Codes de Reed-Solomon

HMIN118 : Théorie de l'information

Université de Montpellier – Faculté des Sciences

→ Excellents de bcp de points de vue
→ Utilisés dans les CD / DVD
→ Très polyvalents

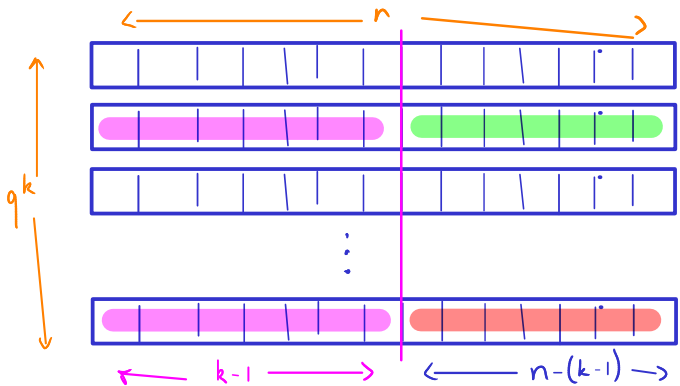
Borne de Singleton

longueur — distance minimale — taille de l'alphabet — dimension

Théorème

Soit C un code $(n, k, d)_q$. Alors $d \leq n - k + 1$.

#messages = # mots de code $= q^k$



préfixe de lgr $k-1$ $= q^{k-1} < q^k$

$\Rightarrow$ $\exists$ deux mots de code u et v qui ont le même préfixe de lgr $k-1$

$\Rightarrow \delta(u, v) \leq n - k + 1$

$\Rightarrow$ la distance minimale est $\leq n - k + 1$.

Borne de Singleton

Hamming : $k=4$, $n=7$

Théorème

Soit C un code $(n, k, d)_q$. Alors $d \leq n - k + 1$.

C : { lgr des messages : dimension } $\xrightarrow{\text{Encodage}}$ { lgr mots de code : longueur }

message $\longleftarrow$ mots (év. $\neq$ mots de code)

Déf Un code qui atteint la borne de Singleton est appelé MDS (Maximum Distance Separable)

↳ Les codes de R-S sont MDS.

Corps finis

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ $\mathbb{F}_q$

Théorème

$\mathbb{Z}/p\mathbb{Z}$ est un corps si (et seulement si) p est premier : on peut y effectuer des additions, soustractions, multiplications et divisions. $(a+b)\times c = ac+bc$, ---

$\mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$ avec les opérations modulo p :

$p = 7$ $\{0, \dots, 6\}$

$5+4 = 2$ $(5+4 = 9 = 7+2)$

$4\times 3 = 5$ $(4\times 3 = 12 = 7+5)$

$6\times 4 = 3$ $(6\times 4 = 24 = 21+3 = 3\times 7+3)$

$2-6 = 3$ $(2-6 = -4 = -7+3)$

$1/3 = 5$ $(3\times 5 = 15 = 2\times 7+1)$

$\Leftarrow 3\times 5 = 1$

$2/3 = 3$ $(2/3 = 2\times 1/3 = 2\times 5 = 3$ car $2\times 5 = 10 = 7+3)$

Polynômes

$$F(X) = \sum_{i=0}^{d} f_i X^i$$

d : degré ; X : variable ; f_i : coefficients $\in \mathbb{F}_q$

Additions / soustractions

$$F = \sum_{i=0}^{d} f_i X^i \qquad G = \sum_{i=0}^{d} g_i X^i$$

$$\Rightarrow F + G = \sum_{i=0}^{d} (f_i + g_i) X^i$$

Multiplication

$$F \times G = \sum_{i=0}^{2d} \left(\sum_{j+k=i} f_j g_k \right) X^i$$

$$F(X) = 1 + 3X + 2X^2 + 5X^3$$

dans $\mathbb{F}_7$

$$G = 3 + 4X + 2X^2 \ (+0X^3)$$

$$F+G = 4 + (0X+) + 4X^2 + 5X^3$$

$$F \times G = (1 + 3X + 2X^2 + 5X^3) \cdot (3 + 4X + 2X^2)$$

$$= 3 + 4X + 2X^2 + 2X + 5X^2 + 6X^3 + 6X^2 + X^3 + 4X^4 + X^3 + 6X^4 + 3X^5 = 3 + 6X + 6X^2 + X^3 + 3X^4 + 3X^5$$

Évaluation et *degree mantra*

Théorème
Si $F \neq 0$ est de degré d, il possède $\leq d$ racines.

$F = \sum_{i=0}^{d} f_i X^i \quad \to F(\alpha) = \sum_{i=0}^{d} f_i \alpha^i$

Preuve $d=0$: $F = f_0 \neq 0$: $F(\alpha) = f_0 \alpha^0 = f_0 \neq 0$
↳ F possède ≤ 0 racines

$d>0$ Soit F n'a pas de racine ✓
Sinon, on suppose $F(\alpha)=0$

Division Euclidienne : $F(X) = Q(X)(X-\alpha) + R(X)$ par $(X-\alpha)$
↳ $R(X) = r_0$ (1 = $\deg R < \deg(X-\alpha)$)

$0 = F(\alpha) = Q(\alpha)(\alpha-\alpha) + R(\alpha) = r_0$

$R(X) = 0$: $F(X) = Q(X) \times (X-\alpha)$ ($\deg(d-1)$)

HR : Q possède $\leq d-1$ racines
$\Rightarrow F$ en possède $\leq d$.

$F(X) = 1 + 3X + 2X^2 + 5X^3$

$F(2) = 1 + 3\times 2 + 2\times 2^2 + 5\times 2^3$
$= 1 + 6 + 1 + 5 = 6$

$H(X) = 3X^2 + 2X + 5$

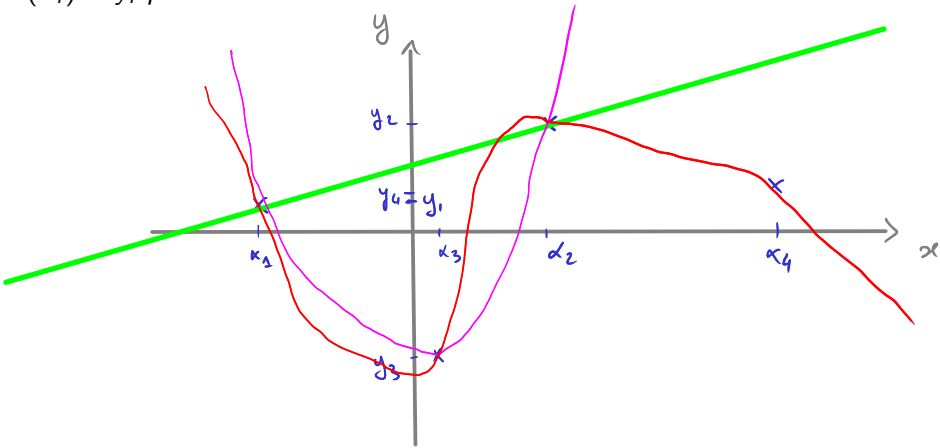
$H(6) = 3\times 6^2 + 2\times 6 + 5 = 6$
$H(2) = 3\times 2^2 + 2\times 2 + 5 = 0$

2 est racine de H | racine zéro

Interpolation

Théorème

Étant donnés $(d+1)$ *couples* (α_i, y_i), $\alpha_i \neq \alpha_j$, *il existe un unique* F *de degré* $\leq d$ *tel que* $F(\alpha_i) = y_i$ *pour tout* i.



Interpolation

(x_0, y_0) (x_1, y_1) (x_2, y_2)

$L_0 = \left(\frac{X-x_1}{x_0-x_1}\right) \times \left(\frac{X-x_2}{x_0-x_2}\right)$ $L_1 = \left(\frac{X-x_0}{x_1-x_0}\right) \times \left(\frac{X-x_2}{x_1-x_2}\right)$ $L_2 = \left(\frac{X-x_0}{x_2-x_0}\right) \times \left(\frac{X-x_1}{x_2-x_1}\right)$

Théorème

Étant donnés $(d+1)$ couples (α_i, y_i), $\alpha_i \neq \alpha_j$, il existe un unique F de degré $\leq d$ tel que $F(\alpha_i) = y_i$ pour tout i.

Unicité Supp. $\exists\, F \neq G$ tq $F(\alpha_i) = y_i$ et $G(\alpha_i) = y_i$ $\forall\, i$.

Alors $(F-G)(\alpha_i) = 0$. Or $\deg(F-G) \leq d$.

On a donc un poly $F-G$ de deg $\leq d$ qui a $(d+1)$ racines : $F-G = 0$

$\Rightarrow F = G$ ∎

Existence

$$L_i(X) = \prod_{\substack{j=0 \\ j \neq i}}^{d} \frac{X-\alpha_j}{\alpha_i-\alpha_j}$$

$\deg(L_i) \leq d$

$L_i(\alpha_j) = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}$

$$F(X) = \sum_{i=0}^{d} y_i L_i(X)$$

$\deg(F) \leq d$

$F(\alpha_j) = y_j$.

Interpolation

Théorème

Étant donnés $(d+1)$ couples (α_i, y_i), $\alpha_i \neq \alpha_j$, il existe un unique F de degré $\leq d$ tel que $F(\alpha_i) = y_i$ pour tout i.

$F(\alpha_i) = y_i \iff \sum_{j=0}^{d} f_j \alpha_i^j = y_i$

$$\begin{cases} f_0 + f_1\alpha_0 + f_2\alpha_0^2 + \dots + f_d\alpha_0^d = y_0 \\ f_0 + f_1\alpha_1 + f_2\alpha_1^2 + \dots + f_d\alpha_1^d = y_1 \\ \vdots \\ f_0 + f_1\alpha_d + f_2\alpha_d^2 + \dots + f_d\alpha_d^d = y_d \end{cases} \iff \begin{pmatrix} 1 & \alpha_0 & \cdots & \alpha_0^d \\ 1 & \alpha_1 & \cdots & \alpha_1^d \\ \vdots & & & \\ 1 & \alpha_d & \cdots & \alpha_d^d \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_d \end{pmatrix} = \begin{pmatrix} y_0 \\ \vdots \\ y_d \end{pmatrix}$$

$V \times \vec{F} = Y$

$\exists V^{-1}$ tq $V^{-1} \times V = I$

$\Rightarrow \boxed{\vec{F} = V^{-1} \times Y}$

Interpolation

Théorème

Étant donnés $(d+1)$ *couples* (α_i, y_i), $\alpha_i \neq \alpha_j$, *il existe un unique* F *de degré* $\leq d$ *tel que* $F(\alpha_i) = y_i$ *pour tout* i.

Un polynôme de degré $\leq d$ peut être défini soit par $(d+1)$ coefficients, soit par sa valeur en $(d+1)$ points.

$F(\alpha_i) = y_i$

Codes de Reed-Solomon

- Alphabet : $\mathbb{F}_q$
- $\alpha_1, \dots, \alpha_n$: éléments distincts de $\mathbb{F}_q$ ($q \geq n$)
- taille de messages k

$\mathbb{F}_7$ $(\alpha_1, \dots, \alpha_7) = (0, 1, \dots, 6)$ $\quad k = 3$

$m = (2, 4, 1) \rightarrow \Pi = 2 + 4X + X^2$

$\rightarrow RS(m) = (2, 0, 0, 2, 6, 5, 6)$

Encodage $m = (m_0, \dots, m_{k-1}) \in \mathbb{F}_q^k \rightarrow \Pi = \sum_{i=0}^{k-1} m_i X^i$

$\rightarrow RS(m) = (\Pi(\alpha_1), \Pi(\alpha_2), \dots, \Pi(\alpha_n)) \in \mathbb{F}_q^n$

$C = \{ (\Pi(\alpha_1), \dots, \Pi(\alpha_n)) : \Pi \text{ est un poly de deg} < k \}$.