Codes Correcteurs d'erreurs

Implémentation de Reed-Solomon

Dorian Lesbre

TIPE - mathématique - informatique

30 juin 2017

Notion de code correcteur

Définitions

L'alphabet : ensemble fini de symboles avec lesquels sont écrit le message. On prendra $\mathbb{F}_{q^m}$ pour alphabet.

Le message : élément de $\mathbb{F}_{q^m}^k$

L'encodeur : fonction injective $enc : \mathbb{F}_{q^m}^k \longrightarrow \mathbb{F}_{q^m}^n$

Le code : sous ensemble de $\mathbb{F}_{q^m}^n$: $\mathcal{C} = \mathrm{Im}(enc)$

Le décodeur : fonction $dec : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^k$

Étude des codes :
On cherche un code $\mathcal{C}$ optimal pour des valeurs n et k fixés.

Étude algorithmique :
Expliciter *enc* et *dec* pour pouvoir les calculer rapidement.

Codes t-correcteurs

Distance et poids

Pour $(c_1, c_2) \in (\mathbb{F}_{q^m}^n)^2$ on définit la distance de Hamming par :

$$\mathrm{d}(c_1,\, c_2) = \sum_{i=1}^{n} \left(1 - \delta(c_{1,i},\, c_{2,i})\right)$$

Le poids est la distance au mot nul : $w(c_1) = \mathrm{d}(c_1, 0)$

C'est le nombre de symboles distincts entre deux mots du code, dans $(\mathbb{F}_2)^4$, on a $\mathrm{d}(1001, 1011) = 1$.

Codes t-correcteurs

Pour $\mathcal{C}$ un code $c \in \mathcal{C}$ et t un entier, on pose :

$$\mathcal{E}(c,t) = \left\{ m \in \mathbb{F}_{q^m}^n \,/\, \mathrm{d}(c,m) \leqslant t \right\}$$

Il s'agit d'un boule centrée en c de rayon t

Codes t-correcteurs

Pour $t \in \mathbb{N}$, on dit qu'un code $\mathcal{C}$ est t-correcteur lorsque les ensembles $\left(\mathcal{E}(c,t)\right)_{c \in \mathcal{C}}$ sont deux-à-deux disjoints. Si moins de t erreurs se sont produites, il existe alors un unique mot du code le plus proche.

Distance minimale et correction

Distance minimale : Pour $\mathcal{C}$ un code, on pose :

$$d_{\min} = \min_{\substack{(c_1, c_2) \in \mathcal{C}^2 \\ c_1 \neq c_2}} \mathrm{d}(c_1, c_2)$$

Théorème

Un code $\mathcal{C}$ de distance minimale $d_{\min}$ est $\left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$-correcteur mais n'est pas $\left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor + 1$-correcteur.

Codes linéaires

Un code $\mathcal{C}$ est linéaire si $\mathcal{C}$ est un sous-espace vectoriel de $\mathbb{F}_{q^m}^n$

Distance d'un code linéaire

Pour $\mathcal{C}$ un code linéaire, on a :

$$d_{\min} = \min_{c \in \mathcal{C} \setminus \{0\}} w(c)$$

Majoration de Singleton

Tout code linéaire de paramètre (n, k) vérifie

$$d_{\min} \leqslant n - k + 1$$

Paramètres de Reed-Solomon

Alphabet : $\mathbb{F}_{q^m}$ un corps fini à q^m éléments.

Paramètres :

- n la longueur du code
- k sa dimension (longueur du message initial)
- $2t$ le nombre de symbole ajoutés

Les paramètres doivent vérifier

$$n = k + 2t = q^m - 1$$

Message : on identifie $\mathbb{F}_{q^m}^n$ à $\mathbb{F}_{q^m,\,n}[X]$ et $\mathbb{F}_{q^m}^k$ à $\mathbb{F}_{q^m,\,k}[X]$.
La liste $(a_0, \ldots, a_k)$ représente le polynôme $a_0 + a_1 X + \ldots + a_k X^k$

Code de Reed-Solomon

Polynôme générateur : il existe α un générateur de groupe cyclique $(\mathbb{F}_{q^m}^*, \times)$. On pose alors

$$G(X) = \prod_{i=1}^{2t} (X - \alpha^i)$$

Code de Reed-Solomon

Le code de Reed-Solomon est l'ensemble des multiples de G :

$$\mathcal{C} = G\mathbb{F}_{q^m,k}[X] = \left\{ G(X)P(X),\ P \in \mathbb{F}_{q^m,k}[X] \right\}$$

Propriétés du code de Reed-Solomon

Propriétés

Le code $\mathcal{C}$ de Reed-Solomon ainsi défini vérifie :

- $\mathcal{C}$ est un code linéaire.
- $d_{\min}(\mathcal{C}) = 2t + 1$ donc $\mathcal{C}$ est t-correcteur.

$\mathcal{C}$ atteint la majoration de Singleton.

Principe de la démonstration : soit $c = \sum_{\ell=1}^{2t} c_{i_\ell} X^{i_\ell} \in \mathcal{C}$ tel que $w(c) \leqslant 2t$. Les $(\alpha^i)_{i \in [\![1, 2t]\!]}$ étant racines de c, on a le système

$$\begin{bmatrix} (\alpha^{i_1})^1 & \cdots & (\alpha^{i_{2t}})^1 \\ \vdots & \ddots & \vdots \\ (\alpha^{i_1})^{2t} & \cdots & (\alpha^{i_{2t}})^{2t} \end{bmatrix} \cdot \begin{bmatrix} c_{i_1} \\ \vdots \\ c_{i_{2t}} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Encodeur

On veut transformer $A \in \mathbb{F}_{q^m,k}[X]$ en multiple de G de degré inférieur à n

Encodeur

1 | $G \leftarrow \prod_{i=1}^{p}(X - \alpha^i)$

2 | $T \leftarrow A * X^p$

3 | $B \leftarrow$ reste de la division de T par G

4 | **renvoie** $T - B$

Ainsi $(a_0, \ldots, a_k)$ devient après codage $(\underbrace{m_1, \ldots, m_{2t}}_{\text{symboles ajoutés}}, \underbrace{a_0, \ldots, a_k}_{\text{message}})$

Correction d'erreur

On suppose que moins de t erreurs se sont produites. Le message reçu s'écrit $D = C + E$ avec E le polynôme d'erreur :

$$E = \sum_{\ell=1}^{v} e_{i_\ell} X^{i_\ell}$$

Inconnues :

- le nombre d'erreur v $(1 \leqslant v \leqslant t)$
- les positions d'erreurs $(i_1, \ldots, i_v)$
- les valeurs d'erreurs $(e_{i_1}, \ldots, e_{i_v})$

Pour $\ell \in [\![1,\ 2t]\!]$ on a $D(\alpha^\ell) = C(\alpha^\ell) + E(\alpha^\ell) = E(\alpha^\ell)$
On connait donc $2t$ valeurs prises par E.

Déterminer les positions d'erreur

Définissons les polynômes :

- $S(X) = \sum_{\ell=1}^{2t} D(\alpha^\ell) X^\ell$
- $\Lambda(X) = \prod_{\ell=1}^{v} (1 - \alpha^{i_\ell} X)$
- $\Omega(X) = \sum_{\ell=1}^{v} e_{i_\ell} \alpha^{i_\ell} \prod_{h=1,\, h \neq k}^{v} (1 - \alpha^{i_h} X)$

Équation-clé

Ces polynômes vérifient :

$$\Lambda S \equiv \Omega \ [X^{2t}]$$

Résolution de l'équation clé

Proposition

Pour tout $(A, B) \in \mathbb{F}_{q^m}[X]$, on a

$$\begin{cases} \deg(A) \leqslant t \text{ et } \deg(B) < t \\ AS \equiv B \ [X^{2t}] \end{cases} \Rightarrow \exists C \in \mathbb{F}_{q^m}[X], \begin{cases} A = C\Lambda \\ B = C\Omega \end{cases}$$

Algorithme d'Euclide étendu

Permet de calculer trois suites finies :

- (P_ℓ) : $P_0 = X^{2t}$ et $P_1 = S$ puis $P_{\ell+1} = P_{\ell-1} - P_\ell Q_\ell$ tant que $P_\ell \neq 0$
- (U_ℓ) et (V_ℓ) tel que $P_\ell = U_\ell P_0 + V_\ell P_1$

On a $\deg(V_\ell) \leqslant \deg(P_0) - \deg(P_{\ell-1})$

Calcul de Λ et Ω

Algorithme d'Euclide

```
1  | P0 ← polynôme X^{2t} de F_{q^m}[X]
2  | P1 ← S
3  | V0 ← polynôme 0 de F_{q^m}[X]
4  | V1 ← polynôme 1 de F_{q^m}[X]
5  | Tant que degre(P1) > t faire
6  |     Q, R ← divise(P0, P1)
7  |     P0, P1 ← P1, R
8  |     V0, V1 ← V1, V0 − Q*V1
9  | C ← 1_{F_{q^m}} / V1(0)
10 | renvoie V1*C, P1*C
```

Déterminer les valeurs et positions d'erreurs

On connait désormais

$$\Lambda(X) = \prod_{\ell=1}^{v}(1 - \alpha^{i_\ell} X) \quad \text{et} \quad \Omega(X) = \sum_{\ell=1}^{v} e_{i_\ell} \alpha^{i_\ell} \prod_{h=1,\, h\neq k}^{v} (1 - \alpha^{i_h} X)$$

Détermination des inconnues

On peut alors déterminer le polynôme E à partir de Λ et Ω :

- v correspond au nombre de racines de Λ donc $v = \deg(\Lambda)$
- les racines de Λ sont les $(\alpha^{-i_\ell})_{\ell \in [\![1,\, v]\!]}$.
- les $(e_{i_\ell})_{\ell \in [\![1,\, v]\!]}$, sont donnés par la formule de Forney :

$$\frac{\Omega(\alpha^{-i_\ell})}{\Lambda'(\alpha^{-i_\ell})} = -e_{i_\ell}$$

Un mot sur la correction d'effacements

Problème : D possède jusqu'à $2t$ bits inconnus, de position connu

Vue matricielle : il existe $G \in \mathcal{M}_{n,k}(\mathbb{F}_{q^m})$ telle que $enc = A \mapsto GA$

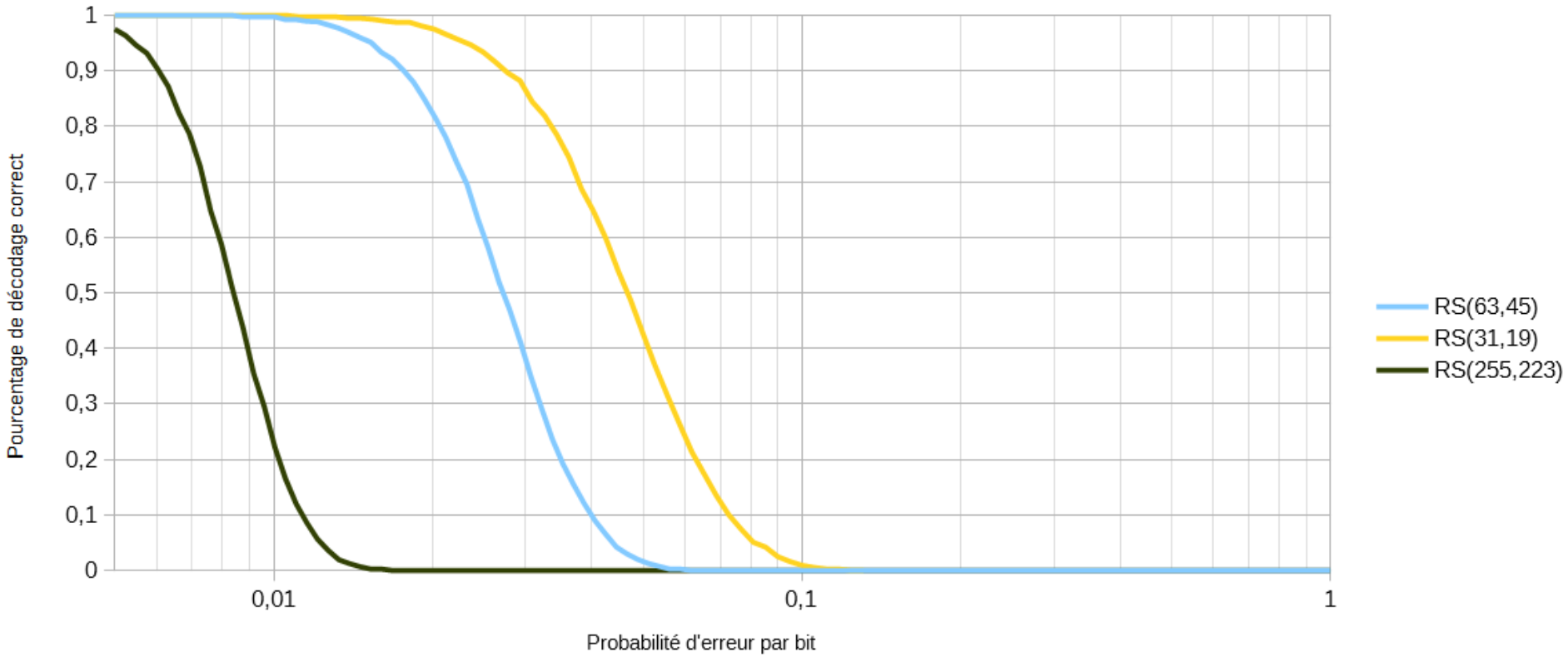
Résolution

Poser $G' \in \mathcal{M}_{k,k}(\mathbb{K})$ et D' extraites de A et D en supprimant les lignes des bits inconnus.
G' est inversible donc on a directement

$$A = G'^{-1} D'$$

Démonstration : si G' non-inversible, on contredit la propriété de distance minimale.

Résultat de la correction



Pourcentage de correction en fonction de la probabilité d'erreur

Démonstration de l'équation clé

$$S(X) = \sum_{k=1}^{2t} D(\alpha^k) X^{k-1} = \sum_{k=1}^{2t} \sum_{h=1}^{v} e_{i_h} \alpha^{k i_h} X^{k-1} = \sum_{h=1}^{v} e_{i_h} \alpha^{i_h} \left(\sum_{k=1}^{2t} (\alpha^{i_h} X)^{k-1} \right)$$

$$= \sum_{h=1}^{v} e_{i_h} \alpha^{i_h} \frac{1 - (\alpha^{i_h} X)^{2t+1}}{1 - \alpha^{i_h} X}$$

$$\Lambda(X) S(X) = \sum_{h=1}^{v} e_{i_h} a^{i_h} (1 - (\alpha^{i_h} X)^{2t+1}) \prod_{k=1,\, k \neq h}^{v} (1 - \alpha^{i_k} X)$$

$$= \sum_{h=1}^{v} \left(e_{i_h} \alpha^{i_h} \prod_{k=1,\, k \neq h}^{v} (1 - \alpha^{i_k} X) \right) - X^{2t+1} \times \ldots$$

$$\equiv \Omega(X) \; [X^{2t}]$$

Démonstration de la Formule de Forney

$$\frac{\Omega(\alpha^{-i_k})}{\Lambda'(\alpha^{-i_k})} = \frac{\sum_{h=1}^{v} e_{i_h}\alpha^{i_h} \prod_{j=1, j\neq h}^{v}(1-\alpha^{i_j}\alpha^{-i_k})}{\sum_{k=1}^{v} -\alpha^{i_h} \prod_{j=1, j\neq h}^{v}(1-\alpha^{i_j}\alpha^{-i_k})} = \frac{e_{i_k}\alpha^{i_k} \prod_{h=1, h\neq k}^{v}(1-\alpha^{i_h}\alpha^{-i_k})}{-\alpha^{i_k} \prod_{h=1, h\neq k}^{v}(1-\alpha^{i_h}\alpha^{-i_k})}$$

$$\frac{\Omega(\alpha^{-i_k})}{\Lambda'(\alpha^{-i_k})} = \frac{e_{i_k}\alpha^{i_k}}{-\alpha^{i_k}} = -e_{i_k}$$