Théorie des codes correcteurs

Mise en place :

$010\ldots 10\ldots$

A —message→ B

Plb : interférences ⇝ erreurs de transmission

Idée : ajouter de la redondance

→ détecter existence d'erreur

↳ renvoyer le signal

↳ correction

Alphabet : ex : $\mathbb{F}_2$, $\mathbb{F}_q$

message :	redondance	transmission	réception
00	→ 00 00	⇝	00 01
01	01 01		↳ erreur
10	⋮		
11	11 11		

* bit de parité

00 ⇝ 000 ⇝ 110

01 ⇝ 011

10 ⇝ 101

11 ⇝ 110

transmission

on ne détecte pas les erreurs

F = alphabet $(F = \mathbb{F}_q)$

$m \geq k$

$\{mots\} \subset F^n$ ← espace vectoriel

F^k ↪ sous-espace

$n-k$ redondance

C = code

$(m_1, \dots, m_n)$

taux d'information ← $\frac{k}{n} < 1$

bon code : $\frac{k}{n}$ proche de 1

r erreurs

$i_1 < \dots < i_r$

m_{i_k} est faux

• corrige beaucoup d'erreurs

Def. distance de Hamming

$$d_H(x,y) = \#\{1 \le i \le n : x_i \neq y_i\}$$

$x = (x_1, \dots, x_n)$ $\quad$ $y = (y_1, \dots, y_n)$

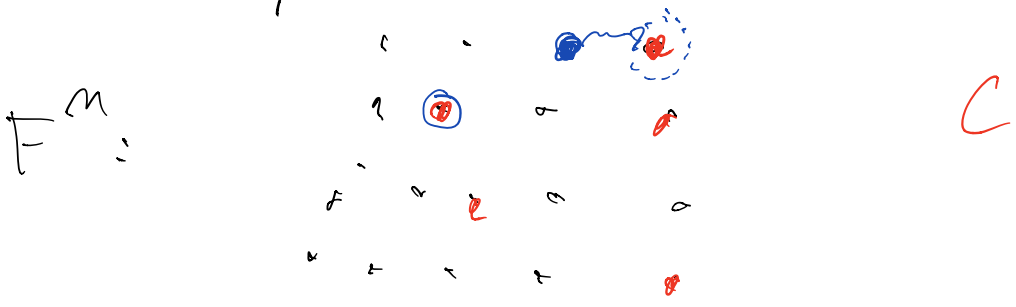
Hyp. r = nbre d'erreurs est petit

procédé de décodage

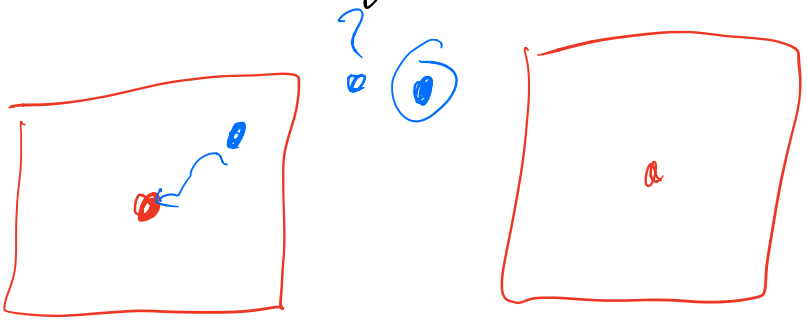
$$D : F^n \longrightarrow F^k = C$$

Notation. $C = F^q \subset F^n$

$$d = \min\{ d_H(x,y) : x \neq y \in C^2 \}$$



Boules centrées en 1 mot de C et de rayon $\epsilon = 2\left\lfloor \frac{d-1}{2} \right\rfloor$ sont disjointes (inégalité triangulaire)



Def : C est dit parfait si

$$F^n = \bigsqcup_{m \in C} B(m, \epsilon)$$

exo : $F = \mathbb{F}_q$ C est parfait

$$\#C \cdot \sum \binom{n}{i} (q-1)^i = q^n$$

Bon code : $\left\lfloor \frac{d}{n} \right\rfloor$ proche de 1

ℓ grand

Codes linéaires

$F = \mathbb{F}_q$

$C = \mathbb{F}_q^k \xrightarrow[\text{ser}]{} \mathbb{F}_q^n$

$d = \min_{0 \neq x \in C} w(x)$

$d_H(x,0) = w(x) =$ 1-ids de x ie le nombre de coordonnées non nulles

Prop : (Borne du singleton)
On a $d \leq n - k + 1$

(à faire)

$(t = 2\left\lfloor \frac{d-1}{2} \right\rfloor)$

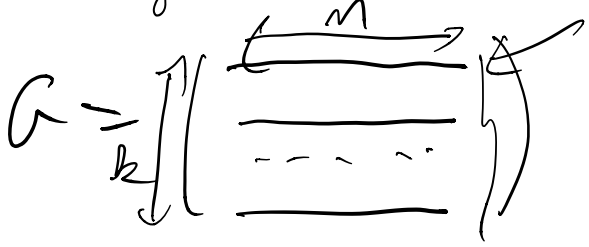
$\frac{d}{n} \leq 1 - \frac{k}{n} + \frac{1}{n}$

Rem : $\frac{d}{n} \longmapsto \frac{k}{n}$

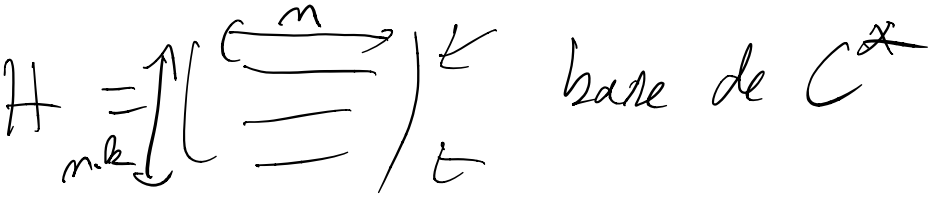
Def : Le code est dit MDS (Max Distance Separable) si $d = n - k + 1$

Matrices

* matrice génératrice — base

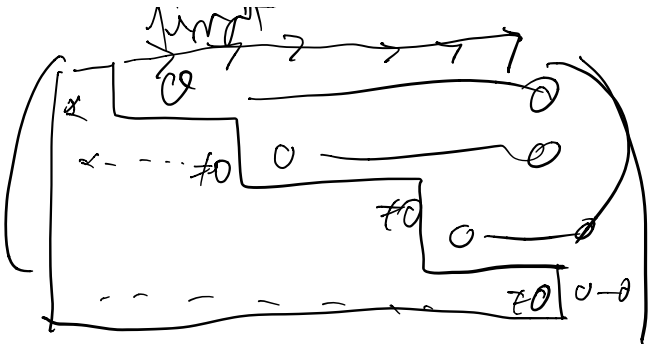


* matrice vérificatrice (ou de contrôle)



Prop : H vérificatrice $\iff G \cdot {}^tH = 0$

En pratique (échelonnement)



pivot de Gauss
sans permutation
(sur les colonnes)

$$x \in C \iff x \, {}^tH = 0$$

Déf : Un code est dit systématique

si $G = (I_k \mid B)$

I_k : le mot n'est pas modifié

B : redondance

$\Updownarrow$ à faire

$$H = (-{}^tB \mid I_{n-k})$$

$\mathbb{F}_q^k$

$m_0 \longrightarrow m \in C \subset \mathbb{F}_q^n$

Transmission

m' $\quad H m' \to = 0$ $\quad m' = m$ (ok si $\leq G$ éliminé)

$m' = m + \varepsilon$

$r = w(\varepsilon) \leq t$

On fait une table

ε tq $w(\varepsilon) \leq G \rightsquigarrow H\varepsilon$ $\quad \varepsilon =$

$m = m' - \varepsilon$

Prop : $d =$ nbre min de colonnes de H ($\in \mathbb{F}_q^{n-k}$) qui sont linéairement dépendantes

($xH = 0$ avec $w(x)$ minimal)

Code de Hamming (de longueur 7)

$q = 2$

$e_0 = (1\ 1\ 0\ 1\ 0\ 0\ 0)$

$e_1 = (0\ 1\ 1\ 0\ 1\ 0\ 0)$

$e_2 = (0\ 0\ 1\ 1\ 0\ 1\ 0)$

$e_3 = (0\ 0\ 0\ 1\ 1\ 0\ 1)$

$$H = \left(\begin{array}{ccccccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$$ ex a

$n = 7 \quad k = 4 \quad d = 3 \Rightarrow t = 1$

Codes linéaires cycliques

(idée = ajouter une structure d'algèbre)

Def : $C \underset{\text{sev}}{\subset} \mathbb{F}_q^n \quad \dim C = k$

est dit cyclique si $\forall m \in C \Rightarrow T(m) \in C$

où $T : (m_1, \dots, m_n) \longmapsto (m_n, m_1, \dots, m_{n-1})$

C
r
$\mathbb{F}_q^n$ $\quad \psi(C) = \{ P \mid g \mid P \}$
Δ

Lemme $\mathbb{F}_q^n \simeq \mathbb{F}_q[X] / (X^n - 1)$

via

$$(x_1, \dots, x_n) \xmapsto{\psi} x_n + x_{n-1} X + \dots + x_1 X^{n-1}$$

Alors $C \subset \mathbb{F}_q^n$ est cyclique ssi $\psi(C)$ est un idéal de $\mathbb{F}_q[X] / (X^n - 1)$

dem : $\psi(C)$ est un sev de $\mathbb{F}_q[X]/(X^n-1)$

c'est un idéal $\Leftrightarrow$ stable par multiplication par X

$$X \cdot (x_n + x_{n-1} X + \dots + x_1 X^{n-1})$$

$$x_n X + x_{n-1} X^2 + \dots + x_2 X^{n-1} + x_1 X^n$$

$$\| \text{ car } \boxed{X^n = 1}$$

$$x_1 + x_n X + \dots + x_2 X^{n-1}$$

Conséquence : { des codes linéaires cycliques de $\mathbb{F}_q^n$ }

$\uparrow$ bijection

{ des idéaux de $\mathbb{F}_q[X]/(X^n-1)$ }

$\uparrow$

{ diviseurs de $X^n - 1$ }

Rappel : $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ | $\exists ! q \mid n = 1$

$\Phi_n(X) = \prod P_i$ P_i irréd

$\forall i$ $\deg P_i$ = l'ordre de $g \in (\mathbb{Z}/n\mathbb{Z})^*$

Point de vue pratique : $C \hookrightarrow \boxed{g \mid X^n - 1}$

* code systématique

$(x_1, \dots, x_k) \in \mathbb{F}_q^k \longmapsto \boxed{C = C_I - C_R}$

où $\boxed{C_I = x_1 X^{n-1} + \dots + x_k X^{n-k}}$ ($n-k$)

C_R $\deg < n-k$ = le reste de la division euclidienne de C_I par g

↓ redondance

$\dots + x_{k+1} X + x_1 X^{n-k-1}$

* codage : $C_I \longmapsto C_I \cdot g$ $\deg \leq n-1$

(pas systématique)

Hyp : q ou $n = 1$

Prop : { codes linéaires cycliques de $\mathbb{F}_q^n$ }

↑ bijection

$\downarrow$

$\{ I \subset \mathbb{Z}/n\mathbb{Z}$ stables par la multiplication par $q \}$

---

dem : P polynôme $\in \mathbb{F}_q[X]$

$\{$ racines de P dans $\overline{\mathbb{F}_q} \} = \{ \alpha, \alpha^q, \ldots, \beta, \beta^q, \ldots \}$ (ζ_q^k, ζ_q^{kq}, ...)

$\cap$

$I \subset$ $\{$ racines de $X^n - 1 \}$

$\cap$ $\qquad$ $\|$

$\mathbb{Z}/n\mathbb{Z}$ $\qquad$ $\{ \zeta_q^k \quad 0 \le k \le n-1 \} \underset{\text{bij}}{=} \mathbb{Z}/n\mathbb{Z}$

ζ_q = racine prim $n$ième de 1

$P = a_1 X^{i_1} + \cdots + a_k X^{i_k}$ $\quad$ d min tq $g | P$ $\Rightarrow$ d

---

Prop : C code linéaire cyclique de $\mathbb{F}_q^n$

$\updownarrow$

$I \subset \mathbb{Z}/n\mathbb{Z}$ $\qquad$ Hyp : $\exists i$, $\exists q$, $\{ i+1, \ldots, i+d \} \subset I$

Conclusion $d \geq D+1$

distance du code

Lem = (Vandermonde)

$$R(X) = \lambda_1 X^{l_1} + \cdots + \lambda_k X^{l_k}$$

Hyp : $R \in C$ $\quad w(R) \leq D$

$\Downarrow$?

$R = 0$

$d = \min w(R)$
$R \neq 0$
$R \in C$

$R \in C \iff g \mid R$

$g = \prod (X - \alpha^q)$
$k \in I$

$R \in C \iff R(\alpha^k) = 0 \quad \forall k \in I$

$\Rightarrow R(\alpha^{i+1}) = \cdots = R(\alpha^{i+D}) = 0$

$(\lambda_1$

$$\begin{pmatrix} \alpha_1^{(i+2)k_2} & \cdots & \alpha_1^{(i+2)k_2} \\ \vdots & & \\ \alpha_2^{(i+d)k_2} & \cdots & \alpha_2^{(i+d)k_d} \end{pmatrix} \begin{pmatrix} \vdots \\ \lambda_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\downarrow$

inversible car matrice extraite d'une matrice de Vdm $\leftarrow$ inversible

$\square$

Pratique : $g(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n$

$$C = \begin{pmatrix} a_0 & \cdots & a_{n-2} & 1 & 0 & \cdots & 0 \\ 0 & & & & & & \\ \vdots & & & & & & \\ & & & & & & \\ 0 & & a_0 & a_{n-2} & & & 1 \end{pmatrix}$$

$$h(X) = \frac{X^{n+k} - 1}{g(X)} = b_0 + b_1 X + \cdots + b_{k-1} X^{k-1} + X^k$$

$$H = \begin{pmatrix} 1 & b_{k-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 & b_{k-1} & \cdots & b_0 \end{pmatrix}$$

$\underline{c \cdot {}^t H = 0}$ donc H = mat vérificatrice

rem : $m(X) \in C \iff m(X) \mid h(X)$ divisible par $X^n - 1$

Codes BCH (ex. : codes pour les CD)

$q, r, n \mid q^r - 1$

$\mathbb{F}_{q^r} \supset \mu_n$ racine n-ième de 1

$$\mathbb{F}_q[X]/(X^n - 1) \xrightarrow{\varphi} \mathbb{F}_{q^r}^{\delta - 1}$$

$$P \longmapsto (P(\alpha), P(\alpha^2), \ldots, P(\alpha^{\delta-1}))$$

$\ker \varphi = BCH(q, n, \delta)$

$\mathbb{F}_q$ idéal

$\langle poly \rangle$

$\updownarrow$

$I \subset \mathbb{F}_q[X]/(X^n - 1)$ stable par q

poly = ppcm des poly minimaux de $\xi_n, \xi_n^2, \ldots, \xi_n^{\delta-1}$

$I = \{ h \mid poly(\xi_n^h) = 0 \}$

$\cup$

$\{1, 2, \ldots, \delta - 1\}$

Fait : $BCH(q, n, \delta)$ est le plus petit code linéaire cyclique de $\mathbb{F}_q^n$ tq

$BCH(q, n, \delta) \hookrightarrow I \subset \mathbb{F}_q[X]/(X^n - 1)$

$I \supset \{1, 2, \ldots, \delta - 1\}$

et donc $\boxed{d \geq \delta}$!

Rem : $BCH(q,n,\delta)$ indépendant de c

$\Leftrightarrow \begin{cases} C = c_1 X^{n-1} + \dots + c_n \in BCH(q,n,\delta) \\ \Leftrightarrow C(\xi_n) = C(\xi_n^2) = \dots = C(\xi_n^{\delta-1}) = 0 \end{cases}$

$\delta = 2t+1 \Rightarrow$ $BCH(q,n,\delta)$ corrige t erreurs

Décodage : $q=2$

$m \longmapsto m' = m + E \quad \mu = w(E) \leq t$

$E = X^{l_1} + \dots + X^{l_\mu}$

But : Calculer $\mu, l_1, \dots, l_\mu$

$m'(\xi_n^i) = \overset{0}{\cancel{m}}(\xi_n^i) + \boxed{E(\xi_n^i)}$

$i = 1, \dots, 2t = \delta - 1$

connu

Principe : à partir de :

$$\begin{cases} \circ\ \mu \leq \epsilon \\ \circ\ \mathcal{E}(\xi_n^1), \dots, \mathcal{E}(\xi_n^t) \end{cases} \longrightarrow \begin{array}{|c|} \hline \mu \\ \ell_1 \\ \vdots \\ \ell_\mu \\ \hline \end{array}$$

$$\mathcal{E}(\xi_n) = \xi_n^{\ell_1} + \dots + \xi_n^{\ell_\mu} \qquad \beta_i = \xi_n^{\ell_i}$$

$$= \beta_1 + \dots + \beta_\mu = S_1(\beta_1, \dots, \beta_\mu)$$

$$\mathcal{E}(\xi_n^2) = \beta_1^2 + \dots + \beta_\mu^2 = S_2(\beta_1, \dots, \beta_\mu)$$

$$\mathcal{E}(\xi_n^\mu) = \beta_1^\mu + \dots + \beta_\mu^\mu = S_\mu(\beta_1, \dots, \beta_\mu)$$

Donc on connaît les sommes de Newton des $\{\beta_1, \dots, \beta_\mu\}$

relation de $\left\{\right.$ en caractéristique 0

Newton 1

$$\sigma_1(\beta_1,\dots,\beta_\mu),\ \dots\ ,\sigma_\mu(\beta_1,\dots,\beta_\mu)$$

$$X^\mu - \sigma_1 X^{\mu-1} + \sigma_2 X^{\mu-2} + \dots + (-1)^\mu \sigma_\mu$$

$$\prod_{i=1}^{\mu}(X-\beta_i) \leadsto \beta_i$$

⚠ relations de Newton ∃ des dénominateurs pb en carac $\neq 0$

Mais il existe un moyen de récupérer les β_i à partir de $\sigma_i(\beta_1,\dots,\beta_\mu)$ en caractéristique q.c.q

Exemples

• code de Hamming $n = \frac{q^r - 1}{q-1}$

$I = \{1, q, q^2, \dots, q^{r-2}\} \subset \mathbb{F}_{q^r}$

stable par multiplication par q

$d = 3$ ✓

• $d \geq 3$ $aX^{ik} + bX^{jk}$ n'est pas divisible par g ($\Leftrightarrow$ n'a pas α^{ik}, α^{jk} pour racine $\forall s = 0, \dots, r-1$)

• $d \leq 3$: $H \in \mathcal{M}_{r,n}$ vecteurs colonnes : n indép 2 à 2 : $n = \frac{q^r - 1}{q-1}$ ← dans chaque droite de $\mathbb{F}_q^r$ $\exists!$ vecteur de H

$d = 4$

généralisation $\mathbb{F}_{127}^x$

Cas particulier $r = 2$

c_1, c_2 ↓ $c_1 + c_2$: combinaison de c_1, c_2

* Minitel

$\mathbb{F}_{128} \simeq \mathbb{F}_2[X] / (X^7 + X^3 + 1)$

$X^7 + X^3 + 1$ irréd car n'a pas de racines dans $\mathbb{F}_4, \mathbb{F}_8$

erreurs

message = 15 octets = 120 bits

$\frac{120}{128}$ mode de 1

$M = a_0 a_1 \dots a_{119}$ $\quad a_i \in \mathbb{F}_2$

$P = a_0 \underbrace{x^{126} + \dots + a_{119} x^7}_{C_I} \equiv \underbrace{a_{120} x^6 + \dots + a_{126}}_{C_R}$

a_{127} = bit de parité

$m = a_0 \dots a_{119} \mid a_{120} \dots a_{126} \mid a_{127}$

$\rightsquigarrow \underline{\epsilon = 1}$ (exact) $\qquad \boxed{d = 3}$

message reçu : Hyp : au + 2 erreurs

- c'est un mot du code $\Rightarrow$ 0 erreur
- sinon : bit de parité 1 ou 2 erreurs
  - 1 erreur $\rightarrow$ on corrige
  - 2 erreurs $\rightarrow$ on demande de renvoyer l'information

ENS

Codes de Reed-Solomon (CD)

$q = 2^m$ $\quad n = q-1$ $\quad \zeta_n \in \mathbb{F}_q^\times$

$q \equiv 1 \ [n]$

$g(X) = \prod_{i=1}^{n-k} (X - \zeta_n^i)$

$\forall I \subset \mathbb{Z}/n\mathbb{Z}$ est stable par la multiplication par q

$I = \{1, 2, \dots, n-k\}$

$\Rightarrow d \geq n-k+1 = q-k$

Borne du singleton : $d \leq q-k$

$\Rightarrow \boxed{d = q-k}$ $\quad \left(\underset{q-1}{n}, k, \underset{q-k}{d}\right)$

exc des CD

$\mathbb{F}_{256} \simeq \mathbb{F}_2[X] / (X^8 + X^7 + X^6 + X^5 + X^4 + X^2 + 1)$ ($P(X)$)

rem : $P(X) + X^8 + X = \frac{X^q - 1}{X - 1}$

exc: mq que $\begin{cases} \cdot P(X) \text{ est irred} \\ \cdot \alpha = \overline{X} \text{ générateur de } \mathbb{F}_{256}^{\times} \end{cases}$

$\alpha = 3_{255}$

$g(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^3)(X-\alpha^4)$ $\quad n = 255$

$d = 5 \quad t = 2$ (octets) $= 16$ bits

codage systématique: $M = a_0 \dots a_{k-1}$

a_i = octets $\in \mathbb{F}_{256}$

$k \leq 255 - 4$

252

En pratique

$k = \begin{matrix} 28 \\ 32 \end{matrix}$

$a_0 X^4 + a_1 X^5 + \dots + a_{k-1} X^{4+k-1}$

ξ

$b_0 + b_1 X + b_2 X^2 + b_3 X^3 =$ reste de la division euclidienne avec g

PB(X) $\rightsquigarrow$ $b_0 + b_1 X + b_2 X^2 + b_3 X^3 + a_0 X^4 + \dots + a_{k-1} X^{3+k}$

Fait: on peut corriger 4 effacements

(exc: CD rayures donc certains octets)

| sont illisibles $\Rightarrow$ on les force $= 0$ |

dem : i_1, i_2, i_3, i_4

$R(X) = \varepsilon_1 X^{i_1} + \varepsilon_2 X^{i_2} + \varepsilon_3 X^{i_3} + \varepsilon_4 X^{i_4}$

$\varepsilon_i \in GF_{256}$ Ag $\alpha, \alpha^2, \alpha^3, \alpha^4$

Φ $\quad$ I

$R() = B()$

$R(\alpha) = B(\alpha)$

$R(\alpha^2) = B(\alpha^2)$

$R(\alpha^3) = B(\alpha^3)$

$R(\alpha^4) = B(\alpha^4)$

$\exists$ solution (car le bon message existe)

et elle est unique

En effet si $\exists 2 \Rightarrow \Delta = R_1 - R_2 = \lambda_1 X^{i_1} + \dots + \lambda_4 X^{i_4}$

alors $\Delta(\alpha) = \Delta(\alpha^2) = \Delta(\alpha^3) = \Delta(\alpha^4)$

$\Rightarrow (X-\alpha)(X-\alpha^2)(X-\alpha^3)(X-\alpha^4) \mid \Delta(X)$

||

$X^4 + \beta_1 X^3 + \beta_2 X^2 + \beta_3 X + \beta_4$ avec $\beta_i \neq 0$

$\Rightarrow$ Δ a au moins 5 monômes non nuls (sauf si $\Delta = 0$)

exo : écrire les détails

Mise en pratique sur les CD

Pb : rayures rendent illisibles bcp de bits consécutifs

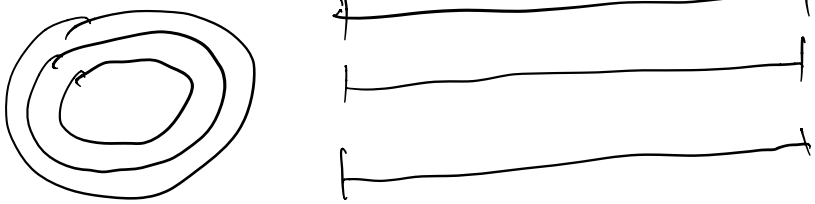
Idée : on va éclater les mots

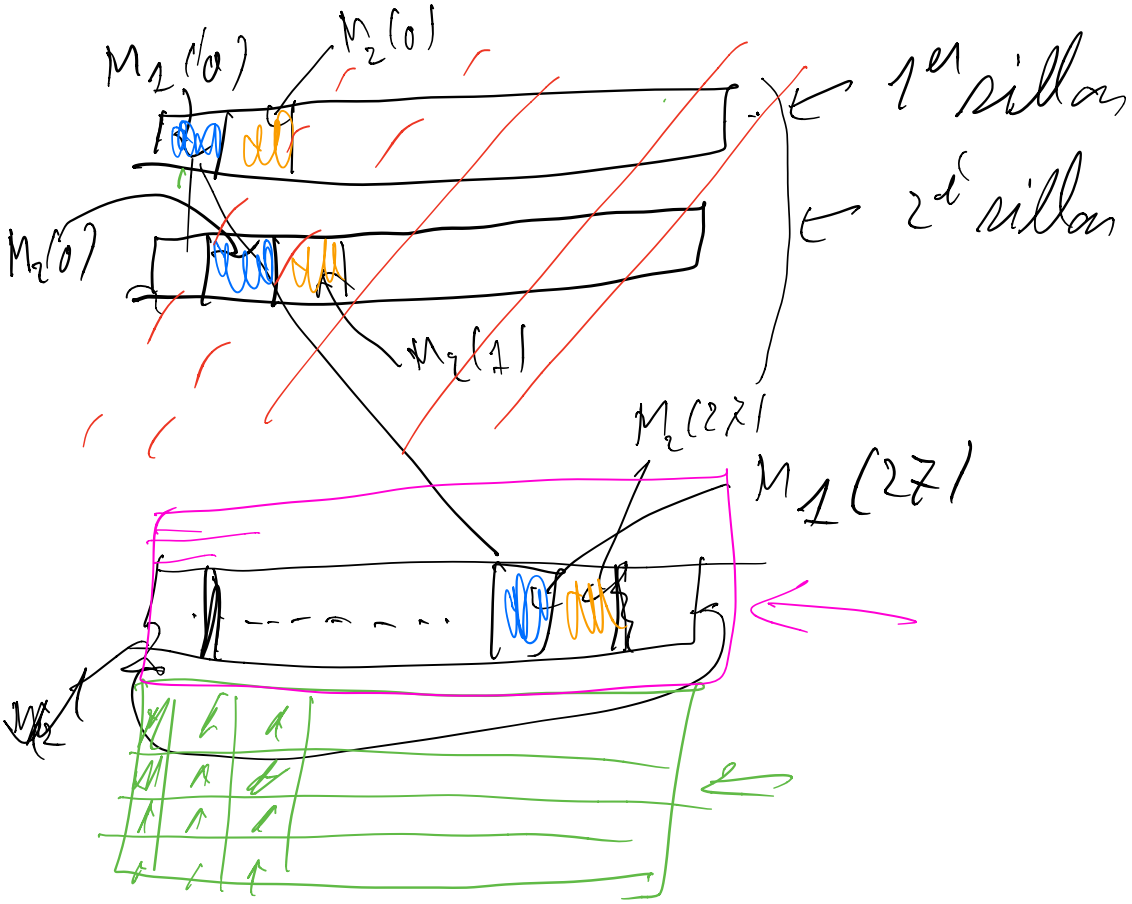
Table d'entrelacement à retard

Mots : 24 octets + 4 octets de redondance

$M_1 = M_1(0) \dots M_1(27)$

+ 4 octets de redondance





Dans la pratique : on suppose des rayures de 2 mm de large

---

3 stratégies :

- $d = 2\lfloor \frac{n}{2} \rfloor + 1$ ⇝ BCH $\quad I \subset \{1, 2, \dots, d-1\}$
- taux d'information (I le plus petit possible) ⇝ Hamming $\quad d = 3$

$\mathbb{F}_q = \{1, g, \dots, g^{q-2}\} \quad g^{q-1} \equiv 1 \ [n]$

* borne du singleton (égalité)
code de Reed-Solomon

---

ex: Codes de Golay

- codes quadratiques (symbole de Legendre)

$$g(X) = \prod (X - \zeta_p^a)$$
$$\left(\frac{a}{p}\right) = 1$$

$$\#I = \frac{p-1}{2}$$

$n = p$
$\mathbb{F}_q$
$\left(\frac{q}{p}\right) = 1$

$q=2$ $p=7$ ⇝ Code de Hamming $(7, 4, 3)$
$q=2$ $p=23$ ⇝ Code de Golay

G_{11} : $q=3$ $n=11$ $(\mathbb{Z}/11\mathbb{Z})^\times \Rightarrow I = \langle 3 \rangle$
$(1, 3, 4, 5, 9)$

$d = 5$

2 corrections parfait

* g_{23} $q=2$ $n=23$ $I = \langle 2 \rangle$

3 – Comédien parfait