Décodage des codes de Reed-Solomon

Bruno Grenet

HMIN118 – Théorie de l'information

Codes de Reed-Solomon (rappel) et décodage

Longueur n

Dimension k

Alphabet $\mathbb{F}_q$

Points évaluation $\alpha_1, \dots, \alpha_n$

$\mathbb{F}_7$, $1, 2, 3, 4, 5, 6$

Message $m \in \mathbb{F}_q^k$ $\xrightarrow{\text{interpol°}}$ Polynôme $\Pi \in \mathbb{F}_q[X]_{<k}$ $\xrightarrow{\text{évaluation}}$ Mot de code $c = (\Pi(\alpha_1), \Pi(\alpha_2), \dots, \Pi(\alpha_n))$

$(1,3,2) \in \mathbb{F}_7^3 \longrightarrow 1 + 3X + 2X^2 \longrightarrow (6,1,0,3,3,0)$

Décodage ?

→ Si on reçoit 610330 ⇝ interpolation
(si aucune erreur : on utilise k valeurs pour interpoler)

→ Si on reçoit 612310 ⇝ ? On veut trouver un poly Π tq $\Pi(1)=6$ $\Pi(2)=1$ $\Pi(3)=2$ $\Pi(4)=3$ $\Pi(5)=1$ $\Pi(6)=0$
en autorisant "quelques" erreurs

Formalisation

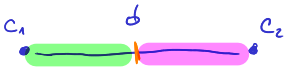
Entrées : n couples $(\alpha_1, y_1), \ldots, (\alpha_n, y_n)$ dans $\mathbb{F}_q^2$

Sortie : Polynôme F de degré $< k$ tel que $\#\{i : F(\alpha_i) \neq y_i\} < \frac{n-k+1}{2}$

Hypothèse : On suppose qu'un tel polynôme F existe !

$d = n - k + 1$

On ne peut pas décoder avec $\geq d/2$



$\alpha_1, \ldots, \alpha_n$: fixé

- On reçoit un mot $y = (y_1, \ldots, y_n)$ et on cherche
  - un mot de code $c = (c_1, \ldots, c_n)$ tq $\#\{i : y_i \neq c_i\} < \frac{n-k+1}{2}$
  - un message $m = (m_1, \ldots, m_k)$

  dt l'encodage est $y_1, \ldots, y_n$ à $< \frac{n-k+1}{2}$ erreurs près.

- Hypothèse on suppose que y est bien un mot de code avec $< \frac{n-k+1}{2}$ erreurs.

Localisateur d'erreur et équation clef

$y = 612310 \rightarrow E(X) = (X-3)(X-5)$
$= X^2 + 6X + 1$

Aussi inconnu que le message !

$$E(X) = \prod_{i:F(\alpha_i) \neq y_i} (X - \alpha_i)$$

Localisateur d'erreur et équation clef

$F(\alpha_i) = y_i$ sauf certains fois

$$E(X) = \prod_{i : F(\alpha_i) \neq y_i} (X - \alpha_i)$$

Équation clef $\qquad \forall i \qquad y_i E(\alpha_i) = F(\alpha_i) E(\alpha_i) \qquad (\star)$

- Si $F(\alpha_i) = y_i$, alors $y_i E(\alpha_i) = F(\alpha_i) E(\alpha_i)$ ✓
- Si $F(\alpha_i) \neq y_i$, alors $y_i E(\alpha_i) = 0 = F(\alpha_i) E(\alpha_i)$ ✓

Localisateur d'erreur et équation clef

$e < \frac{n-k+1}{2}$

$\Rightarrow 2e+k-1 < n$

$$E(X) = \prod_{i:F(\alpha_i)\neq y_i} (X - \alpha_i)$$

Équation clef $\quad \forall i \qquad y_i E(\alpha_i) = F(\alpha_i)E(\alpha_i) \qquad (\star)$

Première tentative

E et F sont des polynômes inconnus. Connu inconnu

$$\bar{E}(X) = \sum_{j=0}^{e} e_j X^j \qquad \bar{F}(X) = \sum_{j=0}^{k-1} f_j X^j \qquad \bar{E}(\alpha_i) = \sum_j e_j \alpha_i^j$$

$$(\star) \qquad \sum_{j=0}^{e} y_i e_j \alpha_i^j = \left(\sum_j f_j \alpha_i^j\right)\left(\sum_j e_j \alpha_i^j\right) \qquad f_j e_k \to U_{jk} \qquad (n \text{ équations})$$

→ Résolution : $e+k+1$ inconnues $< n$ éq. ⇝ NP-difficile

Linéarisation

inconnu inconnu inconnu

$$N = F \times E$$

$$y_i \quad \overline{E}(\alpha_i) = \overbrace{F(\alpha_i)\, E(\alpha_i)}^{N(\alpha_i)}$$

Linéarisation

$$N = F \times E$$

Nouvelle équation clef $\quad \forall i \qquad y_i E(\alpha_i) = N(\alpha_i) \qquad (\star\star)$

Ls satisfaite par ts les couples (α_i, y_i)

Linéarisation

deg < k

deg e

$$N = F \times E$$

Nouvelle équation clef $\quad \forall i \quad y_i E(\alpha_i) = N(\alpha_i) \quad (\star\star)$

Nouvelle tentative

$$E(x_i) = \sum_{j=0}^{e} e_j \alpha_i^j \qquad N(\alpha_i) = \sum_{j=0}^{e+k-1} n_j \alpha_i^j$$

$(\star\star)$ $\quad \sum_{j=0}^{e} y_i e_j \alpha_i^j = \sum_{j=0}^{e+k-1} n_j \alpha_i^j \rightarrow$ n équations linéaires, $2e+k$ inconnues $\Big\}$ or $\boxed{2e+k \leq n}$

$\Rightarrow$ Résolution d'un syst. linéaire à n équations et $\leq n$ inconnues

↳ $\Theta(n^3)$ avec l'algo de Gauss

Existence et unicité de la solution $(\star\star)$ $\forall i,\ y_i : E(\alpha_i) = N(\alpha_i)$

Lemme

Il existe une solution $(N^\star, E^\star)$ *à* $(\star\star)$, *avec* $\deg(N^\star) \leq e + k - 1$ *et* $\deg(E^\star) = e$, *telle que* $N^\star / E^\star = F$.

$E = \prod_{F(\alpha_i) \neq y_i} (X - \alpha_i)$ existe $\hat{m}$ si je ne le connais pas.

↳ Je pose $(N^\star, E^\star) = (\tilde{F} \times E, E)$: par déf.

$\deg(\tilde{F} \times E) \leq e + k - 1 \qquad \deg(E) = e$

e inconnu : à la place on pose $e' = \left\lceil \frac{n-k+1}{2} \right\rceil - 1$ et on pose le $\hat{m}$ syst.

A la place de E, on travaille avec $\tilde{E}'(X) = X^{e-e'} \times E(X)$

Existence et unicité de la solution

$(\star\star)$ $\forall i$ $y_i E(\alpha_i) = N(\alpha_i)$

Lemme

Il existe une solution $(N^\star, E^\star)$ *à* $(\star\star)$, *avec* $\deg(N^\star) \leq e + k - 1$ *et* $\deg(E^\star) = e$, *telle que* $N^\star / E^\star = F$.

Lemme

Si (N, E) *est solution de* $(\star\star)$, $\boxed{N/E} = F$

Supp. qu'il existe une solution $(N,E) \neq (N^\star, E^\star)$

$F = N^\star/E^\star \overset{?}{=} N/E$: $R = N^\star E - N E^\star$. On veut montrer $R = 0$

$\forall i$: $R(\alpha_i) = N^\star(\alpha_i) E(\alpha_i) - N(\alpha_i) E^\star(\alpha_i) = y_i E^\star(\alpha_i) E(\alpha_i) - y_i E(\alpha_i) E^\star(\alpha_i) = 0$

Donc R possède $\geq n$ racines. Or $\deg(R) \leq e + k - 1 < n$.

Degree matters $\Rightarrow R = 0 \Rightarrow N^\star/E^\star = N/E = F$ ∎

Résolution de ($\star\star$)

Théorème

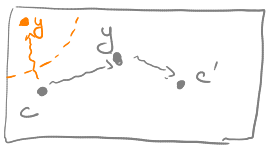
S'il existe F de degré $< k$ tel que $\#\{i : F(\alpha_i) \neq y_i\} < \frac{n-k+1}{2}$ existe, on peut le calculer en temps $O(n^3)$.

Résolution de (⋆⋆)

$\omega \leq 2{,}37\ldots$

Théorème

S'il existe F de degré $< k$ tel que $\#\{i : F(\alpha_i) \neq y_i\} < \frac{n-k+1}{2}$ on peut le calculer en temps $O(n^3)$.



Algorithme de Welch-Berlekamp

E : $(\alpha_i, y_i)_{1\leq i\leq n}$ dans $\mathbb{F}_q$, paramètre k

S : Polynôme $F \in \mathbb{F}_q[X]_{<k}$ tq $\#\{i : F(\alpha_i) \neq y_i\} < \frac{n-k+1}{2}$ s'il en existe un

$O(n^2)$ 1. Construire le syst. linéaire (⋆⋆) : $\sum_{j=0}^{e} y_i \alpha_i^j e_j - \sum_{j=0}^{e+k-1} \alpha_i^j n_j = 0$

$O(n^3)$ ou $O(n^\omega)$ 2. Résoudre le syst. pour trouver (E, N)

↳ Si le système n'a pas de solution, Renvoyer "échec"

$O(ek)$ ou $\tilde{O}(e+k)$ 3. Renvoyer N/E

$O(n)$ ↳ Si E ne divise pas N, renvoyer "échec"