Un autre décodage des Codes de Reed-Solomon

Ronan Quarez

February 15, 2006

1 Introduction

Une information m qui transite par une ligne de communication moderne est une liste de 0 et de 1 codés par une différence de potentiel. Or, au cours de la transmission, il peut par exemple se produire des sautes de tension. Ainsi certains symboles peuvent être altérés. Le problème qui se pose est alors de corriger ces erreurs pour reconstituer m. C'est là qu'interviennent les codes correcteurs d'erreurs.

On considère d'abord que l'information m est constituée d'une suite de blocs (n-uplets) de symboles appartenant à un alphabet fixé $\mathcal{A}$. Il est vrai qu'en pratique, l'aphabet binaire $\mathcal{A} = \{0, 1\}$ est intensement utilisé. Mais ce n'est pas le seul, et dans la suite nous considèrerons que $\mathcal{A} = \mathbb{F}_q$ le corps à q éléments, où $q = p^r$ avec p un nombre premier et r un entier naturel non nul. On traite alors les blocs d'information de m l'un après l'autre.

On commence alors par ajouter, à chaque bloc de m, un certain nombre de symboles pour obtenir un message c. C'est cette redondance qui permet de corriger les erreurs : plus on rajoute de symboles et plus on peut corriger d'erreurs. Encore faut-il ne pas les ajouter n'importe comment, toutes les redondances ne conduisant pas à la même capacité de correction.

On considère, après ajout de la redondance que les blocs obtenus sont de taille n, i.e. ce sont des n-uplets d'éléments de $\mathcal{A} = \mathbb{F}_q$. L'ensembles des blocs obtenus de la sorte constitue le code qui est dorénavant vu comme un sous-ensemble C de $\mathbb{F}_q^n$.

Les différentes étapes du procédés sont représentés sur le diagramme ci-dessous :

$$m \xrightarrow{\text{redondance}} \boxed{\text{c}} \xrightarrow{\text{transmission}} \boxed{\text{c'}} \xrightarrow{\text{decodage}} \boxed{\text{c}} \xrightarrow{\text{troncature}} m$$

On dit qu'un code C est linéaire lorsque c'est un sous-espace vectoriel de $\mathbb{F}_q^n$. On note alors $[n, k, d]$ ses paramètres : n est la longueur, k la dimension et d le poids minimal d'un mot non nul de C défini comme suit.

Le poids de $(a_1, \dots a_n)$ est le cardinal de l'ensemble des indices i tels que $a_i \neq 0$.

On parle aussi pour d, de distance minimale, i.e. elle peut s'interpréter comme la distance minimale entre deux mots du code C.

Si on suppose, pour simplifier, que $d = 2e + 1$, alors, lorsqu'on altère un mot c du code C en un nombre e de coordonnées, on obtient un n-uplet c' à distance e de c. Par ailleurs, il existe un et un seul n-uplet du code (en l'occurence c !) à distance au plus e de c'.

Plus grande est la distance minimale et plus grande est la capacité de correction du code :

Proposition 1.1 *Dès que $e \leq \frac{d-1}{2}$, il est possible de corriger e erreurs.*

Il convient de noter que la proposition précédente ne donne aucun moyen pratique, i.e. aucun algorithme performant, pour décoder. Le décodage efficace est un problème essentiel de la théorie des codes correcteurs. Une classe de codes correcteurs sera d'autant plus intéressante qu'elle possède de bons paramètres (une bonne capacité de correction), et un algorithme de décodage efficace.

On considère, dans la suite, la classe des codes dits de Reed-Solomon, et on décrit une méthode pour les décoder, due à l'origine à Welch et Berlekamp.

2 Les codes de Reed-Solomon

On note $\mathbb{F}_q[X]_s$ le $\mathbb{F}_q$-espace vectoriel des polynômes univariés à coefficients dans $\mathbb{F}_q$ et de degré inférieur ou égal à s. On écrit $\{a_1, \ldots, a_q\}$ les éléments de $\mathbb{F}_q$ ordonnés arbitrairement.

Puis, on considère l'application d'évaluation $\phi : \mathbb{F}_q[X] \to \mathbb{F}_q^q$ qui envoit un polynôme P sur le q-uplet $(P(a_1), \ldots, P(a_q))$.

On note $C = C(k, q)$ l'image par ϕ de $\mathbb{F}_q[X]_{k-1}$ où $k \leq q$. Notons alors que la longueur n du code C est égale à q la taille de l'alphabet $\mathbb{F}_q$. Les codes ainsi obtenus lorsqu'on fait varier q et k sont dits codes de Reed-Solomon.

Proposition 2.1 *Le code $C(k, q)$ est un code linéaire sur $\mathbb{F}_q$ dont les paramètres $[n, k, d]$ vérifient $n + 1 = k + d$.*

On s'intéresse dorénavant au problème du décodage de tels codes.

Ainsi, on part d'un mot c de $C = C(k, q)$, qu'on écrit $(P(a_1), \ldots, P(a_n))$, et on suppose qu'au cours de la transmission, il se produit e erreurs, à savoir qu'exactement e coordonnées du n-uplet sont altérées.

Ainsi, on reçoit le n-uplet c' et le problème est alors de reconstituer c.

3 Interpolation d'un sous-ensemble fini du plan par une fonction algébrique

Nous donnons deux techniques différentes d'interpolations dont chacune conduira à une méthode de décodage des codes de Reed-Solomon.

3.1 Interpolation par une fraction rationnelle

Soit la donnée de n-points du plan affine $\mathbb{F}_q^2$: $(x_i, y_i)_{1 \leq i \leq n}$.

On dit qu'un polynôme $R \in \mathbb{F}_q[X]$ ne coincide pas avec la donnée en au plus t points, lorsque $R(x_i) = y_i$ pour au moins $n - t$ indices $i \in \{1, \ldots, n\}$.

Proposition 3.1 *Soit $e \leq n$. On suppose qu'il existe un polynôme qui ne coincide pas avec la donnée précédente en au plus e points. Alors:*

1) Il existe deux polynômes N et D de $\mathbb{F}_q[X]$, avec N unitaire tel que $\deg N \leq k-1+e$ et $\deg D = e$ tels que, pour tout $i \in \{1,\ldots,n\}$, on ait $N(x_i) = y_i D(x_i)$.

2) On peut trouver un tel couple (N,D) en un temps polynômial en fonction de la taille des données.

3) Un tel couple est unique dès que $e \leq \frac{1}{2}(n-k)$.

L'idée de Welch et Berlekamp consiste à appliquer ce résultat, à la donnée $(a_i, c'_i)_{1\leq i\leq n}$ où l'on rappelle que $\{a_1,\ldots,a_n\} = \mathbb{F}_q$ et que $c' = (c'_1,\ldots,c'_n)$ est le n-uplet reçu après transmission.

Il suffit alors de noter que la donnée a bien été obtenue en altérant e couples de la donnée $(a_i, P(a_i))_{1\leq i\leq n}$ où P est le polynôme de $\mathbb{F}_q[X]_{k-1}$ associé au mot du code de départ : $c = (P(a_1),\ldots,P(a_n))$.

Corollaire 3.2 *Dès que $e \leq \frac{1}{2}(n-k)$, on dispose d'un algorithme pratique pour décoder c' en c .*

3.2 Interpolation par une courbe algébrique plane

Soit encore n-points du plan affine $\mathbb{F}_q^2$: $(x_i, y_i)_{1\leq i\leq n}$.

On considère cette fois un polynôme $R \in \mathbb{F}_q[X,Y]$ qui coincide partout sur la donnée, i.e. tel que $R(x_i, y_i) = 0$ pour tout indice $i \in \{1,\ldots,n\}$.

Proposition 3.3 *1) Il existe un polynôme $Q \in \mathbb{F}_q[X,Y]$, tel que $\max(\deg_X Q, \deg_Y Q) \leq \lceil \sqrt{n} \rceil$ et $Q(x_i, y_i) = 0$ pour tout $i \in \{1,\ldots,n\}$.*

2) De plus, Q peut s'obtenir en temps polynômial en la taille des données.

3) Si par ailleurs $e < n - (1+k)\lceil \sqrt{n} \rceil$, alors $Y - P(X)$ est un facteur du polynôme $Q(X,Y)$.

Dorénavant on fixe un tel polynôme solution Q.

Une fois encore, on applique alors le résultat précédent à la donnée $(a_i, c'_i)_{1\leq i\leq n}$, qui a été obtenue en altérant e couples de la donnée $(a_i, P(a_i))_{1\leq i\leq n}$ où $c = (P(a_1),\ldots,P(a_n))$.

Sous les hypothèses de 3.3, on "retrouve" alors P, et donc le n-uplet c.

A la base de cette réactualisaton de l'idée de Welch et Berlekamp, on trouve Ar, Lipton, Rubenfield et Sudan.

Pour cette deuxième approche, nous sommes donc amenés, pour décoder c', à factoriser Q dans $\mathbb{F}_q[X,Y]$.

4 Factorisation bivariée

Pour factoriser un polynôme dans $\mathbb{F}_q[X,Y]$, il est naturel de d'abord savoir factoriser dans $\mathbb{F}_q[X]$. L'algorithme de Berlekamp permet de satisfaire ce premier point.

4.1 Algorithme de Berlekamp

Soit $P \in \mathbb{F}_q[X]$ qu'on suppose sans facteur carré de degré d. On considère l'algèbre $B = \mathbb{F}_q[X]/(P)$ et l'endomorphisme $\tau : z \mapsto z^q$ dont on peut calculer la matrice dans la base canonique par exemple.

Théoreme 4.1 *1) La dimension de* Ker $(\tau - I)$ *est égale au nombre de facteurs irréductibles de P.*

2) Si $S \in \mathbb{F}_q[X]$ est un représentant non constant et de degré $< d$ d'un élément de $\in$ Ker $(\tau - I)$*, alors l'un au moins des polynômes* pgcd $((S - a_i), P)$*, pour $i \in \{1, \ldots, q\}$, fournit un facteur non trivial de P.*

Voyons maintenant, pour le problème de factorisation bivariée qui nous intéresse, deux manières de se ramener à la situation univariée.

4.2 "A la Kronecker"

On pose $D = \max(\deg_X Q, \deg_Y Q)+1$ et on utilise le morphisme de $\mathbb{F}_q[X]$-algèbre $\phi : \mathbb{F}_q[X, Y] \to \mathbb{F}_q[X]$ tel que $\phi(Y) = X^D$.

En factorisant $\phi(Q)$ dans $\mathbb{F}_q[X]$ par l'algorithme de Berlekamp, on alors peut déduire la factorisation de Q dans $\mathbb{F}_q[X, Y]$. En effet : si $\phi(Q) = Q_1 \times \ldots Q_r$, alors tout facteur non trivial F de Q vérifie $\phi(F) = Q_1^{\epsilon_1} \times \ldots Q_r^{\epsilon_r}$ avec $(\epsilon_1, \ldots, \epsilon_r) \in \{0, 1\}^r$ différent de $(0, \ldots, 0)$ et $(1, \ldots, 1)$.

4.3 "A la Hensel"

On suppose que F est unitaire en X et que $F(X, 0)$ est sans facteur carré. Cette fois-ci les morphismes considérés sont les $\psi_k : \mathbb{F}_q[X, Y]/(Y^{k+1}) \to \mathbb{F}_q[X, Y]/(Y^k)$ avec $k \in \mathbb{N}$. On commence alors par trouver la décomposition de $F(X, 0)$ en produit d'irréductibles de $\mathbb{F}_q[X]$. Puis on relève successivement grâce au Lemme de Hensel.

Théoreme 4.2 *Soient $F, G, H \in \mathbb{F}_q[X, Y]$ unitaires en Y. Supposons que F* mod Y *est sans facteur carré. Soit $k \in \mathbb{N}$ tel que $F \equiv GH$* mod Y^k*. Alors, il existe deux polynômes $\overline{G}, \overline{H}$ unitaires en X, tels que $\overline{G} \equiv G$* mod Y^k*, $\overline{H} \equiv H$* mod Y^k *et $F \equiv \overline{G}\overline{H}$* mod Y^{k+1}*. De plus, $\overline{G}, \overline{H}$ sont uniquement déterminés modulo Y^{k+1}.*

D'où au bout du compte, en procédant comme au paragraphe 4.2, on obtient la factorisation de F dans $\mathbb{F}_q[X, Y]$.

5 Travail demandé au candidat

1) Démonstrations :

   On s'attachera à démontrer quelques-unes des propriétés du texte.

2) Algorithme(s) de décodage

   – Comparer les deux méthodes d'interpolations des paragraphes 3.1 et 3.2, et leurs applications au décodage.

   On interprétera notamment le passage du paragraphe 3.2 : on "retrouve" alors P.

- Sur la factorisation bivariée.
  a) Est-ce que les facteurs irréductibles de $\phi(F)$ se relèvent en des facteurs irréductibles de F ?
  b) Expliquer comment simplifier la méthode de factorisation bivariée dans le cas particulier de l'application au décodage des codes de Reed-Solomon.
  c) Expliquer pourquoi l'algorithme utilisé tel quel pourrait ne pas être forcément polynomial en la taille des données.

3) Paramètres des codes

- Dans le cas où $n = 101$ (pour fixer les idées), sur un graphe où l'on portera $\frac{d}{n}$ en abscisses et $\frac{k}{n}$ en ordonnées, représenter :
  i) les points associés aux paramètres possibles des codes de Reed-Solomon.
  ii) La capacité théorique de correction $\frac{e}{n}$ ainsi que celle proposée par les deux méthodes d'interpolation.
- Donner un sens au concept de corriger "au-delà" de la capacité maximale de correction. Mettre en oeuvre sur des exemples...