I Codes correcteurs d'erreur

(communication internet (fibre ou satellite), lecture d'un CD)

Idée générale : La transmission d'un signal n'est pas totalement fiable, problème de "bruit". On veut être capable de détecter des erreurs, voire de les corriger.

Signal initial $(u_1, \dots, u_k)$ (dans $\mathbb{F}_2^k$ ou $\mathbb{F}_2^k$) —"encodage"→ Signal envoyé $(x_1, \dots, x_n)$ (avec $n \geq k$) —"transmission"→ Signal reçu $(y_1, \dots, y_n)$ avec $y_i = x_i$ "souvent" —"décodage"→ Signal décodé (corrigé ?) $(v_1, \dots, v_k)$

Def
- $(x_1, \dots, x_n)$ "mot du code"
- $\frac{k}{n}$ taux de transmission (partie informative du signal envoyé)
- $r = n - k$ redondance

Question : Peut-on obtenir $(v_1, \dots, v_k) = (u_1, \dots, u_k)$ si un certain nombre de y_i sont $\neq x_i$?

Méthode : Exploiter une structure linéaire (voire algébrique)

1) 3 Exemples historiques simples :

a) "Test de parité"

Pour un signal $(u_1, \dots, u_k) \in \mathbb{F}_2^k$, on envoie $(u_1, \dots, u_k, \sum_{i=0}^{k} u_i)$

c'est à dire la redondance est de 1.

Pour $k = 6$, 101011, on a $x_7 = 0$

- S'il y a une erreur dans le signal reçu (élément de $\mathbb{F}_2^7$), on le détecte car alors $y_7 \neq \sum_{i=0}^{6} y_i$. Mais on ne sait pas localiser (ni corriger l'erreur).
- S'il y a 2 erreurs dans le signal reçu, on a $y_7 = \sum_{i=0}^{6} y_i$ et le destinataire ne peut pas détecter qu'il n'a pas reçu le bon message.

b) Le code à répétition

On répète chaque bit 3 fois.

Ex : $(u_1, u_2, u_3, u_4) \mapsto (u_1, u_1, u_1, u_2, u_2, u_2, u_3, u_3, u_3, u_4, u_4, u_4)$

"décodage majoritaire"
Pour chaque groupe de 3 bits, il y a un élément présenté 2 ou 3 fois, c'est celui qu'on choisit.

Taux de transmission $= \frac{1}{3}$.

On peut corriger 1 erreur mais pas toujours 2.

2a) Premier code de Hamming

4 bits d'information, 5 bits de redondance, "longueur" = 4 + 5 = 9.

u_1	u_2	u_1+u_2
u_3	u_4	u_3+u_4
u_1+u_3	u_2+u_4	$\sum u_i$

Ex : 1101 ⇝

1	1	0
0	1	1
1	0	0

⟹ 110 011101

Supposons que le destinataire reçoive comme 5e bit 0 au lieu de 1 (élément souligné = erreur)

1	1	0
0	0	1
1	0	1

la 2e ligne et la 2e colonne ont un souci.

En supposant qu'il n'y a 1 seule erreur dans la transmission, l'erreur est corrigeable

Taux de transmission : $\frac{4}{9}$ $\left(> \frac{1}{3}\right.$ du code à répétition$\left.\right)$

On peut corriger une erreur, et en détecter 3.

Ex : avec le même signal initial,

si on reçoit

1	1	0
0	0	1
1	0	0

, on sait qu'il y a ≥2 erreurs, mais on ne sait pas où. (pourrait être l'initial ou $\begin{pmatrix}1&1&0\\0&0&\underline{0}\\1&1&0\end{pmatrix}$ ou ⇝)

si on reçoit

1	1	0
0	0	0
1	0	0

, le système de correction croit qu'il y a 1 erreur (et non 3) et corrige faussement en $\begin{pmatrix}1&1&0\\0&0&0\\1&1&0\end{pmatrix}$

si on reçoit

0	0	0
1	0	1
1	0	1

, le destinataire croit avoir reçu le bon message

Idée : * Améliorer cette idée en utilisant de l'algèbre linéaire.

On va définir un code de Hamming avec $k = 4$, $n = 7$ (i.e. $r = 3$ et taux $= \frac{4}{7} > \frac{1}{2}$)

qui corrige 1 erreur et en détecte 2.

* Formaliser ces idées en mettant des notions de distance, de code, de correction dans un contexte mathématique général.

2) Théorie des codes correcteurs linéaires

On travaille sur un corps fini $\mathbb{F}_q$ (très souvent $q=2$ ou une puissance de 2)

Déf * Pour un vecteur (pensé ensuite comme un vecteur ligne) $x \in \mathbb{F}_q^n$, on définit son poids $w(x)$ par son nombre de composantes non nulles.
D'où $0 \leq w(x) \leq n$.

Prop L'application $d_H : \begin{cases} \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{N} \\ (x,y) \longmapsto w(x-y) \end{cases}$ est une distance (dite "de Hamming") sur $\mathbb{F}_q^n$.

Déf * On appelle code linéaire de longueur n un sous-espace vectoriel C de $\mathbb{F}_q^n$.

* Les vecteurs $(x_1, \dots, x_n)$ de C sont les mots du code.
Il y a q^k mots de code si C est de dimension q.

* La distance minimale du code C est définie par

$$d = \min_{x \in C \setminus \{0\}} w(x) \left(= \min_{\substack{x \neq y \\ x \in C \\ y \in C}} w(x-y) \right)$$

* On dit alors que C est un $[n,k,d]$-code (ou un code de paramètres $[n,k,d]$)

Rem On peut définir le poids complet d'un ~~corps~~ vecteur par la collection :

$$\left(w_k(x) = \left| \{ i \in [\![1,n]\!], x_i = k \} \right| \right)_{k \in \mathbb{F}_q}.$$

Alors $w(x) = \sum_{k \in \mathbb{F}_q \setminus \{0\}} w_k(x)$.

Prop Soit C un $[n,k,d]$-code. Alors $d \leq n+1-k$.
(intuition de cette prop : la distance est plus petite que la redondance +1)

Preuve Soit V le sev de $\mathbb{F}_q^n$ formé des vecteurs dont les $k-1$ dernières composantes sont 0.
C'est un sev de dimension $n-k+1$.
Comme $\dim C + \dim V = n+1$, on a $C \cap V \neq \{0\}$. $\Big\}$ $\exists x_0 \in C \setminus \{0\}$, $w(x_0) \leq n-k+1$
~~Et~~ $\forall x \in C \setminus \{0\}$, $w(x) \geq n-k+1$.
Comme d est le minimum des $w(x)$ où $x \in C \setminus \{0\}$, on a $d \leq w(x_0) \leq n-k+1$.

Prop : Soit C un $[n,k,d]$-code.
Les boules (pour la distance de Hamming) fermées et centrées sur les mots du code C et de rayon $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ sont 2 à 2 disjointes.

Preuve : Supposons qu'il existe un $y \in \mathbb{F}_q^n$ dans 2 boules, càd $y \in \overline{B}(x_1,t) \cap \overline{B}(x_2,t)$ où $\begin{matrix} x_1 \in C \\ x_2 \in C \end{matrix}$
Alors $d(x_1,x_2) \leq d(x_1,y) + d(x_2,t) \leq 2t < d$.
D'où $x_1 = x_2$.

Rem : Cette propriété signifie que si le destinataire reçoit un message $x \in \mathbb{F}_q^n$ et qu'on suppose qu'il y a moins de t erreurs dans la transmission, alors x est dans (au plus) une boule de la forme $\overline{B}(c,t)$ pour $c \in C$.
Ce mot c est alors le message que l'expéditeur voulait transmettre.

Q : En pratique, pour un $x \in \mathbb{F}_q^n$ reçu, comment retrouver le c initial ?
Méthode naïve : "table des syndromes" (cf. matrice de contrôle)

Inégalité de Hamming :

En notant $r = n - k$ (la redondance) et $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, on a :

$$\sum_{l=0}^{t} (q-1)^l \binom{n}{l} = \underbrace{1 + (q-1)\binom{n}{1} + \dots + (q-1)^t \binom{n}{t}}_{\text{nombre d'éléments d'une boule fermée de rayon } t} \leq q^r$$

(en multipliant par q^k (= nombre de mots du code), on obtient que le nombre d'éléments de $\mathbb{F}_q^n$ dans les boules disjointes est inférieur au cardinal de $\mathbb{F}_q^r$)

Ex : Pour $q = 2$ et $t = 1$, on a $1 + 4 + n \leq 2^r$, d'où $r \geq 3$.
et $k = 4$

Ceci signifie que la redondance est d'au moins 3, donc que le taux de transmission est $\leq \frac{4}{7}$

On verra par la suite l'exemple d'un tel code atteignant cette borne :
le code de Hamming binaire (qui sera une amélioration du 1er code de Hamming).

Déf : On dit qu'un code est parfait si l'inégalité de Hamming est une égalité.
Cette condition est équivalente à :

$$\mathbb{F}_q^n = \bigcup_{c \in C} \{x \in \mathbb{F}_q^n,\ d(c,x) \leq t\}$$

Il y a 2 manières d'associer des matrices à un code linéaire :
* Soit C est l'image de la matrice $\rightsquigarrow$ matrice génératrice
* Soit C est le noyau de la matrice $\rightsquigarrow$ matrice de contrôle.

Déf [Une matrice génératrice d'un $[n,k,d]$-code est $G \in M_{k,n}(\mathbb{F}_q)$ dont les lignes forment une base de C.
Ainsi C est l'image de l'application linéaire injective :

$$\begin{array}{ccc} \mathbb{F}_q^{\,k} & \longrightarrow & \mathbb{F}_q^{\,n} \\ c & \longmapsto & c.G \end{array}$$

D'où $\forall x \in \mathbb{F}_q^{\,n}$: $x \in C \iff \exists\, c \in \mathbb{F}_q^{\,k},\ x = c.G$
En particulier, G est de rang k ($=$ rang maximal dans $M_{k,n}(\mathbb{F}_q)$, où $k \le n$)

Déf : On dit que G a une forme systématique si elle s'écrit $(I_k \,;\, M)$
Rem : Pivot de Gauss

Ex : a) Code "test de parité"

$$G = \begin{pmatrix} 1 & & & 1 \\ & \ddots & & \vdots \\ & & 1 & 1 \end{pmatrix} \in M_{k,k+1} \quad \text{et} \quad (x_1,\dots,x_k).G = (x_1,\dots,x_k,\textstyle\sum x_i)$$

b) Code de Hamming (premier code...)

a_1	a_2	a_1+a_2
a_3	a_4	a_3+a_4
a_1+a_3	a_2+a_4	$\sum a_i$

$$G = \left(\begin{array}{ccc|ccc} 1 & & & 1 & 0 & 1 & 0 & 1 \\ & 1 & & 0 & 1 & 1 & 0 & 1 \\ & & 1 & 1 & 0 & 0 & 1 & 1 \\ & & 1 & 0 & 1 & 0 & 1 & 1 \end{array}\right)$$

pour le choix

1	2	~~7~~
3	4	8
5	6	9

(Si on fait un autre choix, p. ex. $\begin{matrix}1&2&3\\4&5&6\\7&8&9\end{matrix}$, la matrice n'est plus sous forme systématique)

c) Code de Hamming binaire H_3

On le définit par sa matrice génératrice [illegible] $\mathbb{F}_2$.

$$G = \begin{pmatrix} 1000 & 110 \\ 0100 & 101 \\ 0010 & 011 \\ 0001 & 111 \end{pmatrix}$$

à prouver

Ce code est de distance 3, donc de paramètres $[7,4,3]$.
Il est parfait.
Son taux est $\frac{4}{7}$.

Rem : Les 3 colonnes de redondance signifient qu'on a "ajouté" l'information $\begin{cases} x_1+x_2+x_4 \\ x_1+x_3+x_4 \\ x_2+x_3+x_4 \end{cases}$
Par combinaison linéaire de ces colonnes, on obtient x_1+x_2, x_2+x_3, x_1+x_3, x_4.
À comparer aux 5 colonnes redondantes du code de Hamming naïf.

Def Une <u>matrice de contrôle</u> (ou de parité) d'un $[n,k,d]$-code est une matrice $H \in M_{n-k,n}(\mathbb{F}_q)$ tq $\forall x \in C$, $H.{}^t x = 0$ (ie $C = \operatorname{Ker} H$)

H est une matrice génératrice du code dual $C^\perp = \{x' \in \mathbb{F}_q^n,\ \forall x \in C, \langle x, x'\rangle = 0\}$ pour la forme bilin sym non dég : $\langle\_,\_\rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, $(x,y) \longmapsto \sum x_i y_i$.

En particulier, H est de rang $n-k$ et $H.{}^tG = 0$

Prop Pour G matrice génératrice de C s'écrivant $G = (I_k \mid M)$ avec $M \in M_{k,r}(\mathbb{F}_q)$, une matrice de contrôle de C est $({}^tM \mid I_r)$.

Preuve : ~~Calcul d'orthogonal~~ On note $M = (v_{ij})$

$(x_1,\dots,x_{k+r}) \in C \iff \sum x_i v_{ij} = x_{k+j}\ \forall j \in [\![1,r]\!]$

$\iff \forall j \in [\![1,r]\!]$, $(x_1,\dots,x_{k+r})$ orthogonal à la j^e ligne de H

D'où $C \subseteq \operatorname{Ker} H$.

Or les dimensions sont les mêmes.

Ex : Pour H_3, où $G = \left(\begin{array}{cccc|ccc} 1 & & & & 1 & 1 & 0 \\ & 1 & & & 1 & 0 & 1 \\ & & 1 & & 0 & 1 & 1 \\ & & & 1 & 1 & 1 & 1 \end{array}\right)$, on a $H = \left(\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$

Obs : * chaque colonne de H correspond à un nombre en binaire entre 1 et $2^3-1=7$

On peut définir H_m par sa matrice de ~~parité~~ contrôle $m \times (2^m-1)$ dont les colonnes sont les éléments non nuls de $\{0,1\}^m$.

* Le plus petit nombre de colonnes linéairement dépendantes dans H est 3 et la distance de C est 3.

Prop Soit C un $[n,k,d]$-code et H matrice de contrôle de C. Alors d est le plus petit nombre de colonnes linéaires dépendantes dans H.

Preuve * Supp que tout ensemble de s colonnes de H est libre sur $\mathbb{F}_q$.
Alors pour tout x de $C \setminus \{0\}$, on a $H.{}^tx = 0$, càd $\sum x_j C_j(H) = 0$ (C_j : j^e col)
d'où $w(x) > s$ et donc $d > s$ (car C fini).
* Réciproquement, supposons $\exists$ s colonnes de H lin. dépendantes sur $\mathbb{F}_q$.
Donc $\exists x = (x_1 \dots x_n) \in \mathbb{F}_q^n \setminus \{0\}$ avec $w(x) \leq s$ et $\sum_{j=1}^{n} x_j C_j(H) = 0$ (ie $H.{}^tx = 0$) et donc $x \in C$.
D'où $d \leq s$.

Exo Décoder le mot reçu (0111110) pour le code de Hamming H_3.

1) (tâtonnements) On a $0111001 \in C$
La différence est 0000111. Et $0000111 \in C$.
D'où $0100110 \in C$ et est à distance 1 du mot reçu. → c'est le mot envoyé

2) On calcule $y.{}^tH$

$$(0111110)\begin{pmatrix}1&1&0\\1&0&1\\0&1&1\\1&1&1\\1&0&0\\0&1&0\\0&0&1\end{pmatrix} = (1\,1\,1) = \underbrace{(0010000)}_{\substack{=\varepsilon \text{ erreur} \\ = y - x \\ (\text{car } x.{}^tH = 0)}}\begin{pmatrix}1&1&0\\1&0&1\\0&1&1\\1&1&1\\1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

Def "syndrome" $y.{}^tH$, qui vaut aussi $\varepsilon.{}^tH$

Ici calculer tous les syndromes se fait en prenant les 7 colonnes de H, qui sont $e_i.{}^tH$.) En pratique trop de syndromes à calculer pour les codes

Méthode de décodage "par syndrome"

Soit H la matrice de contrôle de C
x mot émis $\in C$
y mot reçu
$\varepsilon = y - x$ l'erreur, de poids au plus $d-1$ (de telle sorte que $y \in C \Leftrightarrow \varepsilon = 0$)

Déf le syndrome de y est le vecteur ligne $y\,{}^tH$

Prop : * $y \in C \Leftrightarrow y\,{}^tH = 0$ $\left(\Leftrightarrow H.\,{}^ty = 0 \Leftrightarrow {}^ty \in \operatorname{Ker} H = C\right)$

* $y\,{}^tH = (x+\varepsilon).\,{}^tH = \varepsilon.\,{}^tH$ (car $x\,{}^tH = 0$)

Prop On peut préétablir la table des syndromes pour les mots de poids $\leq t = \left[\frac{d-1}{2}\right]$

Prop : Pour ε et ε' de poids au plus t, $(\varepsilon.\,{}^tH = \varepsilon'\,{}^tH \Rightarrow \varepsilon = \varepsilon')$

Preuve : En effet, $(\varepsilon - \varepsilon').\,{}^tH = 0$, donc $\varepsilon - \varepsilon' \in C$. Comme $\varepsilon - \varepsilon'$ est de poids $\leq d-1$, on a $\varepsilon - \varepsilon' = 0$.

Ceci signifie que le syndrome caractérise l'erreur.

Ex • pour H_3, on calcule les syndromes pour les 7 mots de poids ≤ 1.

Mots de poids $\leq e$	Syndromes
1000000	110
0100000	101
e_i	i^e ligne de ${}^tH$ $= i^e$ colonne de H

Décodons $y = 1111000$: $(1111000)\begin{pmatrix} 1&1&0\\ 1&0&1\\ 0&1&1\\ 1&1&1\\ 1&0&0\\ 0&1&0\\ 0&0&1 \end{pmatrix} = (111) = 4^e$ ligne de ${}^tH$ $= 4^e$ colonne de H

D'où $\varepsilon = e_4$ et $x = y - e_4 = (1110000)$

$y = 1001001$ $\quad y.\,{}^tH = (000)$ $\quad$ d'où $x = y \in C$

$y = 0011000$ $\quad y.\,{}^tH = (100)$ $\quad$ d'où $\varepsilon = e_5$ et $x = 0011100$

• pour le 1er code de Hamming :

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

syndrome des mots de poids 1 sont les colonnes de H.
$t = 1$ car $d = 4$.

Décodons $y = 11110111$ $\quad y.\,{}^tH = (0111) = 4^e$ col $\quad x = 11100111$

$y = 01110111$ $\quad y.\,{}^tH = (1110) = C_1 + C_4 = C_2 + C_3$ $\rightsquigarrow$ deux valeurs de x possible

$y = 00100111$ $\quad y.\,{}^tH = (1100) = C_1 + C_2 = C_3 + C_4 = C_5 + C_6$

Rem : Peu de codes parfaits : ~~Rare~~ répétition, Hamming H_m et codes de Golay (semaine prochaine ?)

Hamming H_m : code $[2^m-1, 2^m-m-1, 3]$ sur $\mathbb{F}_2$

définit par sa matrice de contrôle $m \times (2^m-1)$ dont les colonnes sont les éléments non nuls de $\{0,1\}^m$

Prop $d=3$

Preuve $\begin{cases} 2 \text{ colonnes sont toujours indépendantes.} \\ \exists \text{ triplets de colonnes liées.} \end{cases}$

Prop Le code est parfait :

$$1 + n = 2^m \quad \text{d'où} \quad n = 2^r - 1, \quad k = 2^r - r - 1.$$

Réciproquement, un code binaire parfait avec $d=3$ (donc $t=1$) ~~est~~ a ces paramètres.

Ex : Pour $m=7$, on trouve un code $[127, 119, 3]$
le minitel utilisait un code $[128, 120, 3]$ (où on a ajouté un bit de parité)
$120 = 15 \times 8$, càd chaque paquet avait 15 octets.

Meilleure correction :

Pour $t=2$: $1 + n(q-1) + \frac{n(n-1)}{2}(q-1)^2 = q^n$

Il y a une (unique) solution entière : $q=3$, $n=11$, $r=5$ (i.e $k=6$) $\boxed{\text{Golay ternaire}}$
la boule unité a $2^5 = 243$ éléments, d'où 243 syndromes. $[11, 6, 5]$ sur $\mathbb{F}_3$

Pour $t=3$

$$1 + n(q-1) + \frac{n(n-1)}{2}(q-1)^2 + \frac{n(n-1)(n-2)}{6}(q-1)^3 = q^n$$

Solution unique : $q=2$, $n=23$, $r=11$ ($k=12$) $[23, 12, 7]$ sur $\mathbb{F}_2$
la boule a 2048 éléments.

Code de Reed-Solomen (généralisés)

Exemples : CD, sondes spatiales, QR codes

Idée : En plus de la structure linéaire, il y a des propriétés polynomiales qui vont aider à trouver et corriger les erreurs

But : Construire une famille de codes linéaires (de distance maximale $d = n-k+1$) sur $\mathbb{F}_q$ avec un algorithme de décodage "rapide" (polynomial)

Ex : * Code $[6,4,3]$ sur $\mathbb{F}_7$

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

$\operatorname{rg}(H) = 2$ et tout ensemble de 2 colonnes est lin indép

car $\forall \alpha \neq \beta \in \mathbb{F}_7 \setminus \{0\}$ $\begin{vmatrix} 1 & 1 \\ \alpha & \beta \end{vmatrix} = \beta - \alpha \neq 0$ Donc $d \geq 3$ Or $d \leq 3$

* Code $[6,3,4]$ sur $\mathbb{F}_7$

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

Soient $\alpha, \beta, \gamma \in \mathbb{F}_7$ 2 à 2 distincts

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{vmatrix} = (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma) \neq 0 \quad \text{(Vandermonde)}$$

$$\det(\cdot) = \prod_{i<j} (a_i - a_j)$$

D'où c'est bien une matrice de contrôle et tout ensemble de 3 colonnes est lin indép.

Donc $d \geq 4$ Or $d \leq 4$ $(n-k+1)$

D'où $d = 4$.

Def Soit $\mathbb{F}_q$ corps fini, $n \in \mathbb{N}^*$ et $k \in [\![0, n]\!]$

Soit $\alpha_1, \dots, \alpha_n$ dans $\mathbb{F}_q \setminus \{0\}$ 2 à 2 distincts

$v_1, \dots, v_n$ dans $\mathbb{F}_q \setminus \{0\}$

Un code de Reed-Solomon généralisé $[n, k, ?]$ sur $\mathbb{F}_q$ est un code linéaire dont une matrice de contrôle est $V_{n-k,n}^{(\alpha)} \cdot D_n^{(v)}$

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

On appelle α_i les localisateurs du code

v_i les multiplicateurs

Si $n = q-1$ le code est primitif

Si $\forall i$, $v_i = 1$, le code est normalisé.

On note GRS un tel code.

Def Un code RS est un GRS tq $n \mid q-1$

$\alpha \in \mathbb{F}_q$ est d'ordre multip. n

$\forall i$, $\begin{cases} \alpha_i = \alpha^{i-1} \\ v_i = \alpha^{b(i-1)} \end{cases}$ (pour un b entier fixé)