in= \begin{pmatrix} x \,|\, y \\ \leftrightarrow \quad \leftrightarrow \\ 12 \quad 12 \end{pmatrix} \in \mathbb{F}_2^{24}$ avec $w(e) \leqslant 3$ (ie $w(x) + w(y) \leqslant 3$)

Soit $r = c + e$, on a 4 cas :

- $w(x) = 0$
- $w(x) = 1$, $w(y) = 1$ ou 2
- $w(x) = 2$ $w(y) = 1$
- $w(y) = 0$

Notons les syndromes suivants :

$$S = H \cdot^t x = \underbrace{H \cdot^t c}_{=0} + H \cdot^t c = A \cdot^t x +^t y$$

$$T = G \cdot^t r = \underbrace{G \cdot^t c}_{=0} + G \cdot^t e =^t x + A \cdot^t y$$

On verra dans un lemme que :

$$w(x) = 0 \Leftrightarrow w(s) \leqslant 3$$

et

$$w(y) = 0 \Leftrightarrow 0 \Leftrightarrow w(T) \leqslant 3$$

Lemme 1.1.

1. $w(x) = 0 \Leftrightarrow w(s) \leqslant 3$
2. $w(y) = 0 \Leftrightarrow 0 \Leftrightarrow w(T) \leqslant 3$

Démonstration.

Si $w(x) = 0$ alors $S =^t y$
Or $w(x) + w(y) \leqslant 3$ donc $w(s) \leqslant 3$.

Si $w(x) \neq 0$

$$\begin{aligned} w(s) &= w(xA) + w(y) - 2\underbrace{(xA) * y}_{\leqslant w(y)} \\ &\geqslant w(xA) + w(y) - 2w(y) \\ &\geqslant \underbrace{w(x|xA)}_{\geqslant 8 \text{ car } x \neq 0} - \underbrace{(w(x) + w(y))}_{\geqslant 3} \end{aligned}$$

□

Lemme 1.2.

Supposons que $w(s) > 3$ et $w(T) > 3$ alors l'une de ces situations est réalisée :

— $\exists j \in \{1, \cdots, 12\}\ w(T - A_j) \in \{1, 2\}$.
Dans ce cas $y = e_i$ et $x =^t T -^t A_j$

— $\exists j \in \{1, \cdots, 12\}\ w(S - A_j) \in \{1, 2\}$
Dan ce cas $x = e_j$ et $y =^t S -^t A_j$

Démonstration.
O a $w(s) = w(y) = 1$ ou $w(x) = 2\ w(y) = 1$ ou $w(x) = 1$ et $w(y) = 2$

* Supposons $\exists j \in [\![1, 12]\!]\ T = A_j = 0$.
Alors ${}^t x + A \cdot^t y = A \cdot^t e_j$
Donc ${}^t x = A\left({}^t y +^t e_j\right)$ car on est en binaire (donc $- = +$)
Nécessairement $y \neq e_j$ sinon $x = 0$.
$(y + e_j) \cdot G = (y + e_j | (y + e_j) \cdot A)$ est un mot non nul de $\mathcal{G}_{24}$ donc son poids est $\geqslant 8$ (distance minimale)
Donc $w(y + e_j) + w((y + e_j) A) \geqslant 8$
Or $x = (y + e_j) A$ donc $w(y + e_j) + w(x) \geqslant 8$.
C'est impossible car : $\begin{cases} w(x) \leqslant 2 \\ w(y) \leqslant 2 \\ w(e_j) = 1 \end{cases}$ (donc $w(y + e_j) \leqslant 3$)
Donc $\forall j \in [\![1, 12]\!]\ w(T - A_j) > 0$
De même $\forall j \in [\![1, \cdots, 12]\!], w(S - A_j) > 0$

* :Supposons $\exists j \in [\![1, 12]\!]\ T = A_j = 1$.
Soit $z \in \mathbb{F}_2^{12}$ tel que $T - A_j =^t z$ avec $w(z) = 1$

$$^t x + A \cdot^t y - A \cdot^t e_j =^t z$$

donc ${}^t x +^t z = A\left({}^t y +^t e_j\right)$
— Si $y = e_j$ alors $x = z =^t T -^t A_j$
— Si $y \neq e_j$ alors $\underbrace{(y + e_j | (y + e_j) A)}_{(y+e_j)\cdot G}$ est un mot de $\mathcal{G}_{24}$ non nul. Donc son poids est $\geqslant 8$.
Donc $w(y + e_j) + w((y + e_j) A) \geqslant 8$ or $w((y + e_j) A) = w(x + z)$
Donc $w(y + e_j) + w(x + z) \geqslant 8$
Or $w(e_j) = 1$, $w(x) + w(z) \leqslant 3$ et $w(z) = 1$

Donc $w(y+e_j)+w(x+z) \leqslant z(x)+w(y)+w(e_j)+w(z) \leqslant 5$
Contradiction.

* :Supposons $\exists j \in [\![1,12]\!]$ $T = A_j = \mathbf{2}$.
Soit $z \in \mathbb{F}_2^{12}$ tel que $T - A_j =^t z$ avec $w(z) =]mb2$

$$^t x + A \cdot^t y - A \cdot^t e_j =^t z$$

donc $^t x +^t z = A\left(^t y +^t e_j\right)$
— Si $y = e_j$ alors $x = z =^t T -^t A_j$
— Si $y \neq e_j$ alors $\underbrace{(y+e_j|\,(y+e_j)\,A)}_{(y+e_j)\cdot G}$ est un mot de $\mathcal{G}_{24}$ non nul. Donc son poids est $\geqslant 8$.
Donc $w(y+e_j)+w((y+e_j)\,A) \geqslant 8$ or $w((y+e_j)\,A) = w(x+z)$
Donc $w(y+e_j)+w(x+z) \geqslant 8$
Or $w(e_j) = 1$, $w(x)+w(z) \leqslant 3$ et $w(z) = \mathbf{2}$
Donc $w(y+e_j)+w(x+z) \leqslant z(x)+w(y)+w(e_j)+w(z) \leqslant \mathbf{6}$
Contradiction. Donc $y = e_j$

* : Supposons qu'il existe $j \in [\![1,12]\!]$ $w(S-a_j) \in \{1,2\}$
Alors on montre que $x = e_j$ et $y =^t S +^t A_j$

* : Supposons que $\forall j \in lbbracket1,12]\!]$ $w(T+A_j) \geqslant 3$
et $\forall i \in [\![1,12]\!]$, $w(S+A_i) \geqslant 3$

$$w\left(^t x + A\left(^t e_j +^t y\right)\right) \geqslant 3$$

Si $y = e_k$ pour $k \in [\![1,12]\!]$ alors $T =^t x + A_k$ donc $w(T+A_k) \leqslant 2$:
Impossible car $w(T+A_j) \geqslant 3$ $\forall j$
$T =^t x + A^t y$ et $S =^t +A^t x$.
Donc $y \neq e_k$ pour tout k donc $w(y) \neq 1$
De même $w(x) \neq 1$.
Contradiction car $w(x) = 1$ ou $w(y) = 1$

□

Algorithme 1.4.

Entrée : r, G, H

Sortie : c.

1. $S \leftarrow H \cdot^t r$
2. $T \leftarrow G \cdot^t r$
3. Si $w(S) \leqslant 3$ alors rendre $\left(\underbrace{0}_{x} | \underbrace{S}_{y} \right) + r$
4. Si $w(T) \leqslant 3$ alors rendre $\left({}^tT|0\right) + r$ (les deux dernières affirmations découlent du 1er lemme)
5. Si $\exists j \in \{1, \cdots, 12\}$ tel que $w(T + A_j) \leqslant 2$
   Alors rendre $r + \left({}^tT +^t A_j | e_j\right)$
6. Si $\exists j \in \{1, \cdots, 12\}$ $w(S + A_j) \leqslant 2$
   Alors rendre $r + \left(e_j |^t S +^t A_j\right)$
7. Sinon il y avait plus que 3 erreurs.

Remarque 1.6.
Cet algorithme est adaptable à tout code binaire ***auto-dual*** *de distance minimale* $\geqslant 8$ *ayant une matrice génératrice sous forme systématique :*

$$G = (I_K | A)$$

avec $A \cdot^t A = I_K$

Chapitre 2

Code de Reed-Solomon généralisés

But : Construire une famille de codes linéaires MDS sur $\mathbb{F}_q$ ainsi qu'un algorithme de décodage en temps polynomial.

I Codes de Reed-Solomon généralisés

Exemple 2.1. *Construction d'un code* $[6,4,3]_7$
On considère $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$
$Rg(H) = 2$ *et tout ensemble de* 2 *colonnes de* H *est linéairement indépendant.*
En effet soient $\alpha \neq \beta \in \mathbb{F}_7 \backslash \{0\}$

$$\begin{vmatrix} 1 & 1 \\ \alpha & \beta \end{vmatrix} = \beta - \alpha \neq 0$$

Construction d'un code $[6,3,4]_7$ *:*

$$H = \begin{pmatrix} 1 & & \cdots & & & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 \end{pmatrix}$$

Soient $\alpha, \beta, \gamma \in \mathbb{F}_7 \backslash \{0\}$ $\alpha \neq \beta, \alpha \neq \gamma, \beta \neq \gamma$

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{vmatrix} \neq 0$$

car $\alpha \neq \beta, \beta \neq \gamma, \alpha \neq \gamma$
C'est la déterminant d'une matrice de Vandermonde $(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$

Tout ensemble de 3 *colonnes de* H *est donc linéairement indépendant, donc le code de matrice de contrôle* H *ne possède pas de mot de poids* $\leqslant 3$.
Donc $d \geqslant 4$ *or* $d \leqslant 4$ *(Borne de Singleton) donc*

$$d = 4$$

Définition 2.1.

Soit $\mathbb{F}_q$ un corps fini à q éléments.
Soient $n \in \mathbb{N}^*$ et $k \in \{0, \cdots, n\}$
Soient $\alpha_1, \cdots, \alpha_n$ des éléments de $\mathbb{F}_q$ distincts 2 à 2 et non nuls.
Soient $v_1 \cdots, v_n$ des éléments de $\mathbb{F}_q$ non nuls.
Une code de Reed-Solomon généralisé $[n, k]_q$ est un code linéaire dont une matrice de contrôle est :

$$H = V_{n-k,n}^{(\alpha)} \cdot D_n^{(v)}$$

où $V_{n-k,n}^{(\alpha)}$ est une matrice de Vandermonde rectangulaire définie par :

$$V_{n-k,n}^{(\alpha)} = \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \alpha_1^2 & \cdots & \alpha_n^2 \\ \vdots & & \vdots \\ \alpha_1^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix}$$

et

$$D_n^{(v)} = \begin{pmatrix} v_1 & & 0 \\ & \ddots & \\ 0 & & v_n \end{pmatrix}$$

On dit que $\alpha_1, \cdots, \alpha_n$ sont les **localisateurs** du code.
et que $v_1, \cdots, v_n$ sont les **multiplicateurs** du code.
Si $n = q - 1$ on dit que le code est **primitif**.
Si $\forall i \in \{1, \cdots, n\}$ $v_i = 1$ on dit que le code est **normalisé**.
On note **GRS** les code de Reed-Solomon généralisé.

Pour remarque

$$V_{n-k,n}^{(\alpha)} \cdot D_n^{(v)} = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_n^2 v_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-k-1} v_1 & \alpha_2^{n-k-1} v_2 & \cdots & \alpha_n^{n-k-1} v_n \end{pmatrix}$$

Exemple 2.2.

1. $q = 7$, $n = 6$ $\forall i \in \{1, \cdots, 6\}$ $\alpha_i = i$
   $k = 4$ $\forall i \in \{1, \cdots, 6\}$ $v_i = i$

$$H = \begin{pmatrix} 1 & & \cdots & 1 \\ 1 & 2 & \cdots & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 6 \end{pmatrix}$$

2. $q = 8$ $n = 6$ *et* $k = 4$ *On construit* $\mathbb{F}_8$, *il nous faut un polynôme irréductible de degré* 3.

$$\mathbb{F}_8 \equiv \mathbb{F}_2[X]/(P)$$

où P *est irréductible, de degré* 3. *Par exemple on peut prendre* $X^3 + X + 1$, *il est irréductible sur* $\mathbb{F}_2$ *car son terme constant est* $\neq 0$ *et il a un nombre impair de termes.*
Soit $\omega \in \mathbb{F}_8$ *tel que* $\omega^3 + \omega + 1 = 0$
On a $x^8 = x$ *et* $x^7 = 1$
On considère pour $i \in \{1, \cdots, 6\}$ $\alpha_i = \omega^{i=1}$.
On a $\forall i$ $\alpha_i \neq 0$
$\forall i \neq j$ $\alpha_i \neq \alpha_j$ *car l'ordre de* ω *est* 7.

Théorème 2.1.

Un code de Reed-Solomon généralisé est MDS

Démonstration.
Soit $\mathcal{C}$ un code GRS $[n, k, d]_q$.
Soient $\alpha_1, \cdots, \alpha_n \in \mathbb{F}_q \backslash \{0\}$ distincts 2 à 2 ses localisateurs.
$v_1, \cdots, v_n \in \mathbb{F}_q \backslash \{0\}$ ses multiplicateurs.
On a

$$d \leqslant n - k + 1 \text{ (Borne de Singleton)}$$

Montrons que $\mathcal{C}$ ne possède pas de mot non nul de poids $\leqslant n-k$:
Soit $H = V_{n-k,n}^{(\alpha)} \cdot D_n^{(v)}$ une matrice de contrôle de $\mathcal{C}$.
Montrons que tout sous-déterminant d'ordre $n-k$ de H est non nul.

$$H = \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix} \cdots \begin{pmatrix} v_1 & & 0 \\ & \ddots & \\ 0 & & v_n \end{pmatrix}$$

Toute matrice $(n-k) \times (n-k)$ extraite de H est du type :

$$\Delta = \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \beta_1 & \cdots & \beta_i & & \vdots \\ \vdots & & \beta_i^2 & & \vdots \\ \beta_1^{n-k-1} & & \beta_i^{n-k-1} & \cdots & \beta_n^{n-k-1} \end{pmatrix} \cdot \begin{pmatrix} v_{i_1} & & 0 \\ & \ddots & \\ 0 & & v_{i_{n-k}} \end{pmatrix}$$

Avec $\beta_1, \cdots, \beta_{n-k}$ distincts 2 à 2.

$$\begin{aligned} \det(\Delta) &= \begin{vmatrix} 1 & \cdots & 1 \\ \beta_1 & \cdots & \beta_{n-k} \\ \vdots & & \vdots \\ \beta_1^{n-k-1} & & \beta_{n-k}^{n-k-1} \end{vmatrix} \cdot \prod_{j=1}^{n-k} v_{i_j} \\ &= \left(\prod_{i<j} \beta_i - \beta_j \right) \cdot \prod_{j=1}^{n-k} v_{i_j} \\ &\neq 0 \end{aligned}$$

□

Proposition 2.1.

Le dual d'un code GRS est un code GRS (ayant les mêmes localisateurs).

Démonstration.
soit $\mathcal{C}$ un code GRS $[n, k, n-k+1]_q$ de localisateurs $\alpha_1, \cdots, \alpha_n$ et multiplicateurs $v_1, \cdots, v_n$

Montrons qu'il existe $v'_1, \cdots, v'_n \in \mathbb{F}_q^*$ tels que :

$$G = \underbrace{\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}}_{=V_{k,n}^{(\alpha)}} \cdots \underbrace{\begin{pmatrix} v'_1 & & 0 \\ & \ddots & \\ 0 & & v'_n \end{pmatrix}}_{=D_n^{(v')}}$$

soit une matrice de contrôle de $\mathcal{C}^\perp$, *ie* matrice génératrice de $\left(\mathcal{C}^\perp\right)^\perp = \mathcal{C}$.
Notons :

$$H = \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix} \cdot \begin{pmatrix} v_1 & & 0 \\ & \ddots & \\ 0 & & v_n \end{pmatrix}$$

H est une matrice de contrôle de $\mathcal{C}$.
Montrons qu'il existe v'_1, v'_n tels que $G \cdot {}^t H = 0$ *ie* que les lignes de G et H soient orthogonales entre elles.

$$G \cdot {}^t H \Leftrightarrow \forall i \in \{1, \cdots, n-k\|, \forall j \in \{1, \cdots, k\}, \sum_{l=1}^{n} \alpha_l^{i-1} \cdot v_l \cdot \alpha_l^{j-1} \cdot v'_l = 0$$

(on a $H_{i,l} = \alpha_l^{i-1} \cdot v_l$ et $G_{j,l} = \alpha_l^{j-1} \cdot v'_l$)
$\forall i \in \{1, \cdots, n-k\}$ $\forall j \in \{1, \cdots, k\}$

$$\sum_{l=1}^{n} \alpha_l^{i+j-2} \cdot v_k \cdot v'_l = 0$$

$$\underbrace{\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{n-2} & \cdots & \alpha_n^{n-2} \end{pmatrix} \cdot \begin{pmatrix} v_1 & & 0 \\ & \ddots & \\ 0 & & v_n \end{pmatrix}}_{=V_{n-1,n}^{(\alpha)} D_n^{(v)}} \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = 0$$

$V_{n-1,n}^{(\alpha)} D_n^{(v)}$ est une matrice de contrôle d'un GRS $[n, 1, n]_q$
Tous les mots d'un code GRS $[n, 1, n]_q$ ont un poids nul ou $\geqslant n$ donc tous les mots $\neq 0$ ont un poids égal à n.

Donc il existe $(v'_1, \cdots, v'_n)$ de poids n tel que

$$V^{(\alpha)}_{n-1,n} D^{(v)}_n \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = 0$$

$(\forall i, v'_i \neq 0)$ □

Exemple 2.3. *Code* GRS $[6, 4, 3]_7$ *de localisateur* $1, \cdots, 6$ *et multiplicateurs* $1, \cdots, 6$
Une matrice génératrice est :

$$\begin{pmatrix} 1 & & \cdots & 1 \\ 1 & 2 & \cdots & 6 \\ 1^2 & 2^2 & \cdots & 6^2 \\ 1^3 & 2^3 & \cdots & 6^3 \end{pmatrix} \cdot \begin{pmatrix} v'_1 & & 0 \\ & \ddots & \\ 0 & & v'_6 \end{pmatrix}$$

où

$$\begin{pmatrix} 1 & \cdots & 1 \\ 1 & \cdots & 6 \\ \vdots & & \vdots \\ 1^4 & \cdots & 6^4 \end{pmatrix} \begin{pmatrix} 1 \cdot v'_1 \\ \vdots \\ 6 \cdot v'_6 \end{pmatrix} = 0$$

Ce qui correspond à $V^{(\alpha)}_{5,6} \cdot D^{(v)}_6$ *(cd preuve)*
$v'_1 = \cdots = v'_6 = 1$ *est solution (dans* $\mathbb{F}_7$*)*

Conséquence : Interprétation polynomiale :
Soit $\mathcal{C}$ un code *GRS* $[n, k, n-k+1]_q$ de localisateur $\alpha_1, \cdots, \alpha_n$ et multiplicateurs $v_1, \cdots, v_n$
Une matrice génératrice de $\mathcal{C}$ est :

$$G = V^{(\alpha)}_{k,n} \cdot D^{(v')}_n$$

pour un certain $n-$uplet de $\left(\mathbb{F}_q^*\right)^n$ $v=(v_1,\cdots,v_n)$

$$\begin{aligned}
\mathcal{C} &= \left\{mG | m\in\mathbb{F}_q^k\right\}\\
&= \left\{ \left(m_0,\cdots,m_{k-1}\right) \begin{pmatrix} 1 & \cdots & 1\\ \alpha_1 & \cdots & \alpha_n\\ \vdots & & \vdots\\ \alpha_1^{k-1} & \cdots & \alpha_n^{k-1}\end{pmatrix} \begin{pmatrix} v_1' & & 0\\ & \ddots & \\ 0 & & v_n'\end{pmatrix} \text{ tel que } m_i\in\mathbb{F}_q \right\}\\
&= \left\{ \left(\sum_{i=0}^{k-1} m_i\alpha_1^i, \sum_{i=0}^{k-1} m_i\alpha_2^i,\cdots,\sum_{i=0}^{k-1} m_i\alpha_n^i\right) \begin{pmatrix} v_1' & & 0\\ & \ddots & \\ 0 & & v_n'\end{pmatrix} \text{ tq } m_i\in\mathbb{F}_q \right\}\\
&= \left\{ \left(m\left(\alpha_1\right), m\left(\alpha_2\right),\cdots,m\left(\alpha_n\right)\right) \begin{pmatrix} v_1' & & 0\\ & \ddots & \\ 0 & & v_n'\end{pmatrix} \text{ tel que } m(X)\in\mathbb{F}_q[X], \deg(m)\leqslant k-1 \right\}\\
&= \left\{\left(v_1' m\left(\alpha_1\right),\cdots,v_n' m\left(\alpha_n\right)\right) \text{ tel que } m\in\mathbb{F}_q[X], \deg(m)\leqslant k-1\right\}
\end{aligned}$$

Exercice 2.1.
Montrer qu'un code GRS est MDS en utilisant la caractérisation polynomiale.

Rappels
Soit C le code GRS $[6,2,5]_7$ de matrice de contrôle :

$$H = \begin{pmatrix} 1 & 1 & 1 & 11 & 1 & \\ 1 & 2 & 3 & 4 & 5 & 6\\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2\\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3\end{pmatrix} \begin{pmatrix} 1 & & & & & \\ & 2 & & 0 & & \\ & & 3 & & & \\ & 0 & & 4 & & \\ & & & & 5 & \\ & & & & & 6\end{pmatrix}$$

où les coefficients de la 2e ligne de la première matrice sont les localisateurs, et les coefficients diagonaux de la deuxième les multiplicateurs.

$$C = \left\{x\in\mathbb{F}_7^6 \text{ tel que } H\cdot{}^t x = 0\right\}$$

Une matrice génératrice de C est :

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1\\ 1 & 2 & 3 & 4 & 5 & 6\end{pmatrix} \cdot \begin{pmatrix} 1 & & & & & \\ & 1 & & 0 & & \\ & & 1 & & & \\ & 0 & & 1 & & \\ & & & & 1 & \\ & & & & & 1\end{pmatrix}$$

On a les même localisateurs.
Soit $m \in \mathbb{F}_7^2$,

$$\begin{aligned} mG &= (m_0 + m_1, m_0 + 2m_1, m_0 + 3m_1, m_0 + 4m_1, m_0 + 5m_1, m_0 + 6m_1) \\ &= (f(1), f(2), f(3), f(4), f(5), f(6)) \end{aligned}$$

où $f = n_0 + m_1 x$
Donc $C = \{(f(1), f(2), \cdots, f(6)), f \in \mathbb{F}_7[X], \deg(f) < 2\}$ Vérifions que la distance minimale de C est 5 en utilisant :
Le théorème de Singleton : $d \leqslant 6 - 2 + 1 \leqslant 5$
Soit c dans C de poids $\leqslant 4$, montrons que $c = 0$
f dans $\mathbb{F}_7[x]$ tel que $\deg(f) < 2$ et $c = (f(1), \cdots, f(6))$, $d \leqslant 4$ donc

$$\#\{i \in [\![1, 6]\!], f(i) \neq 0\} \leqslant 4$$

$\#\{i \in [\![1, 6]\!]$ tel que $c_i \neq 0\}$
Or $\deg(f) < 2$, $f \in \mathbb{F}_7[x]$ et $\mathbb{F}_7$ est un corps donc f est nul ou f a au plus une racine, donc $f = 0$ et $c = 0$
Donc $\forall c \in C \backslash \{0\}$ $w(c) \geqslant 5$ donc $d = 5$
Exemple de problème si on est pas dans un corps : $\mathbb{Z}/10\mathbb{Z}$

Algorithme de Berlekamp-Welch
Soit C un code GRS $[n, k, n-k+1]_q$ de localisateur $\alpha_1, \cdots, \alpha_n \in \mathbb{F}_q^*$ avec $\forall i \neq j, \alpha_i \neq \alpha_j$

$$C = \{(f(\alpha_1), \cdots, f(\alpha_n)) \,|\, f \in \mathbb{F}_q[x], \deg(f) < k\}$$

On suppose que $d\,(= n - k + 1)$ est impair et on note $t = \dfrac{d-1}{2}$
Soit $c = (f(\alpha_1), \cdots, f(\alpha_n))$ avec $f \in \mathbb{F}_q[x]$ et $\deg(f) < k$
Soit $r \in \mathbb{F}_Q^n$ tel que $d_H(c, r) \leqslant t$
Étant donné r on chercher à retrouver f.
On note $I = \{i \in \{1, \cdots, n\}, c_i \neq r_i\}$
On a $|I| \leqslant t$
n a $f(\alpha_i) = r_i$ pour $i \in \{1, \cdots, n\} \backslash I$ où f est inconnu, et α_i, r_i connus.
Pour retrouver f on va construire deux polynômes $Q_0(x), Q_1(x)$ tel que :

$$\forall i \in \{1, \cdots, n\}, Q_0(\alpha_i) = r_i \cdot Q_1(\alpha_i)$$

où $\deg(Q_0) < n - t, \deg(Q_1) < t + 1$ et on va déduire $f(x)$ à partir de $Q_0(x)$ et $Q_1(x)$

1. Construction de Q_0 et Q_1
   On cherche Q_0 et Q_1 tels que :

$$\begin{cases} \forall i \in \{1, \cdots, n\}, Q_0(\alpha_i) = r_i \cdot Q_1(\alpha_i) & (1) \\ \deg(Q_0) < n - t & (2) \\ \deg(Q_1) < t + 1 & (3) \end{cases}$$

   (1) : n équations, (2) $n-t$ inconnues, (3) : $t+1$ inconnues (donc $n+1$ inconnues dans le système)
   On a un système linéaire à n équation et $n+1$ inconnues donc il possède nécessairement une solution.

2. Construction de f à partir de Q_0 et Q_1
   Considérons le polynôme $\phi(x) = Q_0(x) - f(x) Q_1(x) \in \mathbb{F}_q[x]$.
   Montrons que $\phi = 0$

$$\begin{aligned} \deg(\phi) &\leqslant \max\left(\underbrace{\deg(Q_0)}_{<n-t}, \underbrace{\deg(f(x))}_{<k} + \underbrace{\deg(Q_1(x))}_{\leqslant t}\right) \\ &< \max(n-t, k+t) \\ &< \max\left(\underbrace{n - \frac{n-k}{2}}_{\frac{n}{2}+\frac{k}{2}}, \underbrace{k + \frac{n-k}{2}}_{\frac{n}{2}+\frac{k}{2}}\right) \end{aligned}$$

   $\deg(\phi) < n - t$

   $\forall i \in I \; r_i \neq f(\alpha_i)$
   $\forall i \in \{1, \cdots, n\} \setminus I \; r_i = f(\alpha_i)$
   $I = \{i | r_i \neq f(\alpha_i)\} \; |I| \leqslant t$
   De plus $\forall i \in [\![1, n]\!]$

$$Q_0(\alpha_i) - r_i Q_1(\alpha_i) = 0$$

   Donc $\forall i \in [\![1, n]\!] \setminus I$

$$Q_0(x_i) - f(\alpha_i) Q_1(\alpha_i) = 0$$

   $\forall i \in \{1, \cdots, n\} \setminus I, Q(\alpha_i) = 0$
   ϕ a au moins $n-t$ racines (car $|\{1, \cdots, n\} \setminus I| \geqslant n - t$)
   Or $\phi \in \mathbb{F}_q[X]$ $\mathbb{F}_q$ corps donc $\phi = 0$
   Donc $f(x) = \dfrac{Q_0(x)}{Q_1(x)}$

Remarque 2.1.
Les équations

$$\begin{cases} \forall i \in \{1, \cdots, n\} \\ Q_0(r_i) = r_i Q_1(\alpha_i) \end{cases}$$

peuvent s'écrire :

$$\begin{cases} Q_0 \equiv P \cdot Q_1 [F] \\ \deg(Q_0) < n - t \\ \deg(Q_1) < t + 1 \\ P(\alpha_i) = r_i, \deg(P) < n \\ F = \prod_{i=1}^{n} (x - \alpha_i) \end{cases}$$

et on peut calculer Q_0 et Q_1 en appliquant l'algorithme d'Euclide étendue à F et P

Exemple 2.4.
$C = \{(f(1) f(2), \cdots, f(6)) \,|\, f \in \mathbb{F}_7[x], \deg(f) < 2\}$
C est un code $[6, 2, 5]_7$, C est $2-$correcteur d'erreurs.

Soit : $\begin{cases} f(x) = -x + 2 \\ c = (1, 0, 6, 5, 4, 3) \\ e = (0, 2, 0, 3, 0, 0) \\ r = c + e = (1, 2, 6, 1, 4, 3) \end{cases}$

Connaissant r on souhaite retrouver f.
On cherche $Q_0, Q_1 \in \mathbb{F}_7[x]$ tels que :

6 *équations* $\begin{cases} Q_0(1) - Q_1(1) = 0 = a_0 + a_1 + a_2 + a_3 - b_0 - b_1 - b_2 \\ Q_0(2) - 2Q_1(2) = 0 = q_0 + 2a_1 + 4a_2 + a_3 - 2(b_0 + 2b_1 + 4b_2) \\ Q_0(3) - 6Q_1(3) = 0 = \cdots \\ Q_0(4) - Q_1(4) = 0 \\ Q_0(5) - Q_1(5) = 0 \\ Q_0(6) - Q_1(6) = 0 \end{cases}$

Avec $\deg(Q_0) < 4$ *et* $\deg(Q_1) < 3$

$$\begin{cases} Q_0 = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \\ Q_1 = b_0 + b_1 x + b_2 x^2 \end{cases}$$

7 inconnues !
Ce système a pour solution $\lambda \cdot (5, 6, 6, 1, 6, 6, 6)$ $\lambda \in \mathbb{F}_7$

$$f = \frac{5 + 6x + 6x^2 + x^3}{-1 - x - x^2} = -(x + 5) = -x + 2$$

II Codes de Reed-Solomon

Les codes de Reed-Solomon sont des codes GRS particuliers.

Définition 2.2.

Soit q une puissance d'un nombre premier et soit n un entier divisant $q-1$
Soit α un élément de $\mathbb{F}_q$ d'ordre multiplicatif égal à n. (donc $\alpha^n = 1$ et $\forall i \in \{1, \cdots n-1\}, \alpha^i \neq 0$)
Un code de Reed-Solomon $[n,k]_q$ est un code de Reed-Solomon généralisé de localisations :

$$\alpha_i = \alpha^{i=1}, i = 1, \cdots, n$$

et de multiplicateurs :

$$v_j = \alpha^{b(j-1)}, j = 1, \cdots, n$$

Le code est dit primitif si $n = q-1$
Le code est dit normalisé si $b = 0$

Une matrice de contrôle est :

$$H = \begin{pmatrix} 1 & & \cdots & & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{n-k-1} & & \cdots & \alpha^{(n-k-1)(n-1)} \end{pmatrix} \cdot \begin{pmatrix} 1 & & & & 0 \\ & \alpha^b & & & \\ & & \ddots & & \\ & 0 & & \ddots & \\ & & & & \ddots \\ & 0 & & & \alpha^{b(n-1)} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \alpha^b & \cdots & \alpha^{b(n-1)} \\ \vdots & \alpha^{b+1} & & \vdots \\ \vdots & & & \vdots \\ 1 & \alpha^{b+n-k-1} & & \alpha^{(b+n-k-1)(n-1)} \end{pmatrix}$$

Exemple 2.5. $q = 2^4, n = 15$ ***Polynôme irréductibles de degré*** 4 ***sur*** $\mathbb{F}_2$

$$\begin{cases} \textit{ne s'annulant par en } 0 \textit{ et } 1 \\ \textit{ne sont pas divisibles par } X^2 + X + 1 \end{cases}$$

Pas divisible par x *et par* $X+1$ *:* X^4+X^3+1, $X^4+X^2+1=\left(x^2+X+1\right)^2$
X^4+X+1, $X^4+X^3+X^2+X+1$
$\mathbb{F}_{2^4}\simeq\mathbb{F}_2[X]/\left(X^4+X+1\right)$
Soit $\alpha\in\mathbb{F}_{2^4}$ *tel que* $\alpha^4+\alpha+1=0$
On a $\alpha^{15}=1$
$\alpha^3\neq 1$ *car* $\alpha^4+\alpha+1=0$ *et* X^4+X+1 *est irréductible sur* $\mathbb{F}_2$
$\alpha^5=\alpha^4\cdot\alpha=(\alpha+1)\alpha=\alpha^2+\alpha\neq 1$
On a donc $\alpha^{15}=1$, $\alpha^3\neq 1$ *et* $\alpha^5\neq 1$ *donc* α *est une racine primitive* $15-$*eme de* 1.
Prenons $b=3$ *et* $k=13$ *:*

$$H=\begin{pmatrix}1&1&1&\cdots&1\\1&\alpha&\alpha^2&\cdots&\alpha^{14}\end{pmatrix}\cdot diag\left(1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12},1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12},1,\cdots\right)$$

(5 blocs.)
Interprétation polynomiale

$$H=\begin{pmatrix}1&\alpha^b&\alpha^{2b}&\cdots&\alpha^{b(n-1)}\\1&\alpha^{b+1}&\cdots&\cdots&\alpha^{(n-1)(b+1)}\\\vdots&\vdots&\cdots&\cdots&\vdots\\1&\alpha^i&\left(\alpha^i\right)^2&\cdots&\left(\alpha^i\right)^{(n-1)}\\\vdots&\vdots&\cdots&\cdots&\vdots\\1&\alpha^{b+d-2}&\cdots&\cdots&\alpha^{(n-1)(b+d-2)}\end{pmatrix}$$

$d=n-k+1$
$C=\left\{c\ in\mathbb{F}_q^n|H\cdot^t c=0\right\}$ $c=(c_0,\cdots,c_{n-1})$

$$H\cdot^t c=\begin{pmatrix}c_0+c_1\left(\alpha^b\right)+c_2\left(\alpha^b\right)^2+\cdots+c_{n-1}\left(\alpha^b\right)^{n-1}\\c_0+c_1\left(\alpha^{b+1}\right)+c_2\left(\alpha^{b+1}\right)^2+\cdots+c_{n-1}\left(\alpha^{b+1}\right)^{n-1}\\\vdots\\c_0+c_1\left(\alpha^i\right)+c_2\left(\alpha^i\right)^2+\cdots+c_{n-1}\left(\alpha^i\right)^{n-1}\\\vdots\\c_0+c_1\left(\alpha^{b+d-2}\right)+c_2\left(\alpha^{b+d-2}\right)^2+\cdots+c_{n-1}\left(\alpha^{b+d-2}\right)^{n-1}\end{pmatrix}$$

$$H\cdot^t c=\begin{pmatrix}c\left(\alpha^b\right)\\c\left(\alpha^{b+1}\right)\\\vdots\\c\left(\alpha^{b+d-2}\right)\end{pmatrix}$$

où $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ *donc :*

$$\begin{aligned}H\cdot^t c=0&\Leftrightarrow c\left(\alpha^b\right)=c\left(\alpha^{b+1}\right)=\cdots=c\left(\alpha^{b+d-1}\right)=0\\&\Leftrightarrow g(x)\,|c(x)\end{aligned}$$

où $g(x) = \prod_{i=b}^{bd-2} (x - \alpha_i)$

De plus $g(x) | x^n - 1$ *: on a un code cyclique.*

Remarque : $c \in \mathbb{F}_q^n \Leftrightarrow c(x) \in \mathbb{F}_q[X] / (x^n - 1)$

Chapitre 3

Codes cycliques

C'est une sous-classe des codes linéaires, et ils sont plus facile à encoder.

I Définition et propriétés

$\mathbb{F}_q$ désigne un corps fini à q éléments, et n un entier **non nul**.

Définition 3.1.

Un code linéaire $\mathcal{C}$ de longueur n est dit **cyclique** si toute permutation cyclique d'un mot de code est dans $\mathcal{C}$.

Explication : Si on note les mots sous forme de $n-$uplet (la numérotation commence à 0) $c = (c_0, \cdots, c_{n-1}) \in \mathcal{C}$
Alors $c^\pi = (c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$

$$\begin{array}{ccccc} (\mathbb{F}_q)^n & \leftrightarrow & \mathbb{F}_q[X]_{<n} & \leftrightarrow & \mathbb{F}_q[X]_{/(X^n-1)} \\ c = (c_0, \cdots, c_{n-1}) & \leftrightarrow & c(X) = c_0 + \cdots + c_{n-1}X^{n-1} & \leftrightarrow & \overline{c(X)} = c_0 + c_1\overline{X} + \cdots + c_{n-1}\overline{X^{n-1}} \end{array}$$

On associe à $c \in \mathcal{C}$ le polynôme $\overline{c(X)} \in \mathbb{F}_q[X]_{/(X^n-1)}$.
On associe à $c^\pi \in \mathcal{C}$ le polynôme

$$\overline{c^\pi}(X) = c_{n-1} + c_0\overline{X} + \cdots + c_{n-2}\overline{X}^{n-1} = c_{n-1}\overline{X}^n + c_0\overline{X} + \cdots + c_{n-2}\overline{X}^{n-1}$$

$$\begin{aligned} \overline{c^\pi}(X) &= \overline{X}\left(c_0 + c_1\overline{X} + \cdots + c_{n-1}\overline{X}^{n-1}\right) \\ &= \overline{X} \cdot \overline{c(X)} \end{aligned}$$

Définissons :

$$\overline{\mathcal{C}}(X) = \left\{ c_0 + c_1\overline{X} + \cdots + c_{n-1}\overline{X}^{n-1} | c = (c_0, \cdots, c_{n-1}) \in \mathcal{C} \right\}$$

On a une caractérisation des codes cycliques :

$$\begin{aligned} \mathcal{C} \text{ cyclique } &\Leftrightarrow \forall \overline{c}(X) \in \overline{\mathcal{C}}(X), \overline{c^{\pi}(X)} \in \overline{\mathcal{C}}(X) \\ &\Leftrightarrow \forall \overline{c}(X) \in \overline{\mathcal{C}}(X), \overline{Xc(X)} \in \overline{\mathcal{C}}(X) \end{aligned}$$

Lemme 3.1.

Soit $\mathcal{C}$ un code linéaire de longueur n sur $\mathbb{F}_q$.
$\mathcal{C}$ est cyclique ssi $\overline{\mathcal{C}}(X)$ est un idéal de $\mathbb{F}_q[X]_{/(X^n-1)}$

Démonstration.

$\Rightarrow$

Montrons que : $\forall \overline{a}(X) \in \mathbb{F}_q[X]_{/(X^n-1)}, \forall c(X) \in \overline{\mathcal{C}}(X)$
$\overline{a}(X)\overline{c}(X) \in \overline{\mathcal{C}}(X)$
$\mathcal{C}$ est cyclique donc $\forall \overline{c}(X) \in \overline{\mathcal{C}}(X)$, $\overline{X}\overline{c}(X) \in \overline{\mathcal{C}}(X)$
donc $\overline{X}\left(\overline{X} \cdot \overline{c}(X)\right) \in \overline{\mathcal{C}}(X)$
donc...$\forall i \in \mathbb{N}\ \overline{X}^i\overline{c}(X) \in \overline{\mathcal{C}}(X)$
Or, $\mathcal{C}$ est linéaire donc $\forall \overline{a}(X) = \overline{a_0 + a_1X + \cdots + a_{n-1}X^{n-1}} \in \mathbb{F}_q[X]_{/(X^n-1)}$

$$\overline{a}(X)\overline{c}(X) = a_0\overline{c}(X) + a_1X\overline{c}(X) + \cdots + a_{n-1}X^{n-1}\overline{c}(X) \in \overline{\mathcal{C}}(X)$$

$\Leftarrow$

Comme $\overline{\mathcal{C}}(X)$ est un idéal de $\mathbb{F}_q[X]_{/(X^n-1)}$,

$$\forall \overline{c}(X) \in \overline{\mathcal{C}}(X), \overline{X} \cdot \overline{c}(X) \in \overline{\mathcal{C}}(X)$$

□

L'anneau $\mathbb{F}_q[X]_{/(X^n-1)}$ est un anneau non intègre dont tous les idéaux sont principaux, ce qui va permette de caractériser les codes cycliques.

Théorème 3.1.

Soit $\mathcal{C}$ un code cyclique de longueur n sur $\mathbb{F}_q$
Soit $\overline{\mathcal{C}}(X)$ l'idéal associé à $\mathcal{C}$ (dans $\mathbb{F}_q[X]_{/(X^n-1)}$)
Soit $\overline{g(X)}$ un polynôme de $\overline{\mathcal{C}}(X)$ de plus petit degré et unitaire.
Soit r son degré.

1. $\overline{g}(X)$ engendre $\overline{\mathcal{C}}(X)$ (comme idéal de $\mathbb{F}_q[X]_{/(X^n-1)}$)
2. $g(X)$ est l'unique polynôme unitaire de degré r tel que $\overline{g(X)} \in \overline{\mathcal{C}}(X)$
3. $g(X)$ divise $X^n - 1$ (dans $\mathbb{F}_q[X]$)

Démonstration.

1. Soit $\overline{a}(X) \in \overline{\mathcal{C}}(X)$.
   Effectuons la division euclidienne de $a(X)$ par $g(X)$ dans $\mathbb{F}_q[X]$
   $$a(X) = g(X) \cdot Q(X) + R(X)$$
   avec $Q(X), R(X) \in \mathbb{F}_q[X]$ et $R(X) = 0$ ou $\deg(R(X)) < r$
   On a $\underbrace{\overline{a}(X)}_{\in\overline{\mathcal{C}}(X)} - \underbrace{\overline{g}(X)}_{\in\overline{\mathcal{C}}(X)} \cdot \underbrace{\overline{Q}(X)}_{\in\mathbb{F}_q[X]_{/(X^n-1)}} = \overline{R}(X)$
   donc $\overline{R}(X) \in \overline{\mathcal{C}}(X)$
   Or r est le plus petit degré des polynômes non nuls de $\overline{\mathcal{C}}(X)$ donc $\deg\left(\overline{R}(X)\right) \geqslant r$ ou $\overline{R}(X) = 0$
   Or $R(X) = 0$ ou $\deg(R(X)) < r$ donc $R = 0$ et $\overline{a}(X) = \overline{g}(X) \cdot \overline{Q}(X)$
2. Soit $g'(X)$ tel que $\deg(g'(X)) = r$, $g'(X)$ unitaire et $\overline{g'(X)} \in \overline{\mathcal{C}}(X)$
   $\overline{g}(X) - \overline{g'(X)} \in \overline{\mathcal{C}}(X)$ et $\deg(g - g') < r$ et par définition de r :
   $$g - g' = 0$$
3. Effectuons la division euclidienne de $X^n - 1$ par $g(X)$ dans $\mathbb{F}_q[X]$:
   $$X^n - 1 = g(X) \cdot Q(X) + R(X)$$
   avec $Q(X), R(X) \in \mathbb{F}_q[X]$ et $\deg(R) < r$ ou $R = 0$.
   On a $\overline{0} = \overline{g}(X) \cdot \overline{Q}(X) + \overline{R}(X)$.
   Comme $\overline{g}(X) \in \overline{\mathcal{C}}(X)$ et $\overline{Q}(X) \in \mathbb{F}_q[X]_{/(X^n-1)}$, $\overline{g}(X) \cdot \overline{Q}(X) \in \overline{\mathcal{C}}(X)$ (idéal de $\mathbb{F}_q[X]_{/(X^n-1)}$).
   Donc $\overline{R}(X) \in \overline{\mathcal{C}}(X)$
   Donc $R = 0$ ou $\deg(R) \geqslant r$
   donc par définition de R, $R = 0$.

□

Dans la suite on identifiera :

$$c = (x_0, \cdots, c_{n-1}) \in \mathbb{F}_q^n$$

et

$$c_0 + \cdots + c_{n-1}X^{n-1} \in \mathbb{F}_q[X]_{/(X^n-1)}$$

On note $\mathcal{C}(X) = \left\{ c(X) \in \mathbb{F}_q[X]_{/(X^n-1)} \,|c \in \mathcal{C} \right\}$

Exemple 3.1.

1. *Soit* $n \in \mathbb{N}^*$.
   $X-1|X^n-1$ *dans* $\mathbb{F}_2[X]$ *donc* $X+1$ *engendre un code cyclique* $\mathcal{C}$ *de longueur* n *sur* $\mathbb{F}_2$
   Soit $x \in \mathbb{F}_2^n$

$$\begin{aligned} c \in \mathcal{C} &\Leftrightarrow X+1|c(X) \ \textit{dans}\ \mathbb{F}_2[X] \\ &\Leftrightarrow c(1) = 0 \\ &\Leftrightarrow c_0 + c_1 + \cdots + c_{n-1} = 0 \ \textit{dans}\ \mathbb{F}_2 \\ &\Leftrightarrow c = (c_0, \cdots, c_{n-2}) \cdot \left(\begin{array}{c|c} & 1 \\ I_{n-1} & \vdots \\ & 1 \end{array} \right) \end{aligned}$$

   donc $\mathcal{C}$ *est un code de parité* $[n, n-1, 2]_2$

2. *soit* $n \in \mathbb{N}^*$, *soit* $g(X) = \sum_{i=0}^{n-1} X^i \in \mathbb{F}_2[X]$
   $g(X)\,|X^n+1$ *car* $X^n+1 = (X+1)\,g(X)$
   Soit $c \in \mathbb{F}_2^n$

$$c \in \mathcal{C} \Leftrightarrow \sum_{i=0}^{n-1} X^i | c(X)$$

   Or $\deg(c(X)) \leqslant n-1$ *donc*

$$\begin{aligned} c \in \mathcal{C} &\Leftrightarrow c(X) = \lambda \cdot \sum_{i=0}^{n-1} X^i \ \textit{où}\ \lambda \in \{0,1\} \\ &\Leftrightarrow c = (0, \cdots, 0) \ \textit{ou}\ c = (1, \cdots 1) \end{aligned}$$

   $\mathcal{C}$ *est un code de répétition* $[n, 1, n]_2$

3. $n = 7$, $q = 2$
$X^7 + 1$, *comment factoriser ?*

$$7 = 2^3 - 1$$

Or on sait que $X^{2^n} - X = \prod_{\substack{f \text{ irré} \\ \deg(f)=d, d|n}} f$

Donc $X^{2^n-1} - 1 = \prod_{\substack{f \text{ irré}, f \neq X \\ \deg(f)=d, d|n}} f$

Les irréductibles de degré 3 *sur* $\mathbb{F}_2$ *:*

$$X^3 + ? + 1$$

$$X^3 + X^2 + 1, X^3 + X + 1$$

Donc :

$$X^7 + 1 = (X+1)\left(X^3 + X + 1\right)\left(X^3 + X^2 + 1\right)$$

Les codes cycliques de longueur 7 *sont engendrés par :*
$1, X+1, X^3+X+1, X^3+X^2+1, (X+1)(X^3+X+1), (X+1)(X^3+X^2+1), \left(X^3+X+1\right)\left(X^3+X^2+1\right), X^7+1$
Notons $\mathcal{C}$ *le code cyclique de longueur* 7 *engendré par* $g(X) = X^3 + x + 1$.
Soit $c \in \mathbb{F}_2^7$

$$c \in \mathcal{C} \Leftrightarrow X^3 + X + 1 | c(X)$$

Soit $\alpha \in \mathbb{F}_{2^3}$ *tel que :*

$$\alpha^3 + \alpha + 1 = 0$$

$$X^3+X+1=(X+\alpha)\left(X+\alpha^2\right)\left(X+\alpha^4\right)$$

$$\begin{aligned}
c\in\mathcal{C} &\Leftrightarrow X^3+X+1|c(X)\\
&\Leftrightarrow (X+\alpha)\left(X+\alpha^2\right)\left(X+\alpha^4\right)|c(X)\\
&\Leftrightarrow \begin{cases} X+\alpha|c(X)\\ X+\alpha^2|c(X)\\ X+\alpha^4|c(x)\end{cases}\\
&\Leftrightarrow \begin{cases} c(\alpha)=0\\ c\left(\alpha^2\right)=0\\ x\left(\alpha^4\right)=0\end{cases}\\
&\Leftrightarrow c(\alpha)=0 \text{ car on est sur } \mathbb{F}_2^7[X]\\
&\Leftrightarrow c_0+c_1\alpha+\cdots c_6\alpha^6=0\\
&\Leftrightarrow c_0+c_1\alpha+c_2\alpha^2+c_3(\alpha+1)+c_4\left(\alpha^2+\alpha\right)+c_5\left(\alpha^2+\alpha+1\right)+c_6\left(\alpha^2+1\right)=0\\
&\Leftrightarrow (c_0+c_3+c_5+c_6)+(c_1+c_3+c_4+c_5)\alpha+(c_2+c_4+c_5+c_6)\alpha^2=0\\
&\Leftrightarrow \begin{cases} c_0+c_3+c_5+c_6=0\\ c_1+c_3+c_4+c_5=0\\ c_2+c_4+c_5+c_6=0\end{cases}\\
&\Leftrightarrow \begin{pmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{pmatrix}\begin{pmatrix}c_0\\c_1\\\vdots\\c_6\end{pmatrix}=0
\end{aligned}$$

À permutation des colonnes près, on obtient la matrice de contrôle du code de Hamming $\mathcal{H}_3$

$$\begin{aligned}
&\alpha^0=1\\
&\alpha^1\\
&\alpha^2\\
&\alpha^3=\alpha+1\\
&\alpha^4=\alpha^2+\alpha\\
&\alpha^5=\alpha^2+\alpha+1\\
&\alpha^6=\alpha^2+1\\
&\alpha^7=1
\end{aligned}$$

4. *Soit $n\in\mathbb{N}^*$ tel que $n|q-1$, $k\in[\![0,n]\!]$ et α une racine primitive $n-$ième de l'unité dans $\mathbb{F}_q$.*

Soit $b \in \mathbb{N}$ et on prend le polynôme :

$$g(X) = \left(X - \alpha^b\right)\left(X - \alpha^{b+1}\right)\cdots\left(X - \alpha^{n-k-1}\right)$$

$g(X)$ divise $X^n - 1$ (donc $X - \alpha^i | X^n - 1$ pour $b \leqslant i \leqslant b + n - k - 1$ et $\alpha^i \neq \alpha^j$ pour $i \neq j \in \{b, \cdots, b + n - k - 1\}$
$g(X)$ engendre un code cyclique $\mathcal{C}$ de longueur n
$\forall c \in \mathbb{F}_q^n$,

$$\begin{aligned} c \in \mathcal{C} &\Leftrightarrow g(X) \,|\, c(X) \\ &\Leftrightarrow c\left(\alpha^i\right) = 0, \forall i \in \{b, \cdots, b + n - k - 1\} \\ &\Leftrightarrow \begin{pmatrix} 1 & \alpha^b & \cdots & \left(\alpha^b\right)^{n-1} \\ 1 & \alpha^{b+1} & \cdots & \left(\alpha^{b+1}\right)^{n-1} \\ \vdots & & & \\ 1 & \alpha^{b+n-k-1} & \cdots & \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0 \end{aligned}$$

$\mathcal{C}$ est un code de Reed-Solomon de localisation $\left(1, \alpha, \cdots, \alpha^{n-1}\right)$ et de multiplicateurs $\left(1, \alpha^b, \cdots, \alpha^{(n-1)b}\right)$

II Matrice génératrice et matrice de contrôle.

Soit $\mathcal{C}$ un code cyclique de longueur n sur $\mathbb{F}_q$, de polynôme générateur $g(X)$ avec $\deg(g(X)) = r$
On note $k \in \mathbb{N}^*$ tel que $n - k = r$
Les mots $g(X), Xg(X), \cdots, X^{k-1}g(X)$ sont des mots de $\mathcal{C}$ et forment une base.
En effet ils sont linéairement indépendant (forme échelonnée en degré)
Soit $c(X) \in \mathcal{C}(X)$, soit $m(X)$ tel que $c(X) = m(X)\,g(X)$ avec $\deg(m) \leqslant n - r - 1 \leqslant k - 1$

$$c(C) = m_0 g(X) + \cdots + m_{k-1} X^{k-1} g(X)$$

Donc cette famille est génératrice, comme elle est libre, $\left(g, Xg, \cdots, X^{k-1}g\right)$ forme une base de $\mathcal{C}$. ne matrice génératrice en prenant $\left(1, X, \cdots, X^{n-1}\right)$ comme base de départ et $g(X), \cdots X^{k-1}g(X)$ en base d'arrivée :

$$\begin{pmatrix} g_0 & g_1 & \cdots & \cdots & g_{r-1} & 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & & & \ddots & \ddots & \ddots & \vdots & & \\ & & & & & & & & & 0 \\ 0 & \cdots & & & g_0 & & & & g_{r-1} & 1 \end{pmatrix}$$

On a $c = mG$ où $m = (m_0, \cdots, m_{k-1})$
$\mathcal{C}$ est un code $[n,k]_q$

$$\mathcal{C} = \left\{mG | m \in \mathbb{F}_q^k\right\} = \left\{ \underbrace{m(X)\, g(X)}_{\deg < n} | m(X) \in \mathbb{F}_q[X], \deg(m(X)) k \right\}$$

Autre matrice génératrice
On a : $X^i = g(X) Q_i(X) + R_i(X)$ pour $0 \leqslant i \leqslant k-1$ avec $\deg R_i(X) < n-k$
$X^{i+r} - R_i(X) = g(X) Q_i(X) \in \mathcal{C}(X)$ et $\left(X^{i+r} - R_i(X)\right)_{0 \leqslant i \leqslant k-1}$ est libre.
Donc une matrice génératrice de $\mathcal{C}$ est du type :

$$\left(\begin{array}{c|c} -R_0 & \\ -R_1 & \\ & I \\ \vdots & \\ -R_{k-1} & \end{array}\right)$$

en prenant pour base de départ $\left(1, \cdots, X^{r-1}, X^r, \cdots, X^{n-1}\right)$.

Exemple 3.2.
$q-2, n-7, g = X^3 + X + 1$
Première matrice génératrice :

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

Deuxième matrice génératrice :

$$\begin{aligned} X^3 &\mod X^3 + X + 1 = X + 1 \\ X^4 &\mod X^3 + X + 1 = X^2 + 1 \\ X^5 &\mod X^3 + X + 1 = X^3 + X^2 \mod X^3 + X + 1 = X^2 + X + 1 \\ X^6 &\mod X^3 + X + 1 = X^4 + X^3 \mod X^3 + X + 1 \\ &= X^2 + 1 + X^3 \mod X^3 + X + 1 = X^2 + 1 \end{aligned}$$

$$G' = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad X^n - 1 = g(X) h(X)$$

Soit $h(x) \in \mathbb{F}_q[X]$ unitaire de degré k tel que :

$$h(X) \cdot g(X) = X^n$$

Le polynôme $h(X)$ est appelé **polynôme de contrôle**.
Soit $c \in \mathcal{C}$, soit $m(X) \in \mathbb{F}_q[X]$ tel que :

$$c(X) = m(X)\, g(X)$$

Alors $c(X) \cdot h(X) = m(X) \cdot g(X) h(X) = m(X)(X^n - 1) = 0$ dans $\mathbb{F}_q[X]_{/(X^n-1)}$
$\forall c \in \mathcal{C}$

$$c(X) \cdot h(X) \equiv 0 \,[X^n - 1]$$

Soit $a(X) = c(X) \cdot h(X) = \sum_{i=0}^{n+k-1} a_i X^i$
On a $a(X) \equiv 0\,[X^n - 1]$ et $\forall l \in [\![0, n+k-1]\!]$:

$$a_l = \sum_{\substack{0 \leqslant i \leqslant k \\ 0 \leqslant l-i \leqslant n-1}} h_i \cdot c_{l-i}$$

L'indiçage équivaut à : $\max(0, l-n+1) \leqslant i \leqslant \min(k, l)$

$$\begin{aligned} a(X) &= \sum_{i=0}^{n-1} a_i X^i + \sum_{i=n}^{n+k-1} a_i X^i \\ &= \sum_{i=0}^{n-1} a_i X^i + \sum_{i=0}^{k-1} a_{n+i} X^{n+i} \\ &\equiv \sum_{i=0}^{k-1} (a_i + a_{i+n}) X^i + \sum_{i=k}^{n-1} a_i \cdot X^i \,[X^n - 1] \end{aligned}$$

NB : degré de a ? g est de degré au plus $n-k$, donc h est de degré au plus k, comme $c = (c_0, \cdots, c_{n-1})$ c est de degré au plus $n-1$ donc $c \cdot h$ est de degré au plus $n+k-1$
On a $a(X) \equiv 0\,[X^n - 1]$ donc :
$\sum_{i=0}^{k-1} (A_i + a_{i+n}) X^i + \sum_{i=k}^{n-1} a_i X^i = 0$
En particulier $\forall l \in [\![k, n-1]\!], a_l = 0$
$\forall k \in [\![k, n-1]\!], a_l = \sum_{max(0,l-n+1) \leqslant i \leqslant \min(k,l)} h_i \cdot c_{l-i}$

Donc $\begin{cases} \forall l \in \{k, \cdots, n-1\} : \\ \sum_{i=0}^{k} h_i \cdot c_{l-i} = 0 \end{cases}$

On a donc $\forall c \in \mathbb{F}_q^n$: (on va de $l = k$ à $n-1$

$$c \in \mathcal{C} \Rightarrow \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & & & 0 \\ 0 & h_k & \cdots & & & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_0 & 0 & \cdots & & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ & & & & & & & & 0 \\ 0 & \cdots & & 0 & & & h_k & \cdots & h_0 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ \vdots c_{n-1} \end{pmatrix}$$

Théorème 3.2.

Soit $\mathcal{C}$ un code cyclique de longueur n, dimension k et polynôme générateur $g(X)$ ($\deg(g) = n-k, g$ unitaire).
Soit $h(x) = X^k + \cdots + h_1 X + h_0$ le polynôme de contrôle de $\mathcal{C}$.
Une matrice de contrôle de $\mathcal{C}$ est :

$$\begin{pmatrix} 1 & h_{k-1} & \cdots & h_0 & 0 & \cdots & & & 0 \\ 0 & 1 & \cdots & & & h_0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & h_0 & 0 & \cdots & & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ & & & & & & & & 0 \\ 0 & \cdots & & 0 & & & 1 & \cdots & h_0 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ \vdots c_{n-1} \end{pmatrix}$$

Démonstration.

- H possède $n-k$ liges linéairement indépendantes, donc $\mathrm{Rg}(H) = n-k$
- $\forall c \; in\mathcal{C} \; H \cdot {}^t c = 0$ (d'après $(*)$)
  Donc $\mathcal{C}$ est inclus dans le code $\mathcal{C}'$ de matrice de contrôle H.
- $\dim(\mathcal{C}) = k$, $\dim(\mathcal{C}') = \dim(\ker(H)) = n - (n-k) = k$
- Conclusion : $\mathcal{C} = \mathcal{C}'$

□

Remarque 3.1.
Le dual de $\mathcal{C}$ a pour matrice génératrice H, $\mathcal{C}'$ est donc un code cyclique de

longueur n et de polynôme générateur

$$1 + h_{k-1}X + \cdots + h_1X^{k-1} + h_0X^k = \underbrace{X^k h\left(\frac{1}{X}\right)}_{\text{polynôme réciproque de}} \quad k$$

On a bien $X^k h\left(\frac{1}{X}\right) | X^n - 1$.
En effet $g(X) \cdot h(X) = X^n - 1$ *donc*

$$\begin{aligned} X^k h\left(\frac{1}{X}\right) \cdot X^{n-k} g\left(\frac{1}{X}\right) &= X^n \cdot \left(\frac{1}{X^n} - 1\right) \\ &= 1 - X^n \end{aligned}$$

Exemple 3.3.

1. *$q = 2$ $g(X) = X + 1$ $\mathcal{C}$ code cyclique de longueur n et polynôme générateur g.*
   Le polynôme de contrôle de $\mathcal{C}$ est $h(X) = \sum_{i=0}^{n-1} X^i$ *($h(X) \cdot g(X) = X^n - 1$)*
   Le dual de $\mathcal{C}$ est le code cyclique de polynôme générateur :

$$X^{n-1} h\left(\frac{1}{X}\right) = h(X) \text{ (code de répétition)}$$

2. *$q = 2$, $n = 7$ $g = X^3 + X + 1$*

$$\left(X^7 + 1\right) = (X + 1)\left(X^3 + X + 1\right)\left(X^3 + X^2 + 1\right)$$

$$\begin{aligned} h &= (X + 1)\left(X^3 + X^2 + 1\right) \\ &= X^4 + X63 + X + X^3 + X^2 + 1 \\ &= X^4 + X^2 + X + 1 \end{aligned}$$

Une matrice de contrôle est $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$

III Factorisation de $X^n - 1$.

On suppose que n et q premiers entre eux.(alors $X^n - 1$ est sans facteur carré).
On veut factoriser $X^n - 1$ sur une extension de $\mathbb{F}_q$ en produit de facteurs linéaires.
Pour cela, on va chercher le corps fini (extension de $\mathbb{F}_q$) contenant les racines $n-$ième de 1.
Soit m le plus petit entier non nul tel que $n|q^m - 1$: c'est l'ordre multiplicatif de q modulo n.
alors : $X^n - 1|X^{q^m-1} - 1$
donc les racines de $X^n - 1$ sont dans $\mathbb{F}_{q^m}$
soit α une racine primitive $n-$ième de 1 dans $\mathbb{F}_{q^m}$.
Donc on a $X^n - 1 = \prod_{i=0}^{n-1} (X - \alpha_i)$ (factorisation dans $\mathbb{F}_{q^m}[X]$
On va chercher à rassembler les facteurs linéaires pour obtenir une factorisation dans $\mathbb{F}_q[X]$

Définition 3.2.

Soit $s \in \{0, \cdots, n-1\}$
La **q-classe cyclotomique de s modulo n** est :

$$C(s) = \left\{ s, \underset{\text{mod } n}{s \cdot q}, \underset{\text{mod } n}{s \cdot q^2}, \cdots, \underset{\text{mod } n}{s \cdot q^{m_s-1}} \right\}$$

où m_s est le plus petit entier non nul tel que $s \cdot q^{m_s-1} \equiv s\,[n]$ Les classes cyclotomiques forment une partition de $\{0, \cdots, n-1\}$
On définit :

$$M_{\alpha^s}(X) = \prod_{i \in C(s)} \left(X - \alpha^i\right)$$

On a $X^n - 1 = \prod_S M_{\alpha^s}(X)$ où s parcourt les représentants des classes cyclotomiques.

A-t-on une factorisation sur $\mathbb{F}_q[X]$ en produit d'irréductibles ?

Proposition 3.1.

$M_{\alpha^s}(X)$ est un polynôme irréductible de $\mathbb{F}_q[X]$ (polynôme minimal de α^s sur $\mathbb{F}_q$)

Démonstration.
$\sigma : \begin{array}{ccc} \mathbb{F}_{q^m} & \to & \mathbb{F}_{q^m} \\ a & \mapsto & a^q \end{array}$ est un automorphisme laissant fixes les éléments de $\mathbb{F}_q$.
$\forall a \in \mathbb{F}_{q^m}$:

$$a \in \mathbb{F}_q \Leftrightarrow a^q = a$$

Montrons que $\forall i \in \{0, \cdots m_s\}, a_i \in \mathbb{F}_q$

$$\begin{aligned} M_{\alpha^s}(X) &= \prod_{i \in C(s)} \left(X - \alpha^i\right) \text{ par définition} \\ &= \sum_{i=0}^{m_s} a_i X^i \\ M_{\alpha^s}(X)^q &= \left(\sum_{i=0}^{m_s} a_i X^i\right)^q \\ &= \sum_{i=0}^{m_s} a_i^q X^{q \cdot i} \end{aligned}$$

Montrons que $M_{\alpha^s}(Q)^q = M_{\alpha^s}(X^q)$
et $M_{\alpha^s}(X^q) = \sum_{i=0}^{m_s} a_i X^{qi}$
Or

$$\begin{aligned} M_{\alpha^s}(X)^q &= \prod_{i \in C(s)} \left(X - \alpha^i\right)^q \\ &= \prod_{i \in C(s)} \left(X^q - \alpha^{iq}\right) \\ &= \prod_{i \in C(s)} \left(X^q - \alpha^{iq \mod n}\right) \\ &= \prod_{j \in C(s)} \left(X^q - \alpha^j\right) \\ &= M_{\alpha^s}(X^q) \end{aligned}$$

car $\alpha^n = 1$
Donc $M_{\alpha^s}(X) \in \mathbb{F}_q[X]$

Soit f irréductible dans $\mathbb{F}_q[X]$ divisant $M_{\alpha^s}(X)$
Or $M_{\alpha^s}(X) = \prod_{i \in C(s)} \left(X - \alpha^i\right)$
Donc $\exists i \in C(s)$ tel que $f\left(\alpha^i\right) = 0$
donc $\exists i \in C(s)$ tel que $f\left(\alpha^i\right) = 0$ et $f\left(\alpha^i\right)^q = f\left(\alpha^{iq}\right) = 0$ car $f \in \mathbb{F}_q[X]$
donc $\exists i \in C(s)$:

$$\begin{aligned} f\left(\alpha^i\right) &= f\left(\alpha^{qi}\right) \\ &= f\left(\alpha^{q^2 i}\right) \\ &= \cdots \\ &= 0 \end{aligned}$$

donc $\forall i \in C(s), f\left(\alpha^i\right) = 0$
Donc $f = M_{\alpha^s}(X)$ □

Exemple 3.4.
$q = 2$ $n = 7 = 2^3 - 1$
$\mathbb{F}_{2^3} \simeq \mathbb{F}_2[X]_{/(X^3+X+1)}$
Soit $\alpha \in \mathbb{F}_{2^3}$ tel que $\alpha^3 + \alpha + 1 = 0$ alors $\alpha^7 = 1$ ($\alpha \in \mathbb{F}_{2^3}$), or 7 est premier donc α est une racine primitive 7-ème de l'unité.

$$X^7 - 1 = \prod_{i=0}^{6} \left(X - \alpha^i\right)$$

$C(0) = \{0\}$ *on aura un polynôme de degré* 1
$C(1) = \{1, 2, 4\}$ *on aura un polynôme de degré* 3
$C(3) = \{13, 6, 5\}$ *on aura un polynôme de degré* 3

$M_{\alpha^1} = \left(X - \alpha^1\right)\left(X_\alpha^2\right)\left(X - \alpha^4\right)$
$M_{\alpha^3} = \left(X - \alpha^3\right)\left(X - \alpha^5\right)\left(X - \alpha^6\right)$

$$X^7 - 1 = \underbrace{\left(X - \alpha^0\right)}_{=X+1} \underbrace{\left(X - \alpha\right)\left(X - \alpha^2\right)\left(X - \alpha^4\right)}_{=X^3+X+1} \left(X - \alpha^3\right)\left(X - \alpha^5\right)\left(X - \alpha^6\right)$$

$$\begin{aligned} M_{\alpha^3} &= \left(X - \alpha^3\right)\left(X - \alpha^5\right)\left(X - \alpha^6\right) \\ &= \left(X^+ \underbrace{\left(\alpha^3 + \alpha^5\right)}_{=\alpha^2} X + \alpha\right)\left(X + \alpha^6\right) \quad = X^3 + \alpha^2 X^2 + \alpha X + \alpha^6 X^2 + \alpha X + 1 \\ &= X^3 + \left(\alpha^2 + \alpha^6\right) X^2 + 1 \\ &= X^3 + X^2 + 1 \end{aligned}$$

Exemple avec $q = 2$ *et* $n = 5$
$2^4 \equiv 1\,[5]$, $2^2 \equiv -1\,[5] \not\equiv 1\,[5]$
On cherche une racine primitive 5*-ème de* 1 *dans* $\mathbb{F}_{2^4}$

$$\mathbb{F}_{2^4} \equiv \mathbb{F}_2\,[X]_{/(X^4+X+1)}$$

Irréductible de degré 4 *:*
Pas être divisible par X *ou* $X+1$ *: constante égale à* 1 *et nombre impair de terme.*
Pas être divisible pas X^2+X+1*.*

- X^4+X+1
- $\cancel{X^4+X^2+1} = \left(X^2+X+1\right)^2$
- X^4+X^3+1
- $X^4+X^3+X^2+X+1$

Soit $\alpha \in \mathbb{F}_{2^4}$ *tel que* $\alpha^4+\alpha+1=0$
$\alpha^5 = \alpha^2+\alpha$ *donc* α *racine primitive* $15-$*ème de l'unité.*
Si $g(\alpha)=0$, $g \in \mathbb{F}_q[X]$
Alors $g(\alpha) = g\left(\alpha^i\right) = \cdots = 0$
$g\left(\alpha^i\right) = 0\ \forall i \in C(1)$
f *irréductible* $\in \mathbb{F}_q[X]$ *tel que* $f(\alpha)=0$ $f = \prod_{i \in C(1)} \left(X-\alpha^i\right)$

$$g \in \mathbb{F}_q[X] \ \ tq\ g(\alpha)=0$$

alors $\forall i \in C(1), g\left(\alpha^i\right) = 0 \Leftrightarrow X-\alpha^i | g$
Soit $\xi = \alpha^5$
Alors $\xi^5 = 1$ *et* $\forall i \in \{1,\cdots,4\}$ $\xi^i \neq 1$

$$X^5-1 = \prod_{i=0}^{4} \left(X-\xi^i\right)$$

$C(0) = \{0\}$
$C(1) = \{1,2,4,3\}$
$X^5+1 = \left(X-\xi^0\right)\left(X-\xi^1\right)\left(X-\xi^2\right)\left(X-\xi^3\right)\left(X-\xi^4\right) = (X-1)\left(X^4+X^3+X^2+X+1\right)$

Chapitre 4

Codes BCH

I Principe (cas linéaire)

On va chercher à construire des codes dont on connaît à l'avance une borne de la distance, tout en restant dans $\mathbb{F}_2$.

On sait : construire une famille de codes binaires qui corrige 1-correcteur d'erreur de longueur $2^r - 1$ ($r \geqslant 2$)

On veut : construire un code binaire, 2-correcteur d'erreurs de longueur $2^r - 1$ (dans $\mathbb{F}_2$)

On aura besoin de se placer dans une extension de $\mathbb{F}_2$.
On rappelle que le code binaire de Hamming, de longueur $n = 2^r - 1$ ($r \geqslant 2$), est défini par une matrice de contrôle :

$$\left(\begin{array}{c|c|c} H_1 & \cdots & H_n \end{array} \right)$$

où pour $i \in \{1, \cdots, n\}$, H_i provient de la décomposition de i en base 2.
Ces colonnes sont les vecteurs non nuls de $(\mathbb{F}_2)^r$ rangé dans un certain ordre.
À permutation des colonnes près, on va considérer une autre matrice de contrôle H où on rangera dans l'ordre suivant :

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \end{pmatrix} \in \mathcal{M}_{1,n}(\mathbb{F}_{2^r})$$

où α est racine d'un polynôme irréductible P de $\mathbb{F}_2[X]$ de degré r et α est d'ordre n.

$$\alpha \in \mathbb{F}_{2^r} \simeq \mathbb{F}_2[X]_{/(P)}$$

Exemple 4.1 (Un petit exemple pour $r = 3$, $n = 7$)**.**
Matrice de contrôle du code de Hamming de longueur 7 *:*

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \in \mathcal{M}_{3,7}(\mathbb{F}_2)$$

Soit $\alpha \in \mathbb{F}_{2^3}$ *tel que* $\alpha^3 + \alpha + 1 = 0$
Considérons $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix} \in \mathcal{M}_{1,7}(\mathbb{F}_{2^3})$
Soit c *dans le code de matrice de contrôle* H *:*

$$\begin{aligned} H \cdot c = 0 \Leftrightarrow \sum_{i=0}^{6} c_i \alpha^i = 0 \\ \Leftrightarrow c_0 + c_1\alpha + c_2\alpha^2 + c_3(1+\alpha) + c_4\left(\alpha + \alpha^2\right) + c_5\left(\alpha^2 + \alpha + 1\right) + c_6\left(1 + \alpha^2\right) = 0 \\ \Leftrightarrow (c_0 + c_3 + c_5 + c_6) + (c_1 + c_3 + c_4 + c_5)\alpha + (c_2 + c_4 + c_5 + c_6)\alpha^2 = 0 \\ \Leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ \vdots \\ c_6 \end{pmatrix} = 0 \end{aligned}$$

En prenant la base d'arrivé $\left(1, \alpha, \cdots, \alpha^6\right)$ *et la base d'arrivée* $\left(1, \alpha, \alpha^2\right)$
Maintenant *soit* $\mathcal{C}$ *le code définie sur* $\mathbb{F}_2$ *de matrice de contrôle :*

$$H = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \end{pmatrix} \in \mathcal{M}_{1,n}(\mathbb{F}_{2^r})$$

$$\mathcal{C} = \left\{ c \in \mathbb{F}_2^n | H \cdot^t c = 0 \right\}$$

Soit $y = c + e$ *avec* $c \in \mathcal{C}$ *et* $w(e) \leqslant 1$
Soit :

$$\begin{aligned} S = H \cdot^t y = \underbrace{H \cdot^t c}_{=0} + H \cdot^t e \\ = \begin{cases} 0 & si\ e = 0 \\ \alpha^i & si\ e = \left(0, \cdots, \underset{\substack{\uparrow \\ i+1}}{1}, 0, \cdots 0\right) \end{cases} \end{aligned}$$

Algorithme 4.1.

Entrée y tel que $y = c + e$, $c \in \mathcal{C}$ et $w(e) \leqslant 1$

Sortie c

1. $S \leftarrow H \cdot^t y$
2. Si $S = 0$ alors rendre (y)
3. Déterminer $i \in \{0, \cdots, n-1\}$ te lque $S = \alpha^i$ Et rendre $(y + e)$
   où $e = \left(0, \cdots, \underset{\substack{\uparrow \\ i+1}}{1}, 0, \cdots 0\right)$

Remarque 4.1. *Soit* $c \in \mathbb{F}_2^n$
O a $c \in \mathcal{C} \Leftrightarrow c(\alpha) = 0 \Leftrightarrow M_\alpha(X) | c(X)$
Si on prend $y(X) = c(X) + e(X)$ *où* $w(e) \leqslant 1$ *:*

1. $S \to y(\alpha)$
2. *Si* $S = 0$ *rendre* y
3. *déterminer* $i \in \{0, \cdots, n-1\}$ *tel que* $S = X^i$
   Rendre $\left(y(X) + X^i\right)$

Or $M_\alpha(X) | X^n - 1$ donc $\mathcal{C}$ est le code cyclique de longueur n et de polynôme générateur $G(X) = M_\alpha(X) = \text{ppcm}\left(M_\alpha(X), M_{\alpha^2}(X)\right)$ (c'est un code BCH)
Pour construire un code binaire 2-correcteur d'erreurs de longueur $n = 2^r - 1$ on a ajouter une ligne à H :

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ f(1) & f(\alpha) & & \cdots & f\left(\alpha^{n-1}\right) \end{pmatrix}$$

où $f : \mathbb{F}_{2^r} \to \mathbb{F}_{2^r}$
Soit $y = c + e$ avec $e(X) = X^i + X^j$ et $0 \leqslant i < j \leqslant n-1$

$$\begin{aligned} S &= H \cdot^t c + H \cdot^t e \\ & H \cdot^t e \\ &= \begin{pmatrix} \alpha^i + \alpha^j \\ f\left(\alpha^i\right) + f\left(\alpha^j\right) \end{pmatrix} \end{aligned}$$

Notons u et v les coordonnées de S.
Si $f = \text{Id}$ on n'a pas assez d'information
Si $f =: x \mapsto x^2$ on a : $\begin{cases} u = \alpha^i + \alpha^j \\ v = \alpha^{2i} + \alpha^{2j} = \left(\alpha^i + \alpha^j\right)^2 = u^2 \end{cases}$
Si $f : x \quad x^3$ on obtient : $\begin{cases} u = \alpha^i + \alpha^j \\ v = \alpha^{2i} + \alpha^{3j} = \left(\alpha^i\right)^3 + \left(\alpha^j\right)^3 = \left(\alpha^i + \alpha^j\right)^3 + \alpha^i\alpha^j\left(\alpha^i + \alpha^j\right) \end{cases}$
Ceci équivaut à $u = \alpha^i + \alpha^j$ et $c = u^3 + \alpha^i\alpha^j \cdot u$
Ce qui équivaut à $u = \alpha^i + \alpha^j$ et $\alpha^i\alpha^j = \dfrac{v + u^3}{u}$
α^i et α^j sont racines du polynôme $P(z) = z^2 + uz + \dfrac{v + u^3}{u}$

Algorithme 4.2.

Entrée : y tel que $y = c + e$ et $\begin{cases} c \in \mathcal{C} = \left\{ x \in \mathbb{F}_2^n \mid \underbrace{H}_{(*)} \cdot {}^t x = 0 \right\} \\ w(e) \leqslant 2 \end{cases}$

Sortie : c

1. $S \to H \cdot {}^t y$, $u, v \to$ coordonées de S
2. Si $S = 0$ alors rendre (y)
3. Si $v = u^3$ alors déterminer $i \in \{0, \cdots, n-1\}$ tel que $u = \alpha^i$
   rendre $(y + e)$ où $e = \left(0, \cdots, \underset{\substack{\uparrow \\ i+1}}{1}, 0 \cdots, 0\right)$
   En représentation polynomiale : rendre $(y(X) + e(X))$ où $e(X) = X^i$
4. $P \to z^2 + uz + \dfrac{v + u^3}{u}$
5. Déterminer $i < j \in \{0, \cdots, n-1\}$ tels que $P\left(\alpha^i\right) = P\left(\alpha^j\right) = 0$
6. Rendre $y + e$ $(y(X) + e(X)$ en représentation polynomiale) où $e = \left(0, \cdots, \underset{\substack{\uparrow \\ i+1}}{1}, 0 \cdots, 0, \underset{\substack{\uparrow \\ j+1}}{1}, 0 \cdots, 0\right)$ $(e(X) = X^i + X^j)$

$(*) : H = \begin{pmatrix} 1 & & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \cdots & \alpha^{3(n-1)} \end{pmatrix}$

Remarque 4.2.
On utilise parfois le réciproque de P :

$$P^* = 1 + uZ + \frac{v + u^3}{u} Z^2 = Z^2 P\left(\frac{1}{Z}\right)$$

et on cherche $i < j$ tel que $P^*\left(\alpha^{-i}\right) = P^*\left(\alpha^{-j}\right) = 0$
***Avantage :** Si $S \neq 0$ le degré de P^* fournit le nombre d'erreurs.*

Remarque 4.3.

Soit $c \in \mathbb{F}_2^n$

$$\begin{aligned} c \in \mathcal{C} &\Leftrightarrow \underbrace{\begin{pmatrix} c(\alpha) \\ c\left(\alpha^3\right) \end{pmatrix}}_{H \cdot {}^t c} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\ &\Leftrightarrow M_\alpha(X) \,|\, c(X) \;\; et \; M_{\alpha^3}(X) \,|\, c(X) \\ &\Leftrightarrow \underbrace{ppcm\left(M_\alpha(X), M_{\alpha^3}(X)\right)}_{divise\ X^n-1} \,|\, c(X) \end{aligned}$$

C'est donc un code cyclique de longueur n *et de polynôme générateur :*

$$\begin{aligned} g(X) &= ppcm\left(M_\alpha(X), M_{\alpha^3}(X)\right) \\ &= ppcm\left(M_\alpha(X), M_{\alpha^2}(X), M_{\alpha^3}(X), M_{\alpha^4}(X)\right) \end{aligned}$$

$M_\alpha(X), M_{\alpha^2}(X), M_{\alpha^3}(X), M_{\alpha^4}(X)$ *sont tous égaux.*
$i \in \{0, \cdots, r-1\}$ $3 \equiv 1 \times 2^i \mod n$ $(n = 2^r - 1)$

Exemple 4.2 (Exemple pour $r = 4$)**.**
On considère $\alpha \in \mathbb{F}_{2^4}$ *tel que* $\alpha^4 + \alpha + 1 = 0$
On a bien :

1. $X^4 + X + 1$ *irréductible dans* $\mathbb{F}_2[X]$

$$car \begin{cases} X^4 + X + 1 \mod X = 1 \neq 0 \\ X^4 + X + 1 \mod X + 1 = 1 \neq 0 \\ X^4 + X + 1 \mod X^2 + X + 1 = 1 \neq 0 \end{cases}$$

2. α *d'ordre* 15 *car :* $\alpha^3 \neq 0$ $\alpha^5 = \alpha^2 + \alpha \neq 1$

On considère le code sur $\mathbb{F}_2$ *de matrice de contrôle :*

$$H = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \cdots & \left(\alpha^3\right)^4 \end{pmatrix}$$

C'est-à-dire le code cyclique de longueur 15 *et de polynôme générateurs* $g(X) = M)_\alpha(X) M_{\alpha^3}(X)$
Que vaut $M_{\alpha^3}(X)$ *?*
$\left(\alpha^3\right)^5 = 1$ *donc* α^3 *est racine de* $X^5 + 1 = (X+1)\left(X^4 + X^3 + X^2 + X + 1\right)$
$\deg M_{\alpha^3}(X) = 4$ *car* $C(3) = \{3, 6, 12, 9\}$
Donc $M_{\alpha^3}(X) = X^4 + X^3 + X^2 + X + 1$
Soit $y = c + e$ *avec* $c \in \mathcal{C}$ *et* $e(X) = X^2 + X^6$.

$$Soit\ X = H \cdot {}^t y = \begin{pmatrix} \alpha^2 + \alpha^6 \\ \left(\alpha^3\right)^2 + \left(\alpha^3\right)^6 \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ \alpha^2 \end{pmatrix}$$

$u = \alpha^3$ *et* $v = \alpha^2$
On veut retrouver e *connaissant* u *et* v.

$$u^3 = \alpha^9 \neq v$$

Soit :

$$\begin{aligned}
P(Z) &= Z^3 + uZ + \frac{u^3 + v}{u} \\
&= Z^2 + \alpha^3 Z + \frac{\alpha^9 + \alpha^2}{\alpha^3} \\
&= Z^2 + \alpha^3 Z + \frac{\alpha^{11}}{\alpha^3} \\
&= Z^2 + \alpha^3 z + \alpha^8 \\
P\left(\alpha^0\right) &= 1 + \alpha^3 + \alpha^8 \\
&= \alpha^3 + \alpha^2 \neq 0 \\
P\left(\alpha^1\right) &= \alpha^2 + \alpha^4 + \alpha^8 \\
&= \alpha \neq 0 \\
P\left(\alpha^2\right) &= \alpha^4 + \alpha^5 + \alpha^8 \\
&= \alpha + 1 + \alpha^2 + \alpha + \alpha^2 + 1 \\
&= 0
\end{aligned}$$

Comme le produit des racines de P *est* α^8, *on a* $P\left(\alpha^6\right) = 0$
On a donc :

$$e(X) = X^2 + X^6$$

II Définition et théorème (borne BCH)

Définition 4.1.

Soit n un entier non nul, soit q une puissance d'un nombre premier.
On suppose n et q **premiers entre eux**.
Soit m l'ordre multiplicatif de q modulo n.
Soit α une racine primitive n-ième de l'unité dans $\mathbb{F}_{q^m}$. $(nq^m - 1)$
Soit b un entier et soit $\delta \in \mathbb{N}^*$.
Le code **BCH** de distance prescrite δ et associé à α est le code cyclique de longueur n et de polynôme générateur :

$$\begin{aligned} g(X) &= \text{ppcm}\left(M_{\alpha^b}(X), \cdots, M_{\alpha^{b+\delta-2}}(X)\right) \\ &= \text{ppcm}\left(M_{\alpha^i}(X), i \in \left\{\underbrace{b, b+1, \cdots, b+\delta-2}_{\delta-1 \text{ entiers}}\right\}\right) \end{aligned}$$

Si $b = 1$ on dit que le code est **BCH strict**
Si $n = q^m - 1$ on dit que le code est **BCH primitif**.

Théorème 4.1 (Borne BCH)**.**

La distance minimale d'un code BCH de distance prescrite δ est au moins δ

Démonstration.
Supposons que le code possède un mot $\mathcal{C}$ de poids $\leqslant \delta - 1$

$$c(X) = c_{i_1} X^{i_1} + c_{i_2} X^{i_2} + \cdots + c_{i_{\delta-1}} X^{i_{\delta-1}}$$

avec $\begin{cases} 0 \leqslant i_1 < i_2 \cdots < i_{\delta-1} \leqslant n-1 \\ c_{i_1}, \cdots, i_{i_{\delta-1}} \in \mathbb{F}_q \end{cases}$
On veut montrer que

$$\forall j \in \{1, \cdots, \delta - 1\}, c_{i_j} = 0$$

On a $g(X) | c(X)$
Donc $\forall i \in \{0, \cdots, \delta - 2\}$

$$M_{\alpha^{b+i}}(X) | c(X)$$

donc $\forall i \in \{0, \cdots, \delta-2\}$

$$c\left(\alpha^{b+i}\right) = 0$$

donc :

$$\begin{pmatrix} \alpha^{bi_1} & \cdots & \alpha^{bi_{s-1}} \\ \alpha^{(b+1)i_1} & \cdots & \alpha^{(b+1)i_{\delta-1}} \\ \vdots & & \vdots \\ \left(\alpha^{b+\delta-2}\right)^{i_1} & \cdots & \alpha^{(b+\delta-2)i_{\delta-1}} \end{pmatrix} \cdot \begin{pmatrix} c_{i_1} \\ c_{i_2} \\ \vdots \\ c_{i_{\delta-1}} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

On a $H_1 = \begin{pmatrix} 1 & \cdots & 1 \\ \alpha^{i_1} & \cdots & \alpha^{i_{\delta-1}} \\ \vdots & & \vdots \\ \alpha^{(\delta-2)i_1} & \cdots & \alpha^{(\delta-2)i_{\delta-1}} \end{pmatrix} \operatorname{diag}\left(\alpha^{bi_1}, \cdots, \alpha^{bi_{\delta-1}}\right)$

Notons pour $j \in \{1, \cdots, \delta-1\}$ $\rho_j = \alpha^{i_j}$

On a $H_1 = H_2 \cdot \operatorname{diag}\left(\rho_1^b, \cdots, \rho_{\delta-1}^b\right)$ où $H_2 = \begin{pmatrix} 1 & \cdots & 1 \\ \rho_1 & \cdots & \rho_{\delta-1} \\ \rho_1^2 & \cdots & \rho_{\delta-1}^2 \\ \vdots & & \vdots \\ \rho_1^{\delta-2} & \cdots & \rho_{\delta-1}^{\delta-2} \end{pmatrix}$

Or α est une racine **primitive $n$ième de l'unicité de** 1 et $0 \leqslant i_1 < i_2 \cdots < i_{\delta-1} < n$

Donc $\forall j \neq l \in \{1, \cdots, \delta-1\}$ $\rho_j \neq \rho_l$

Donc $\det(H_2) \neq 0$ (déterminant matrice de Vandermonde)

Donc $\det(H_1) \neq 0$

Donc $\begin{pmatrix} c_{i_1} \\ \vdots \\ c_{i_{\delta-1}} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ donc $c = 0$ □

Exemple 4.3.

1. *BCH strict de longueur* 15 *binaire et de distance prescrite* 3 *:*
   Soit $\alpha \in \mathbb{F}_{2^4}$ *tel que* $\alpha^4 + \alpha + 1 = 0$
   On a $X^4 + X + 1$ *irréductible et* α *d'ordre* 15.
   Soit $g(X) = ppcm(M_\alpha(X), M_{\alpha^2}(X)) = X^4 + X + 1$ *car* $M_{\alpha^2}(X) = M_\alpha(X)$
   g engendre un code BCH de longueur 15 *et de distance* $\geqslant 3$ *de dimension* 11 *(donc distance* $\leqslant 5$ *par Singleton)*
   $g(X)$ *est un mot de poids* 3 *donc :*

$$d = 3$$

2. *BCH strict de longueur* 15 *et de distance prescrite* 5.
Soit $\alpha \in \mathbb{F}_{2^4}$ *tel que* $\alpha^4 + \alpha + 1 = 0$, α *d'ordre* 15.
Soit $g(X) = ppcm(M_\alpha(X), M_{\alpha^2}(X), M_{\alpha^3}(X), M_{\alpha^4}(X))$
$g(X)$ *engendre un code BCH binaire de longueur* 15 *et de distance prescrite* 5 *donc distance* $\geqslant 5$.

$$C(1) = \{1, 2, 4, 6\}$$

donc

$$M_\alpha = M_{\alpha^2} = M_{\alpha^4}$$

et $M_{\alpha^3} = X^4 + X^3 + X^2 + X + 1$ *(cf exemple précédent et CC1)*
Donc

$$\begin{aligned} g(X) &= \left(X^4 + X + 1\right)\left(X^4 + X^3 + X^2 + X + 1\right) \\ &= X^8 + X^7 + X^6 + X^5 + X^4 + X^5 + X^4 \\ &+ X^3 + X^2 + X + X^4 + X^3 + X^2 + X + 1 \\ &= X^8 + X^7 + X^6 + X^4 + 1 \end{aligned}$$

Le code est donc $[15, 7, d]_2$ *avec* $d \geqslant 5$ *par BCH et* $d \leqslant 9$ *(Singleton)*
De lus g *est de poids* 5 *donc* $d = 5$

III Décodage des codes BCH

Soit $n \in \mathbb{N}^*$, soit $t \in \mathbb{N}$ et soit $\delta = 2t + 1$, soit q une puissance d'un nombre premier ($q \wedge n = 1$). Soit α ne racine primitive n-ième de 1 dans $\mathbb{F}_{q^m}$ ($m = \mathrm{ord}_q(n)$)
Le code BCH (strict) $\mathcal{C}$ de longueur n, de distance prescrite δ, associé à α est le code cyclique de polynôme générateur :

$$g(x) = \mathrm{ppcm}\left(\underbrace{M_\alpha}_{\in \mathbb{F}_q[X]}(x), \cdots, M_{\alpha^{2t}}(x)\right) \in \mathbb{F}_q[X]$$

$\mathcal{C} = \{m(x) \cdot g(x) \,|\, m(x) \in \mathbb{F}_q[X], \deg(m) < n - \deg(g)\}$
Soit $c \in \mathbb{F}_q^n$:

$$\begin{aligned} c \in \mathcal{C} &\Leftrightarrow g(x) \,|\, c(x) \\ &\Leftrightarrow \forall i \in \{1, \cdots, 2t\}, c\left(\alpha^i\right) = 0 \end{aligned}$$

Soit $c \in \mathcal{C}$:
$y(x) = c(x) + e(x)$ avec $w(e) = r \leqslant t$.

$e(x) = \sum_{j=1}^{r} Y_j x^{i_j}$, $Y_j \in \mathbb{F}_q, Y_i \neq 0$ où $0 \leqslant i_1 < \cdots < i_r \leqslant n-1$.
On a $\forall i \in \{1, \cdots, 2t\}$:

$$\begin{aligned} S_i &= \underbrace{c\left(\alpha^i\right)}_{=0} + e\left(\alpha^i\right) \\ &= \sum_{k=1}^{r} Y_r X_k^i \text{ où } X_k = \alpha^{i_k} \end{aligned}$$

On a donc les $2t$ équations suivantes :

$$\begin{cases} S_1 = Y_1 X_1 + \cdots + Y_r X_r \\ S_2 = Y_1 X_1^2 + \cdots + Y_r X_r^2 \\ \cdots \\ S_{2t} = Y_1 X_1^{2t} + \cdots + Y_r X_r^{2t} \end{cases}$$

But : déterminer $r, Y_1, \cdots, Y_r, X_1, \cdots, X_r$
Sont connus : $S_1, \cdots, S_{2t}$ les syndromes.
Elle sont linéaires en les Y_i mais polynomiales en les X_i.
On a $2t$ équations, et $2r \leqslant 2t$ inconnues.

Définition 4.2.

Le polynôme localisateur d'erreurs est :

$$\sigma(z) = \prod_{j=1}^{r} (1 - X_j z) \in \mathbb{F}_{q^n}[z]$$

But : déterminer $\sigma(z)$.
Notation : $\sigma(z) = 1 + s_1 z + \cdots s_r z^r$

1 Premier algorithme : via système linéaire

On veut déterminer $\sigma(z)$, et plus précisément les coefficients $s_1, \cdots, s_r$ de $\sigma(z)$ comme solutions d'un système linéaire.
On a $\forall j \in \{1, \cdots, r\}$, $\sigma\left(X_j^{-1}\right) = 0$
$\forall j \in \{1, \cdots, r\}$:

$$X_j^{r+1} + s_1 X_j^r + \cdots + s_r X^j = 0$$

On la réécrit :

$$\begin{cases} X_1^{r+1} + s_1 X_1^r + \cdots + s_r X_1 = 0 \ (\times Y_1) \\ X_2^{r+1} + s_1 X_2^r + \cdots + s_r X_2 = 0 \ (\times Y_2) \\ \cdots \\ X_r^{r+1} + s_1 X_r^r + \cdots + s_r X_r = 0 \ (\times Y_r) \end{cases}$$

En sommant :

$$S_{r+1} + S_1 S_r + \cdots s_r S_1 = 0$$

(On rappelle : $S_i = \sum_{j=1}^{r} Y_j X_j^i$)
On multiplie chaque ligne par $X_1, \cdots, X_r$:

$$\begin{cases} X_1^{r+1} + s_1 X_1^r + \cdots + s_r X_1 = 0 \ (\times Y_1 X_1) \\ X_2^{r+1} + s_1 X_2^r + \cdots + s_r X_2 = 0 \ (\times Y_2 X_2) \\ \cdots \\ X_r^{r+1} + s_1 X_r^r + \cdots + s_r X_r = 0 \ (\times Y_r X_r) \end{cases}$$

$S_{r+2} + s_2 S_{r+1} + \cdots + s_r S_2 = 0$
On re multiplie par $X_1, \cdots, X_r$:

$$\begin{cases} X_1^{r+1} + s_1 X_1^r + \cdots + s_r X_1 = 0 \ \left(\times Y_1 X_1^2\right) \\ X_2^{r+1} + s_1 X_2^r + \cdots + s_r X_2 = 0 \ \left(\times Y_2 X_2^2\right) \\ \cdots \\ X_r^{r+1} + s_1 X_r^r + \cdots + s_r X_r = 0 \ \left(\times Y_r X_r^2\right) \end{cases}$$

On obtient : $S_{r+3} + s_1 2 S_{r+1} + \cdots + s_r S_3 = 0$
On ré-itere pour avoir r équations : donc r fois, jusqu'à obtenir :

$$\begin{cases} S_{r+1} + s_1 S_r + \cdots + s_r S_1 = 0 \\ S_{r+2} + s_1 S_{r+1} + \cdots + s_r S_2 = 0 \\ S_{r+3} + s_1 S_{r+2} + \cdots + s_r S_3 = 0 \\ \cdots S_{2r} + s_1 S_{2r-1} + \cdots + s_r S_r = 0 \end{cases}$$

On obtient r équations linéaires, d'inconnues $s_1, \cdots, s_r$:

$$\begin{pmatrix} S_1 & S_2 & \cdots & S_r \\ S_2 & S_3 & \cdots & S_{r+1} \\ \vdots & & & \\ S_r & S_{r+1} & \cdots & S_{2r-1} \end{pmatrix} \begin{pmatrix} s_r \\ s_{r-1} \\ \vdots \\ s_1 \end{pmatrix} = \begin{pmatrix} -S_{r+1} \\ -S_{r+2} \\ \vdots \\ -S_{2r} \end{pmatrix}$$

$\forall i, j \in \{1, \cdots, r\}$:

$$\begin{aligned} \mathcal{S}_{ij} &= S_{i+j-1} \\ &= \sum_{k=1}^{r} Y_k X_k^{i+j-1} \\ &= \left(V \cdot D \cdot {}^t V\right)_{i,j} \end{aligned}$$

où $\begin{cases} V = \left(X_i^{j-1}\right)_{1 \leqslant i,j \leqslant r} \\ D = \operatorname{diag}\left(X_1 Y_1, \cdots, X_r Y_r\right) \end{cases}$ toutes deux inversibles

Algorithme 4.3.

Entrée : $g(x), \alpha, t, y(x)$

Sortie : $c(t), m(x)$

1. Pour $i = 1, \cdots, 2t$:
   $S_i \leftarrow y\left(\alpha^i\right)$
2. Si $\forall i \in \{1, \cdots, r\}\ S_i = 0$:
   $c \leftarrow y$
3. $r \leftarrow t$
   $$y \leftarrow \begin{pmatrix} S_1 & \cdots & S_r \\ \vdots & & \vdots \\ S_r & \cdots & S_{2r-1} \end{pmatrix}$$
4. Tant que g non inversible, faire :
   $r \leftarrow r - 1$
   $$g \leftarrow \begin{pmatrix} S_1 & \cdots & S_r \\ \vdots & & \\ S_r & \cdots & S_{2r-1} \end{pmatrix}$$
5. Déterminer $s_1, \cdots, s_r$ tels que :
   $$g \begin{pmatrix} s_r \\ \vdots \\ s_1 \end{pmatrix} = \begin{pmatrix} -S_{r+1} \\ \vdots \\ -S_{2r} \end{pmatrix}$$
6. $\sigma \leftarrow 1 + s_1 z + \cdots + s_r z^r$
7. Déterminer $X_1, \cdots, X_r$ tels que $\sigma\left(X_i^{-1}\right) = 0$
8. Déterminer $_1, \cdots, i_r$ tels que $X_j = \alpha^{i_j}$
9. Déterminer $Y_1, \cdots, Y_r$ solution de :
   $$\begin{cases} S_1 = X_1 Y_1 + \cdots + X_r Y_r \\ \vdots \\ S_{2t} = \cdots \end{cases}$$
10. $c \leftarrow y - \sum_{j=1}^{r} Y_j x^{i_j}$
11. Rentre c/g

Exemple 4.4 (Avec $n = 15$, $t = 2$, $\alpha^4 = \alpha + 1$)**.**
Faire au préalable la table de $\alpha^4 + \alpha + 1 = 0$
$g = ppcm\left(M_\alpha, M_{\alpha^2}, M_{\alpha^3}, M_{\alpha^4}\right) = ppcm\left(x^4 + x + 1, x^4 + x^2 + x + 1\right)$
Soit $y = c + e$ *avec* $c \in \mathcal{C}$*, et* $e(x) = x^2 + x^6$

$$\begin{aligned} S_1 &= \alpha^2 + \alpha^6 = \alpha^3 \\ S_2 &= \alpha^6 \\ S_3 &= \alpha^6 + \alpha^{13} = \alpha^2 \\ S_4 &= \alpha^{12} \end{aligned}$$

$$\mathcal{S} = \begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} = \begin{pmatrix} \alpha^3 & \alpha^6 \\ \alpha^6 & \alpha^2 \end{pmatrix}$$

$\det(y) = \alpha^5 + \alpha^{12} \neq 0$ *donc* $r = 2$.
On résout :

$$\begin{pmatrix} \alpha^3 & \alpha^6 \\ \alpha^6 & \alpha^2 \end{pmatrix} \begin{pmatrix} s_2 \\ s_1 \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha^{12} \end{pmatrix} \Leftrightarrow \begin{pmatrix} \alpha^3 & \alpha^6 \\ 0 & \alpha^{11} \end{pmatrix} \begin{pmatrix} s_2 \\ s_1 \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha^{14} \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} s_1 = \alpha^3 \\ s_2 = \dfrac{\alpha^2 + \alpha^9}{\alpha^3} = \alpha^8 \end{cases}$$

On obtient le polynôme localisateur :

$$\sigma(z) = 1 + \alpha^3 z + \alpha^8 z^2$$

$$\begin{aligned} \sigma\left(\alpha^0\right) &= 1 + \alpha^3 + \alpha^8 = \alpha^6 \neq 0 \\ \sigma\left(\alpha^1\right) &= 1 + \alpha^4 + \alpha^{10} \neq 0 \\ &\vdots \\ \sigma\left(\alpha^9\right) &= 1 + \alpha^{12} + \alpha^{11} = 0 \\ &\vdots \\ \sigma\left(\alpha^{13}\right) &= 1 + \alpha + \alpha^4 = 0 \end{aligned}$$

On a donc :

$$e(x) = x^{15-9} + x^{15-13} = x^6 + x^2$$

2 Deuxième algorithme : via Euclide étendu (partiel)

Définition 4.3.

— Le polynôme **syndrome** est définie par :

$$S(z) = \sum_{i=1}^{2t} S_i z^{i-1}$$

— Le polynôme **évaluateur d'erreurs** est :

$$w(z) = \sum_{i=1}^{r} X_i Y_i \prod_{j=1, j\neq i}^{r} (1 - X_j z)$$

Propriétés 4.1.

— $\forall l \in \{1, \cdots, r\}$

$$w\left(X_l^{-1}\right) = X_l Y_l \prod_{j=1, j\neq l}^{r} \left(1 - X_j X_l^{-1}\right)$$

— $\sigma \wedge w = 1$ (σ et w sont **premiers entre eux**).
— $\deg(w) < t$

But : déterminer $\sigma(z)$ et $w(z)$

Théorème 4.2 (Équation-clé)**.**

$$S(z)\,\sigma(z) \equiv w(z) \left[z^{2t}\right]$$

Démonstration.

$$\begin{aligned} S(z) &= \sum_{i=1}^{2t} S_i z^{i-1} \\ &= \sum_{i=1}^{2t} \left(\sum_{j=1}^{r} Y_j X_j^i \right) z^{i-1} \\ &= \sum_{j=1}^{r} X_j Y_j \sum_{i=1}^{2t} (X_j z)^{i-1} \\ &= \sum_{j=1}^{r} X_j Y_j \text{ par } (*) : \\ &\equiv \sum_{j=1}^{r} X_j Y_j \frac{1}{1 - X_j z} \left[z^{2t} \right] \end{aligned}$$

$$(*) \quad \left[\sum_{i=1}^{2t} (X_j z)^{i-1} \right] (1 - X_j z) \equiv 1 \left[z^{2t} \right]$$

$$\text{car } S(z) = \sum_{j=1}^{r} X_j Y_j \prod_{i=1, i \neq j}^{r} (1 - X_i z) / (\sigma(z)) \left[z^{2t} \right]$$

$$\text{donc } S(z)\sigma(z) = \underbrace{\sum_{j=1}^{r} X_j Y_j \prod_{i=1, i \neq j}^{r} (1 - X_i z)}_{w(z)} \left[z^{2t} \right]$$

□

On cherche à résoudre l'équation-clé :

$$S(z)\sigma(z) \equiv z(z) \left[z^{2t} \right]$$

d'inconnues $\sigma(z)$ et $w(z)$

Théorème 4.3.

$$\begin{aligned} r_0 = z2t, & r_1 = S(z) \\ u_0 = 1, & \qquad u_1 = 00 \\ v_0 = 0, & v_1 = 0 \end{aligned}$$

et pour $i \geqslant 1$: tant que $r_i \neq 0$:

$$\begin{aligned} r_{i+1} &= \text{reste}(r_{i-1}, r_i) \\ q_{i+1} &= \text{quotiet}(r_{i-1}, r_i) \\ u_{i+1} &= u_{i-1} - q_{i+1} u_i \\ v_{i+1} &= v_{i-1} - q_{i+1} v_i \end{aligned}$$

Soit $k \in \mathbb{N}$ tel que $\deg(r_k) < t$ et $\deg(r_{k-1}) \geqslant t$
Alors :

$$\sigma(z) = \frac{v_k(z)}{v_k(0)} \text{ et } w(z) = \frac{r_k(z)}{r_k(0)}$$

Démonstration.
On a : $\begin{cases} \forall i \in \{0, \cdots, k\} \\ r_i(z) = z^{2t} \times u_i(z) + S(z) \times v_i(z) \end{cases}$
En particulier :

$$(1)\ \ S(z) \cdot v_k(z) + z^{2t} \cdot u_k(z) = r_k(z)\ \ (\times \sigma(z))$$

Or :

$$S(z)\sigma(z) \equiv w(z)\ \left[z^{2t}\right]$$

donc, il existe $u(z)$ tels que :

$$(2)\ \ S(z) \cdot \sigma(z) + z^{2t} \cdot u(z) = w(z)\ \ (\times v_k(z))$$

On en déduit de (1) et (2) :

$$\underbrace{z^{2t}(\sigma(z) u_k(z) - v_k(z) u(z))}_{\deg \geqslant 2t \text{ ou } \sigma(z)u_k(z) - v_k(z)u(z) = 0} = \underbrace{r_k(z)}_{<t} \underbrace{\sigma(z)}_{\leqslant t} - \underbrace{v_k(z)}_{?} \underbrace{w(z)}_{<t}$$

Or $\deg(v_k(z)) = \deg(r_0(z)) - \deg(r_{k-1}(z)) = 2t - \underbrace{\deg(r_{k-1}(z))}_{\geqslant t} \leqslant t$

Donc :

$$\deg(r_k(z)\sigma(z) - v_k(z) w(z)) < 1t$$

Nécessairement, $\begin{cases} r_k(z)\,\sigma(z) - v_k(z)\,w(z) = 0 \ \ (3) \\ \sigma(z)\,u_k(Z) - v_k(z)\cdot u(z) = 0 \ \ (4) \end{cases}$ D'après (3), $\sigma(z)\,|v_k(z)\,w(z)$.
Or $\sigma(z) \wedge w(z) = 1$.
Donc d'après le lemme de Gauss :

$$\sigma(z)\,|v_k(z)$$

D'après (4) :

$$v_k(z)\,|\sigma(z)\,u_k(z)$$

Or $u_k(z) \wedge v_k(z) = 1$ donc $v_k(z)\,|\sigma(z)$
Donc $\sigma(z)$ et $v_k(z)$ sont doc égaux, à une constante multiplicative près. De plus $\sigma(0) = 1$ donc :

$$\sigma(z) = \frac{v_k(z)}{v_k(0)}$$

D'après (3) : $r_k(z)/v_k(0) = w(z)$ □

Algorithme 4.4.

Entrée : g, α, t, y

Sortie : m

1. $S \leftarrow \sum_{i=1}^{r} \underbrace{y\left(\alpha^i\right)}_{S_i} z^{i-1}$
2. Si $S = 0$ alors $c \leftarrow y$
3. $r_0 \leftarrow z^{2t}, v_0 \leftarrow 0$
   $r_1 \leftarrow S, v_1 \leftarrow 1$
   Tant que $\deg(r_1) \geqslant t$ faire :
   $q \leftarrow$ quotient (r_0, r_1)
   $r_0, r_1 \leftarrow r_1, r_0 - q \cdot r_1$
   $v_0, v_1 \leftarrow v_1, v_0 - q v_1$
4. $\sigma(z) \leftarrow \dfrac{v_1(z)}{v_1(0)}$
   $w(z) \leftarrow \dfrac{r_1(z)}{v_1(0)}$
5. $r \leftarrow \deg(\sigma)$
6. Déterminer $X_1, \cdots, X_r$ tels que $\sigma\left(X_j^{-1}\right) = 0$
7. Déterminer $i_1, \cdots, i_r$ tels que $X_j = \alpha^{i_j}$
8. Pour $l = 1, \cdots, r$ faire $Y_l \leftarrow \dfrac{w\left(X_l^{-1}\right)}{X_l \prod_{j=1, j\neq l}^{r}\left(1 - X_l^{-1} X_j\right)}$
9. $c \leftarrow y - \sum_{j=1}^{r} Y_j x^{i_j}$
10. rendre c/g

Les étapes 4, 8, 9 sont inutiles avec $q = 2$.

Exemple 4.5 (Pour $q = 2$, $n = 15$ $t = 2$, $\alpha^4 = \alpha + 1$)**.** *soit* $y = c + e$ *avec* $c \in \mathcal{C}$ $e = x^2 + x^6$
$S(z) = S_1 + S_2 z + S_3 z^2 + S_4 z^3$ *avec* $S_1 = \alpha^3, S_2 = \alpha^6, S_3 = \alpha^2, S_4 = \alpha^{12}$
On applique l'algorithme d'Euclide étendu partiel à z^4 *et* $S = \alpha^{12} z^3 + \alpha^2 z^2 + \alpha^6 z + \alpha^3$

Initialisation :

$$z^4 = z^4 \times 1 + S \times 0$$
$$S = z^4 \times 0 + S \times 1$$

On divise z^4 *par* $\alpha^{12}z^3 + \alpha^2 z^2 + \alpha^3$, *on obtient :*

$$z^4 = \left(\alpha^3 z + \alpha^8\right) \cdot \left(\alpha^{12}z^3 + \alpha^2 z^2 + \alpha^3\right) + \alpha^{13}z^2 + \alpha^8 z + \alpha^{11}$$

$$z^4 = z^4 \times 1 + S \times 0$$
$$S = z^4 \times 0 + S \times 1$$
$$\alpha^{13}z^2 + \alpha^8 z + \alpha^{11} = z^4 \times 1 + S \times \left(\alpha^3 z + \alpha^8\right)$$

On a :

$$\alpha^3 z + \alpha^8 = \left(\alpha^{13}z^2 + \alpha^8 z + \alpha^{11}\right)\left(\alpha^{14}z + \alpha^{14}\right) + \alpha^{12}$$

On s'arrête car $\deg < 2$

$$z^4 = z^4 \times 1 + S \times 0$$
$$S = z^4 \times 0 + S \times 1$$
$$\alpha^{13}z^2 + \alpha^8 z + \alpha^{11} = z^4 \times 1 + S \times \left(\alpha^3 z + \alpha^8\right)$$
$$\alpha^{12} = z^4 \times ? + S \times \left(1 + \left(\alpha^{14}z + \alpha^{14}\right)\left(\alpha^3 z + \alpha^8\right)\right)$$

On obtient, à un coefficient multiplicatif près $\sigma(z)$ *:*
$\alpha^2 z^2 + \left(\alpha^2 + \alpha^7\right) z + \alpha^7 + 1 = \alpha^2 z^2 + \alpha^{12} z + \alpha^9$
$\sigma(z) = 1 + \alpha^3 z + \alpha^8 z^2$

Comme précédemment, on a :

$$\sigma\left(\alpha^{13}\right) = \sigma\left(\alpha^9\right) = 0$$

D'où $e(x) = x^2 + x^6$

Chapitre 5

Codes de Goppa

I Rappels

Soit $\mathcal{C}$ un code BCH strict binaire de longueur n, de distance prescrite δ et associé à α racines primitives n-ièmes de 1 dans $\mathbb{F}_{2^m}$.

$$\begin{aligned}\mathcal{C} &= \{c \in \mathbb{F}_2^n |\, g(x) \,|c(x)\} \text{ où } f(x) = \text{ppcm}\left(M_\alpha, \cdots, M_{\alpha^{s-1}}\right\} \\ &= \left\{ c \in \mathbb{F}_2^n |\, \underset{\alpha \in \mathbb{F}_{2^m}}{\underset{\uparrow}{c(\alpha)}} = \cdots = c\left(\alpha^{s-1}\right) = 0 \right\} \\ &= \left\{c \in \mathbb{F}_2^m |\, H \cdot {}^t c = 0\right\}\end{aligned}$$

où $H = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \left(\alpha^2\right)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{\delta-1} & \cdots & \left(\alpha^{\delta-1}\right)^{n-1} \end{pmatrix} \in \mathcal{M}_{d-1,n}\left(\mathbb{F}_{2^m}\right)$

$\mathcal{C}$ est dans $\mathbb{F}_2^n$.
$\mathcal{C} = \mathcal{C}' \cap \mathbb{F}_2^n$ où $\mathcal{C}'$ est le code de Reed-Solomon défini sur $\mathcal{F}_{2^m}$ de localisateurs $1, \alpha, \cdots, \alpha^{n-1}$ et de multiplicateur $1, \alpha, \cdots, \alpha^{n-1}$, de longueur n et de dimension $n - (\delta - 1) = k$, de distance $\delta = n - k + 1$.

Généralisation

$\mathcal{C}_{\text{BCH}}$ définie sur $\mathbb{F}_q$ de longueur n, valant $\mathcal{C}_{\text{RS}} \cap \mathbb{F}_q^n$ se généralise en les codes de **Goppa** :
Ce sont $\mathcal{C}_{\text{Goppa}}$ sur $\mathbb{F}_q$ vaudront $\mathcal{C}_{\text{GRS}} \cap \mathbb{F}_q^n$.
que valent leur localisateurs ? Leur multiplicateurs ?

II Définition

Soit $\mathcal{C}$ un code BCH strict sur $\mathbb{F}_q$ de longueur n, de distance prescrite $2t+1$, associé à α racine primitive n-ième de 1 dans $\mathbb{F}_{q^m}$.
Soit $c \in \mathbb{F}_q^n$.

$$\begin{aligned}
c \in \mathcal{C} &\Leftrightarrow \forall i \in [\![1, 2t]\!], c\left(\alpha^i\right) = 0 \\
&\Leftrightarrow \underbrace{\sum_{i=0}^{2t-1} c\left(\alpha^{i+1}\right) z^i}_{\in \mathbb{F}_{q^m}[z]} = 0 \\
&\Leftrightarrow \sum_{i=0}^{n-1} c\left(\alpha^{i+1}\right) z^i \equiv 0 \left[z^{2t}\right] \\
&\Leftrightarrow \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} c_j \left(\alpha^{i+1}\right)^j z^i \equiv 0 \left[z^{2t}\right] \\
&\Leftrightarrow \sum_{j=0}^{n-1} c_j \underbrace{\left(\sum_{j=0}^{n-1} \left(\alpha^{i+1}\right)^j z^i \right)}_{(*)} \equiv 0 \left[z^{2t}\right]
\end{aligned}$$

$(*)$:

$$\begin{aligned}
\left(\sum_{j=0}^{n-1} \left(\alpha^{i+1}\right)^j z^i \right) &= \sum_{i=0}^{n-1} \left(\alpha^{-j}\right)^{(-i-1)} z^i \\
&= \sum_{i=0}^{n-1} \left(\alpha^{-j}\right)^{n-1-i} z6i \\
&= \frac{z^n - \left(\alpha^{-j}\right)^n}{z - \alpha^{-j}} = \frac{z^n - 1}{z - \alpha^{-j}}
\end{aligned}$$

$$c \in \mathcal{C} \Leftrightarrow \sum_{i=0}^{n-1} c_i \frac{z^n - 1}{z - \alpha^{-j}} \equiv 0 \left[z^{2t}\right]$$

Notons $\dfrac{1}{z - \alpha^{-j}}$ l'inverse de $z - \alpha^{-j}$ modulo z^{2t}.

On a :

$$c \in \mathcal{C} \Leftrightarrow (z^n - 1) \sum_{i=0}^{n-1} c_i \frac{1}{z - \alpha^i} \equiv 0 \left[z^{2t}\right]$$
$$\Leftrightarrow \sum_{i=0}^{n-1} c_i \frac{1}{z - \alpha^{-i}} \equiv 0 \left[z^{2t}\right]$$

Mise en garde!!! : dans cette définition $g(z)$ n'a rien à voir avec un polynôme générateurs, c'est juste une notation

Définition 5.1.

Soit $g(z)$ un polynôme unitaire de degré r dans $\mathbb{F}_{q^m}[z]$.
Soient $\gamma_0, \cdots, \gamma_{n-1} \in \mathbb{F}_{q^m}$ distincts 2 à 2.
Soit $L = \{\gamma_0, \cdots, \gamma_{n-1}\}$, $|L| = n$.
On suppose que $\forall i \in [\![0, n-1]\!]$, $g(\gamma_i) \neq 0$.
Le code de goppa $\Gamma(L, g)$ sur $\mathbb{F}_q$ est définie par :

$$\Gamma(L, g) = \left\{ c \in \mathbb{F}_q^n \text{ tel que } \sum_{i=0}^{n-1} c_i \frac{1}{z - \gamma_i} \equiv [g(z)] \right\}$$

où $\frac{1}{z - \gamma_i}$ est l'inverse de $z - \gamma_i$ modulo $g(z)$

Remarque 5.1. *$\Gamma(L, g)$ est linéaire*

Exemple 5.1.
$g(z) = z^{2t}$
β est une racine primitive n-ième de 1 dans $\mathbb{F}_{q^m}$.
$L = \{\beta^{-0}, \beta^{-1}, \cdots, \beta^{-(n-1)}\}$
$\Gamma(L, g)$ est le code BCH strict associé à β de distance prescrite $2t + 1$.

III Propriétés

Déterminons une matrice de contrôle (à coefficients dans $\mathbb{F}_{q^m}$) de $\Gamma(L, g)$.
Soit $c \in \mathbb{F}_q^m$.

$$c \in \Gamma(L, g) \Leftrightarrow \sum_{j=0}^{n-1} c_j \frac{1}{z - \gamma_j} \equiv 0 \left[g(z)\right]$$

$\forall j \in [\![0, n-1]\!]$, $g(z) = (z-\gamma_j)\dfrac{g(z)-g(\gamma_j)}{z-\gamma_j} + g(\gamma_j)$ or $g(\gamma_j) \neq 0$.

Donc $(z-\gamma_j)\underbrace{\dfrac{g(z)-g(\gamma_j)}{z-\gamma_j}\left(\dfrac{-1}{g(\gamma_j)}\right)}_{\text{inverse de } (z-\gamma_j) \mod g(z)} \equiv 1\,[g(z)]$

$$c \in \Gamma(L,g) \Leftrightarrow \sum_{j=0}^{n-1} c_j \frac{g(z)-g(\gamma_j)}{z-\gamma_j}\left(\frac{-1}{f(\gamma_j)}\right) \equiv 0\ [g(z)]$$

Notons : $\begin{cases} h_j = \dfrac{1}{g(\gamma_j)} \\ g(z) = \displaystyle\sum_{k=0}^{r} g_k z^k \end{cases}$

On a :

$$\begin{aligned} \frac{g(z)-g(\gamma_j)}{z-\gamma_j} &= \sum_{k=0}^{r} g_k \frac{z^k-\gamma_j^k}{z-\gamma_j} \\ &= \sum_{k=0}^{r} g_k \sum_{i=0}^{k-1} (\gamma_j)^{k-1-i} z^i \end{aligned}$$

Donc

$$c \in \Gamma(L,g) \Leftrightarrow \sum_{j=0}^{n-1} c_j \left(\sum_{k=0}^{r} g_k \sum_{i=0}^{k-1} (\gamma_j)^{k-1-i} z^i\right) h_j \equiv 0\ [g(z)]$$

Le polynôme du membre de gauche de la congruence a un degré $< r = \deg(g)$ donc la convergence est une égalité.

$$
\begin{aligned}
c \in \Gamma(L,g) &\Leftrightarrow \sum_{j=0}^{n-1} c_j h_j \sum_{k=0}^{r} g_k \sum_{i=0}^{k-1} \gamma_j^{k-1-i} z^i = 0 \\
&\Leftrightarrow \sum_{i=0}^{r-1} \left(\sum_{j=0}^{n-1} c_j h_j \sum_{k=i+1}^{r} g_k \gamma_j^{k-1-i} \right) z^i = 0 \\
&\Leftrightarrow \forall i \in [\![0, r-1]\!], \sum_{j=0}^{n-1} c_j h_j \left(\sum_{k=i+1}^{r} g_k \gamma_j^{k-1-i} \right) = 0 \\
&\left(c = (c_0, \cdots, c_{n-1}) \Leftrightarrow c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}\right) \\
&\Leftrightarrow \begin{matrix} i = r-1 \\ i = r-2 \\ \vdots \\ i = 0 \end{matrix} \begin{pmatrix} g_r & \cdots & g_r \\ g_r\gamma_0 + g_{r-1} & & g_r\gamma_{n-1} + g_{r-1} \\ \vdots & & \vdots \\ g_r\gamma_0^{r-1} + g_{r-1}\gamma_0^{r-2} + \cdots g_1 & & g_r\gamma_{n-1}^{r-1} + \cdots + g_1 \end{pmatrix} \cdot \begin{pmatrix} h_0 c_0 \\ \vdots \\ h_{n-1} c_{n-1} \end{pmatrix} = 0 \\
&\Leftrightarrow \underbrace{\begin{pmatrix} g_r & 0 & \cdots & \cdots & 0 \\ g_{r-1} & g_r & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ g_1 & \cdots & \cdots & g_{r-1} & g_r \end{pmatrix}}_{\text{matrice inversible car } g_r \neq 0} \underbrace{\begin{pmatrix} 1 & \cdots & 1 \\ \gamma_0 & \cdots & \gamma_{n-1} \\ \vdots & & \vdots \\ \gamma_0^{r-1} & \cdots & \gamma_{n-1}^{r-1} \end{pmatrix}}_{V \text{ matrice de Vandermone}} \underbrace{\begin{pmatrix} h_0 & & 0 \\ & \ddots & \\ 0 & & h_{n-1} \end{pmatrix}}_{D} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0 \\
&\Leftrightarrow V \cdot D \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0
\end{aligned}
$$

$\Gamma(L,g) = G_{\text{GRS}} \cap \mathbb{F}_q^n$

Théorème 5.1.

Le code de Goppa $\Gamma(L,g)$ a pour dimension $k \geqslant n - r \cdot m$ et pour distance $d \geqslant r + 1$.

Démonstration.

1. La distance $\geqslant r+1$?
   supposons que $\Gamma(L,g)$ possède un mot c non nul de poids $\leqslant r$.

Or $D \cdot c$ a le même poids que c (car D est diagonale inversible) donc V possède un sous-déterminant d' ordre r égal à 0.
Or toute sous-matrice de V d'ordre r est inversible car V est la matrice de Vandermonde r *timesn*.
C'est absurde.

2. Dimension ?
$$H = V \cdot D \in \mathcal{M}_{r,n}\left(\mathbb{F}_{q^m}\right)$$
On déduit de H une matrice $\tilde{H} \in \mathcal{M}_{r\times m,n}\left(\mathbb{F}_q\right)$ telle que $\Gamma(L,g) = \left\{c \in \mathbb{F}_q^n \text{ tq } \tilde{H} \cdot {}^t c = 0\right\}$.
$\tilde{H}$ possède $r \times m$ lignes et est à coefficient dans $\mathbb{F}_q$.
Son rang est $\leqslant r \times m$ et la dimension de $\Gamma(L,g)$ est $\dim\left(\mathrm{Ker}\left(\tilde{H}\right)\right) = n - \mathrm{Rg}\left(\tilde{H}\right) \geqslant n - r \times m$

□

Exemple 5.2 (Pour $q = 2, m-3$)**.**
$L = \left\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 = 1, 0\right\}$ *où* $\alpha \in \mathbb{F}_{2^3}$ $\alpha^3 = \alpha + 1$, $r = \deg(g) = 2$
$$g(z) = 1 + \alpha z + z^2$$
Les éléments de L *sont distincts* 2 *à* 2 *car* α *est d'ordre* 7.
On a $|L| = 8$.
$$\begin{aligned} g(\alpha) &= 1 \neq 0 \\ g\left(\alpha^2\right) &= \alpha^2 \neq 0 \\ g\left(\alpha^3\right) &= \alpha \neq 0 \\ g\left(\alpha^4\right) &= \alpha^2 \neq 0 \\ g\left(\alpha^5\right) &= \alpha^5 \neq 0 \\ g\left(\alpha^6\right) &= \alpha^6 \neq 0 \\ g\left(\alpha^7\right) &= \alpha \neq 0 \\ g(0) &= 1 \neq 0 \end{aligned}$$

donc $\Gamma(L,g)$ *est bien défini.*
De plus :
$$\Gamma(L,g) = \left\{c \in \mathbb{F}_2^8 \text{ tel que } H \cdot {}^t c = 0\right\}$$
Avec $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & 0 \end{pmatrix} diag\left(1, \alpha^5, \alpha^6, \alpha^5, \alpha^2, \alpha^2, \alpha^6, 1\right)$
Donc :
$$H = \begin{pmatrix} 1 & \alpha^5 & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^2 & \alpha^6 & 1 \\ \alpha & 1 & \alpha^2 & \alpha^2 & 1 & \alpha & \alpha^6 & 0 \end{pmatrix} \in \mathcal{M}_{2,8}\left(\mathbb{F}_8\right)$$

avec $\left(1, \alpha, \alpha^2\right)$ *base de* $\mathbb{F}_8$ *sur* $\mathbb{F}_2$.
On déduit de H *une matrice de contrôle* $\tilde{H}$ *:*

$$\begin{array}{c} 1 \\ \alpha \\ \alpha^2 \\ 1 \\ \alpha \\ \alpha^2 \end{array} \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Déterminons le rang de $\tilde{H}$ *: (on fait un pivot de Gauss pour mettre cette matrice sous forme échelonnée)*
On trouve $Rg\left(\tilde{H}\right) = 6$,

$$\Gamma\left(L, g\right) = \left\{c \in \mathbb{F}_2^8 \text{ tel que } \tilde{H} \cdot {}^t c = 0\right\} = \operatorname{Ker} \tilde{H}$$

Donc $\dim \Gamma\left(L, g\right) = 8 - 6 = 1$.
La distance minimale est $\geqslant 3$ *(car* $\deg\left(g\right) = 2$*) et* $\leqslant 8-2+1-7$ *par la borne de Singleton.*

On peut améliorer la borne sur la distance minimale dans un cas particulier sur $\mathbb{F}_2$:

Théorème 5.2.

Supposons $q = 2$ et que $g\left(z\right)$ n'a pas de racine multiple.
Alors la distance minimale de $\Gamma\left(L, g\right)$ est supérieur ou égale à $2r + 1$.

Démonstration.
On va montrer que $\Gamma\left(L, g\right) = \Gamma\left(L, g^2\right)$

— On a $\Gamma\left(L, g^2\right) \subset \Gamma\left(L, g\right)$ car $\forall c \in \mathbb{F}_2^n$:

$$\sum_{i=0}^{n-1} c_i \frac{1}{z - \gamma_i} \equiv 0 \left[g\left(z\right)^2\right] \Rightarrow \sum_{i=0}^{n-1} c_i \frac{1}{z - \gamma_i} \equiv 0 \left[g\left(z\right)\right]$$

En effet, $g | g^2$.

— Soit $c \in \Gamma\left(L, g\right)$, $\displaystyle\sum_{i=0}^{n-1} c_i \frac{1}{z - \gamma_i} \equiv 0 \left[g\left(z\right)\right]$

Considérons le polynôme $f\left(z\right) = \displaystyle\prod_{i=0}^{n-1} \left(z - \gamma_i\right)^{d_i} \in \mathbb{F}_{2^m}\left[z\right]$ où $d_i =$

$\begin{cases} 0 & \text{si } c_i = 0 \\ 1 & \text{si } c_i = 1 \end{cases}$ à noter que $d_i = 0, 1 \in \mathbb{N}$ et $c_i = 0, 1 \in \mathbb{F}_2$!

$$\frac{f'(z)}{f(z)} = \sum_{i=0}^{n-1} \frac{c_i}{z - \gamma_i}$$

Donc $\dfrac{f'(z)}{f(z)} \equiv 0 \ [g(z)]$ donc $f'(z) \equiv 0 \, [g(z)]$

Notons $f(z) = \sum_{i=0}^{s} f_i z^i$

$$\begin{aligned} f'(z) &= \sum_{i=0}^{s} f_i i z^{i-1} = \sum_{i=0, i \text{impair}} f_i z^{i-1} \\ &= \sum_{j, 2j+1 \leqslant s} f_{2j+1} z^{2j} \end{aligned}$$

De plus $f_{2j+1} \in \mathbb{F}_{2^m}$ donc $f_{2j+1} = f_{2j+1}^{2^m}$
Donc $f'(z) = \sum_j f_{2j+1}^{2^m} z^{2j}$.

$$f'(z) = \sum_j \left(f_{2j+1}^{2^{m-1}} z^j \right)^2 = \left(\sum_j f_{2j+1}^{2^{m-1}} z^j \right)^2$$

$f'(z)$ est le carré d'un polynôme de $g(z) \,|\, f'(z)$, $g(z)$ est donc sans facteur carré.
donc $g(z)^2$ divise $f'(z)$ donc $\dfrac{f'(z)}{f(z)} \equiv 0 \left[g(z)^2 \right]$ donc $c \in \Gamma\left(L, g^2\right)$.

Conclusion : $\Gamma(L, g) = \Gamma\left(L, g^2\right)$.
D'après le théorème précédemment, la distance minimale de $\Gamma\left(L, g^2\right)$ est $\geqslant 2r + 1 = \deg\left(g^2\right) + 1$ donc la distance de $\Gamma(L, g)$ est $\geqslant 2r + 1$. □

IV Décodage

Théorème 5.3.

$$Z(z)\,\sigma(z) \equiv w(z)\ [g(z(]$$

où :

$$\begin{cases} S(z) = \sum_i \dfrac{y_i}{z-\gamma_i}\ [g(z)] & y = c + e, c \in \Gamma(L,g), w(e) = \lfloor \dfrac{r}{2} \rfloor \\ \sigma(z) = \prod_{r \in M} (z-\gamma_i) & \text{où } M = \{i \text{ tel que } e_i \neq 0\}, \deg(\sigma) \leqslant t \\ w(z) = \sum_{i \in M} e_i \prod_{j \in M, j \neq i} (z-\gamma_j) & \deg(w) < t \end{cases}$$

Chapitre 6

Cryptosystème de Mac Eliece

1978 : Mc Eliece propose un cryptosystème basé sur la théorie des codes correcteurs.

Même époque : Rivest Shamer Adleman : RSA, cryptosystème basé sur la théorie des nombres.

1994 : Shor : ordinateur "hypothétique" quantite : Casser RSA : relancer l'intêret pour les cryptosystèmes basée :
Cryptographie post-quantique : sur le théorie des codes correcteurs, sur les réseaux, sur les systèmes polynomiaux.

Qu'est ce qu'un cryptosystème ?
Alice veut envoyer un message m à Bob mais Charles écoute sur la ligne. Elle va utiliser un cryptosystème pour transmettre à Bob.

Définition 6.1.

Un **cryptosystème** est un 5-uplet (M, C, K, E, D) avec :

1. M est un ensemble appelé ensemble des messages en clair.
2. C est un ensemble appelé ensembles des messages chiffrés.
3. K est un ensemble appelé espaces des clés.
4. $E = \{E_k | k \in K\}$ est une famille de fonctions M dans C appelées fonctions de chiffrements.
5. $D = \{D_k | k \in K\}$ est une famille de fonctions de C dans M, appelées fonctions de déchiffrements.

À chaque clé e de K, on associe une clé d de K telle que pour tout m de M, $D_b(E_e(m)) = m$
Alice calcule le cryptogramme $c = E_e(m)$ en utilisant la clé de chiffrement e de Bob. Elle envoie c à Bob, celui-ci calcule $D_b(c)$ avec sa clé de déchiffrement d.
La clé de déchiffrement est secrète.

On va construire un cryptosystème à clés publiques en 4 phases :

1. Génération des clés
2. Chiffrement
3. Déchiffrement
4. Sécurité.

1. **Génération des clés** :
   On va considérer un code linéaire $\mathcal{C}\ [n, k, d]_q$ pour lequel on connaît un algorithme de décodage jusqu'à t erreurs en temps polynomial

   Exemple 6.1.
   C de binaire de Goppa, $\Gamma(\mathbb{F}_{2^m}, g)$ où $g(z)$ est un polynôme irréductible dans $\mathbb{F}_{2^m}[z]$ de degré t.

   Soit G une matrice génératrice de $\mathcal{C}$, $G \in \mathcal{M}_{k,n}(\mathbb{F}_q)$.
   Soit S une matrice inversible aléatoire de $\mathcal{M}_{k,k}(\mathbb{F}_q)$.
   Soit P une matrice de permutation aléatoire de $\mathcal{M}_{n,n}(\mathbb{F}_q)$
   Soit $G' = S \times G \times P$

   Remarque 6.1.
   Le code engendré par G' a pour distance minimal d

Clé publique : G' (et t) (de Bob)
Clé privée : $S, G, P.$ (de Bob)
Taille clé publique : $k \times n$

2. **Chiffrement** :
Alice veut envoyer $m \in \mathbb{F}_q^k$: Elle calcule $c = m \cdot G' + e$ où $e \in \mathbb{F}_q^n$ où e aléatoire et $w(e) \leqslant t$
Elle envoie c à Bob
Complexité du chiffrement : $k \times n$.

3. **Déchiffrement** :
Bob reçoit c.
Il calcule :

$$\begin{aligned} y &= c \cdot P^{-1} \\ &= mG'P^{-1} + \underbrace{eP^{-1}}_{\text{poids } \leqslant t} \\ &= \underbrace{(mSG)}_{\text{mot du code } \mathcal{C}} + \underbrace{e \cdot P^{-1}}_{\text{erreur de poids } \leqslant t} \end{aligned}$$

car $G' = SGP$
Bob utilise l'algorithme de décodage associé à $\mathcal{C}$ pour retrouver $(mS)G$ pour $x = mS$ il en déduit $m = x \cdot S^{-1}$.
Complexité du déchiffrement : $\mathcal{O}\left(n^2\right)$ avec algorithme de décodage en temps quadratique.

4. **Sécurité**
La sécurité du cryptosystème est basé sur le problème du décodage par syndrome :
Soit H une matrice $(n-k) \times n$ de rang n sur $\mathbb{F}_q$, soit S dans $\mathbb{F}_q^{n-k}$, déterminer e tel que $H \cdot {}^t e = S$ avec $w(e) \leqslant t$.

Exemple 6.2 $(q = 2, n = 1024, t = 50)$**.**

$$\mathcal{C}_{1024}^{50} \sim 3 \times 10^{85} \textit{ possibilité}$$

Attaques :
— Stern
— Contour et Zijlstra : Projet tutoré (à venir) (ISD) : Information Set Decoding.

I Exemples

Bob construit le code de Goppa binaire $\mathcal{C} = \Gamma(L, g)$ où $g(z) = z$ et L le corps fini privé de 0 : $\mathbb{F}_{2^3} \setminus \{0\} = \left\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\right\}$ où $\alpha^3 + \alpha + 1 = 0$

$\mathcal{C}$ est bien définie car g ne s'annule pas sur L.
De plus g est sans facteur carré de degré 1 donc la distance minimale de $\mathcal{C}$ est $\geqslant 2 \times 1 + 1 = 3$

$$\mathcal{C} = \left\{ c \in \mathbb{F}_2^7, \tilde{H} \cdot^t c = 0 \right\}$$

où $\tilde{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha^6 & & & & & & \\ & \alpha^5 & & & & 0 & \\ & & \alpha^4 & & & & \\ & & & \alpha^3 & & & \\ & & & & \alpha^2 & & \\ & & & & & \alpha^1 & \\ & & 0 & & & & 1 \end{pmatrix} = \begin{pmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \end{pmatrix}$

On en déduit $\mathcal{C} = \left\{ c \in \mathbb{F}_2^7, H \cdot^t c = 0 \right\}$ avec :

$$H = \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right) \begin{matrix} \alpha^2 \\ \alpha \\ 1 \end{matrix}$$

Une matrice génératrice de $\mathcal{C}$ est donc :

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

Bob construit $S = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ privé, d'inverse $S^{-1} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

$$P = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \text{ privé}$$

S et P sont pris **au hasard**, avec les conditions S inversible et P matrice de permutation.

Il calcule $G' = S \times G \times P = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$: public $(t = 1)$

Alice veut envoyer $m = (1, 0, 1, 1)$ à Bob.
Elle calcule le cryptogramme $c = mG' + e$ où :

$$\begin{aligned} e &= (0, 1, 0, 0, 0, 0, 0) \\ &= (0, 1, 0, 0, 1, 0, 1) + (0, 1, 0, 0, 0, 0, 0, 0) \\ &= (0, 0, 0, 0, 1, 0, 1) \end{aligned}$$

Elle envoie le cryptogramme c à Bob, qui calcule :

$$y = c \cdot P^{-1} = (0, 0, 1, 0, 1, 0, 0)$$

qui est un mot de $\mathcal{C}$ perturbé en 0 ou 1 position.
Déterminons le mot de $\mathcal{C}$ le plus proche de y :
Soit

$$\begin{aligned} S(z) &= \sum_i \frac{y_i}{z - L_i} \mod z^2 \\ &= \frac{1}{z - \alpha^3} + \frac{1}{z - \alpha^2} \mod z^2 \\ &= \frac{z^2 - \alpha^6}{z - \alpha^3}\left(\frac{-1}{\alpha^6}\right) + \left(\frac{z^2 - \alpha^{10}}{z - \alpha^5}\right)\left(\frac{-1}{\alpha^{10}}\right) \mod z^2 \\ &= \left(z + \alpha^3\right) \cdot \alpha + \left(z + \alpha^5\right) \alpha^4 \\ &= \alpha + \alpha^2 z \end{aligned}$$

Pour rappel l'équation clé est :

$$S(z)\,\sigma(z) \equiv w(z) \mod \left(z^{2t}\right)$$

où $\sigma(z) = \prod_{i \in I} \left(z - \alpha^i\right)$
Appliquons l'algorithme d'Euclide étendu à z^2 et $\alpha^2 z + \alpha$:

$$\begin{aligned} \mathbf{z^2} &= z^2 \cdot 1 + \left(\alpha^{\mathbf{2}}\mathbf{z} + \alpha\right) \cdot 0 \\ \alpha^{\mathbf{2}}\mathbf{z} + \alpha &= z^2 \cdot 0 + \left(\alpha^2 z + \alpha\right) \cdot 1 \\ \alpha^{\mathbf{5}} &= z^2 \cdot 1 + \left(\alpha^2 z + \alpha\right) \cdot \underbrace{\left(\alpha^{\mathbf{5}}\mathbf{z} + \alpha^{\mathbf{4}}\right)}_{\alpha^5(z+\alpha^6)} \end{aligned}$$

Polynôme localisateur d'erreur : $\left(z + \alpha^6\right)$
Le mot de code associé à y est donc :

$$y + (0, 0, 0, 0, 0, 1, 0) = (0, 0, 1, 0, 1, 1, 0)$$

On a donc :

$$\begin{aligned} mSG &= (0,0,1,0,1,1,0) \\ mS &= (0,0,1,0) \\ m &= (0,0,1,0)\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = (1,0,1,1) \end{aligned}$$

Attaque :
Si on dispose de $c = (0,0,0,0,1,0,1) = (mG' + e)$ avec $w(e) \leqslant 1$ et

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

Question : Comment trouver m à l'aide de ces seules informations ?

$$\begin{aligned} G' &\sim \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \end{aligned}$$

En fait on trouve $H' = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$ et on trouve $H' \cdot {}^t c = \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix}$
Donc $e = (0,1,0,0,0,0,0)$ Une fois qu'on a H', on calcule : $H' \times^t c = \underbrace{H' \times^t (mG')}_{0} + \underbrace{H' \times^t e}_{0 \text{ où } e=0, \text{ ou colonne de } H'}$

On a donc l'équation :

$$
\begin{aligned}
mG' &= (0,1,0,0,1,0,1) \\
&\Leftrightarrow \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \\
&\Leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ * & * & * & * \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ \vdots \end{pmatrix} \\
&\Leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}
\end{aligned}
$$