Codes de Goppa

Préparation à l'agrégation - option Calcul formel

Antoine Chambert-Loir

Mots clefs. — Codes correcteurs, corps finis, interpolation, algorithme d'Euclide.

1. Introduction

Soit $\mathbf{F}$ un corps fini dont on note q le cardinal. Un *code linéaire* de type $[n, k, d]$ sur $\mathbf{F}$ n'est rien d'autre qu'un sous-espace vectoriel C de dimension k de l'espace $\mathbf{F}^n$ dont la distance minimale est égale à d : pour tout $\mathbf{x} = (x_1, \dots, x_n) \in C \setminus \{0\}$,

$$w(\mathbf{x}) := \#\{i \in \{1, \dots, n\} \quad ; \quad x_i \neq 0\} \geqslant d,$$

l'inégalité étant une égalité pour au moins un élément de $C \setminus \{0\}$. La fonction w sur $\mathbf{F}^n$ définie par la formule précédente est appelée *poids de Hamming* ; l'application $(\mathbf{x}, \mathbf{y}) \mapsto w(\mathbf{x} - \mathbf{y})$ est une distance sur $\mathbf{F}^n$, appelée *distance de Hamming*.

Étant donné un tel code C, le codage et le décodage obéissent à la problématique suivante.

Codage. — Le message à envoyer est écrit sous forme d'une suite $\mathbf{x}_1, \mathbf{x}_2, \dots$ d'éléments de $\mathbf{F}^k$; chacun de ces éléments est transformé en un élément de $\mathbf{F}^n$ au moyen d'une application linéaire $\gamma\colon \mathbf{F}^k \to \mathbf{F}^n$ dont l'image est C ; c'est la suite image $\gamma(\mathbf{x}_1), \gamma(\mathbf{x}_2), \dots$ qui est diffusée.

Décodage. — Compte tenu des erreurs de transmission (bruit électromagnétique, etc.), le destinataire reçoit une suite $\mathbf{y}_1, \mathbf{y}_2, \dots$, éventuellement distincte de la suite voulue ; il s'agit de remplacer chaque $\mathbf{y}_i$ par l'élément de C le plus approprié. Soit donc $\mathbf{y}$ un élément de $\mathbf{F}^n$; s'il est obtenu à partir d'un élément $\mathbf{y}'$ de C avec modification d'au plus c coordonnées, on a $w(\mathbf{y} - \mathbf{y}') \leqslant c$; si de plus $2c + 1 \leqslant d$, il y a au plus un tel $\mathbf{y}'$. Si on peut le trouver, on récupère le mot $\mathbf{x} \in \mathbf{F}^k$ initial en lui appliquant l'application linéaire $\delta\colon C \to \mathbf{F}^k$ inverse de γ.

Matrice de parité. — Étant donné un code C de longueur n et de dimension k, une matrice de parité H est une matrice $(n - k) \times n$ dont le noyau (dans $\mathbf{F}^n$) est égal à C.

Syndrome. — Avec les notations précédentes, le vecteur $\mathbf{y} - \mathbf{y}'$ est appelé *vecteur d'erreur*. Les vecteurs d'erreurs possibles sont l'ensemble $\mathbf{y} + C$; pour retrouver $\mathbf{y}'$, il est nécessaire de déterminer ceux de poids minimal, si possible efficacement. On appelle *syndrome* de $\mathbf{y}$ le vecteur $\sigma(\mathbf{y}) = H\mathbf{y}$, où H est une matrice de parité fixée pour C. On a $\sigma(\mathbf{y}) = 0$ si et seulement si $\mathbf{y} \in C$; en fait, $\mathbf{y}$ étant donné, tous les

---

25 janvier 2007.

vecteurs d'erreurs possibles fournissent le même syndrome, et inversement. Une fois le syndrome calculé, le décodage consiste donc à déterminer les vecteurs d'erreurs de poids minimal qui produisent ce syndrome.

2. Codes de Goppa

Pour définir un tel code, les données sont les suivantes :

– un corps $\mathbf{F}'$ à $q' = q^m$ éléments (donc « contenant » $\mathbf{F}$) ;
– un polynôme $G \in \mathbf{F}'[X]$;
– une partie $L = \{z_1, \dots, z_n\}$ de $\mathbf{F}'$ sur laquelle G ne s'annule pas.

Le code $C = \Gamma(L, G)$ est l'ensemble des vecteurs $\mathbf{a} = (a_1, \dots, a_n) \in \mathbf{F}^n$ tels que la fraction rationnelle

$$R_{\mathbf{a}}(X) = \sum_{i=1}^{n} \frac{a_i}{X - z_i} \tag{2.1}$$

ait un numérateur multiple de $G(X)$. La longueur de ce code est n ; si $r = \deg G$, on peut démontrer que sa dimension k et sa distance minimale d vérifient $k \geqslant n - mr$ et $d \geqslant r + 1$.

Soit C' l'ensemble des vecteurs $\mathbf{a} \in (\mathbf{F}')^n$ pour lesquels le numérateur de $R_{\mathbf{a}}(X)$ est multiple de $G(X)$; on a donc $C = C' \cap (\mathbf{F})^n$. En outre, C' est un code linéaire sur $(\mathbf{F}')^n$ dont on peut assez facilement écrire une matrice de parité. Comme G ne s'annule pas en z_i, le polynôme $X - z_i$ est inversible modulo G ; il existe donc un unique polynôme $f_i(X)$ de degré $< r$ tel que $(X - z_i)f_i(X) \equiv 1 \pmod{G(X)}$ et la condition pour $\mathbf{a} \in (\mathbf{F}')^n$ d'appartenir à C' est simplement

$$\sum_{i=1}^{n} a_i f_i(X) = 0 \quad ; \tag{2.2}$$

autrement dit, en regardant ce que cela donne pour chaque coefficient, r équations linéaires à coefficients dans $\mathbf{F}'$. Ces équations sont linéairement indépendantes sur $\mathbf{F}'$. On peut obtenir une matrice de parité pour le code C en choisissant une base de $\mathbf{F}'$ sur $\mathbf{F}$ et en récrivant chacune de ces équations comme m équations linéaires à coefficients dans $\mathbf{F}$, mais les équations obtenues ne sont plus forcément linéairement indépendantes.

Donnons un exemple. Prenons $\mathbf{F} = \mathbf{F}_2$, $G(X) = X^2 + X + 1$, $\mathbf{F}' = \mathbf{F}_8$ et $L = \mathbf{F}' = \{0, 1, \omega, \omega^2, \dots, \omega^6\}$, où ω est un générateur du groupe multiplicatif de $\mathbf{F}'$. On a donc $q = 2$, $m = 3$, $r = 2$ et $n = 8$. On énumère les élements de L en posant $z_1 = 0$ et $z_i = \omega^{i-2}$ pour $2 \leqslant i \leqslant 8$. Pour tout i, on a la formule (générale)

$$f_i(X) = -\frac{G(X) - G(z_i)}{X - z_i} G(z_i)^{-1},$$

ce qui donne ici

$$f_i(X) = -\frac{1}{G(z_i)}(X + z_i + 1).$$

La matrice

$$H' = \begin{pmatrix} \frac{1}{G(0)} & \frac{1}{G(1)} & \cdots & \frac{1}{G(\omega^6)} \\ \frac{0}{G(0)} & \frac{1}{G(1)} & \cdots & \frac{\omega^6}{G(\omega^6)} \end{pmatrix}$$

est donc une matrice de parité pour le code C'. Elle est bien de rang 2. Pour obtenir une matrice de parité pour le code C, il faut se rappeler que $(1, \omega, \omega^2)$ est une base de $\mathbf{F}'$ sur $\mathbf{F}$, donc ω est annulé par un polynôme irréductible de degré 3 à coefficients dans $\mathbf{F}$; on suppose qu'il s'agit du polynôme $t^3 + t + 1$. On a alors, par exemple

$$\frac{1}{G(\omega)} = \frac{1}{\omega^2 + \omega + 1} = \frac{1}{\omega^2 + \omega^3} = \frac{1}{\omega^2(\omega + 1)} = \frac{1}{\omega^5} = \omega,$$

et l'on peut ainsi obtenir la matrice de parité

$$H' = \begin{pmatrix} 1 & 1 & \omega^2 & \omega^2 + \omega & \omega^2 & \omega & \omega & \omega^2 + \omega \\ 0 & 1 & \omega + 1 & \omega^2 + 1 & \omega^2 + \omega + 1 & \omega^2 + \omega + 1 & \omega^2 + 1 & \omega + 1 \end{pmatrix},$$

puis en déduire

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

3. Retour sur l'algorithme d'Euclide

Soit A et B des polynômes à coefficients dans un corps K. On note $r = \deg(A)$ et on suppose $r > \deg(B)$. On s'intéresse aux couples de polynômes non nuls (P, Q) tels que $BP \equiv Q \pmod{A}$, où le degrés de P et Q sont les plus petits possibles. On va chercher des solutions avec $\deg(P) \leqslant \frac{1}{2}r$ et $\deg(Q) < \frac{1}{2}r$. Observons d'abord que si cette relation est vérifiée, Q est multiple du pgcd D de A et B ; une condition nécessaire à l'existence d'un tel couple (P, Q) est que le degré de D vérifie $\deg(D) < \frac{1}{2}r$.

On remarque ensuite qu'un tel couple est unique à multiplication par un scalaire près. Si (P, Q) et (P_1, Q_1) en sont deux, on a en effet $QP_1 - PQ_1 \equiv 0 \pmod{A}$, mais le polynôme de gauche est de degré au plus $r - 1$, donc est nul.

Pour déterminer explicitement un tel couple, nous allons utiliser l'algorithme d'Euclide.

Appliquons en effet l'algorithme d'Euclide étendu aux polynômes A et B. On obtient donc trois suites $(A_0, A_1, A_2, \ldots, A_n = 1)$, $(U_0, \ldots, U_n)$, $(V_0, \ldots, V_n)$ de polynômes de $K[X]$, avec $(A_0, A_1) = (A, B)$, $(U_0, U_1) = (1, 0)$, $(V_0, V_1) = (0, 1)$ et où, notant q_{k+2} le quotient de la division euclidienne de A_k par A_{k+1}, $(A_{k+2}, U_{k+2}, V_{k+2}) = (A_k, U_k, V_k) - (A_{k+1}, U_{k+1}, V_{k+1})q_{k+2}$. On a aussi $A_k = AU_k + BV_k$ pour tout k ; en particulier $BV_k \equiv A_k \pmod{A}$. Soit s le plus petit entier tel que

$$\deg(A_{s-1}) \geqslant \frac{1}{2}r > \deg(A_s).$$

Un tel entier existe puisque le pgcd de A et B est supposé être de degré $< \frac{1}{2}r$. Montrons qu'un couple minimal (P, Q) est donné par $P = V_s$ et $Q = A_s$.

On a déjà $\deg(A_s) < \frac{1}{2}r$. Montrons que $\deg(V_s) < \frac{1}{2}r$. Supposons $\deg(A) > \deg(B)$; par récurrence, on a, pour $k \geqslant 2$

$$\deg(U_k) = \deg(q_3) + \cdots + \deg(q_k) = \deg(A_1) - \deg(A_{k-1})$$
$$\deg(V_k) = \deg(q_2) + \cdots + \deg(q_k) = \deg(A_0) - \deg(A_{k-1}).$$

En particulier, $\deg(V_s) < \frac{1}{2}r$.

4. Décodage

On suppose avoir reçu un vecteur $\mathbf{a} = (a_1, \ldots, a_n)$ de $\mathbf{F}^n$ et on cherche à retrouver le mot $\widehat{\mathbf{a}}$ du code C qui lui correspond, sous l'hypothèse qu'il n'y a eu $< \frac{1}{2}r$ erreurs de transmission.

Pour tout i, soit $f_i(T)$ le polynôme de degré $< r$ tel que $1 \equiv f_i(T)(T - z_i) \pmod{G(T)}$. Le syndrome de $\mathbf{a}$ est le polynôme $S(T) = \sum_{i=1}^{n} a_i f_i(T)$. C'est aussi celui du vecteur d'erreur $\varepsilon = \mathbf{a} - \widehat{\mathbf{a}}$.

Soit $I \subset \{1, \ldots, n\}$ l'ensemble des indices où $\widehat{a}_i \neq \widehat{a}_i$. On suppose qu'il y a eu strictement moins de $\frac{1}{2}r$ erreurs, c'est-à-dire que $\mathrm{Card}(I) < \frac{1}{2}r$, et on veut les corriger. On définit des polynômes $\sigma(T)$ et $\omega(T)$ par les formules

$$\sigma(T) = \prod_{i \in I}(T - z_i), \qquad \omega(T) = \sum_{i \in I} \varepsilon_i \prod_{\substack{j \in I \\ j \neq i}} (T - z_j).$$

On a la congruence $S(T)\sigma(T) \equiv \omega(T) \pmod{G(T)}$. Par suite, les polynômes σ et ω peuvent être obtenus à l'aide de la méthode décrite au paragraphe précédent.

Pour terminer le décodage, il faut vérifier que σ est bien de la forme $\prod_{i \in I}(T - z_i)$ pour une partie I de $\{1, \ldots, n\}$ à déterminer explicitement, puis calculer les coefficients ε_i.

5. Suggestions

(1) Étant donnée une matrice de parité H pour un code C, expliquer comment trouver un homomorphisme $\gamma\colon \mathbf{F}^k \to \mathbf{F}^n$ d'image C. Pouvez-vous trouver un tel homomorphisme pour lequel les k coordonnées du vecteur de départ soit simplement recopiées (par exemple en les k premières coordonnées du vecteur d'arrivée) ?

(2) Démontrer que le système d'équations (2.2) est de rang r, autrement dit, que C' est un code linéaire sur $\mathbf{F}'$ de dimension $n - r$. (Écrire la matrice H' de ce système comme un produit de la matrice de Vandermonde $r \times n$ (z_j^{i-1}) et de matrices triangulaires convenables).

(3) Soit $x_1, \ldots, x_m, y_1, \ldots, y_m$ des éléments distincts d'un corps K. Montrer que la matrice $m \times m$ dont le coefficient d'indice (i, j) est égal à $1/(x_i - y_j)$ est inversible.

(4) On suppose que G n'a que des racines simples. Montrer alors que la distance minimale du code C' est égale à $r+1$. Comment pourriez-vous étendre cette démonstration au cas général ?

(5) Démontrer les bornes indiquées concernant les paramètres des codes de Goppa $\Gamma(L, G)$.

(6) Prendre $\mathbf{F} = \mathbf{F}_2$, $G(X) = X^3 + X + 1$ (irréductible sur $\mathbf{F}$). Si $\mathbf{F}' = \mathbf{F}_{2^m}$ avec $m = 5$ (ou plus généralement non multiple de 3), on peut choisir $L = \mathbf{F}'$ (pourquoi ?). Énumérer tous les éléments du code C et déterminer la distribution des poids de ses éléments ; vérifier que sa distance minimale est 7, bien que la borne donnée dans le texte soit 4.

(7) On suppose que $\mathbf{F} = \mathbf{F}_2$ et que G est irréductible. Soit $\mathbf{a}$ un élément non nul de C de poids w et soit $I \subset \{1, \ldots, n\}$ l'ensemble des i tels que $a_i = 1$ et posons $f(T) = \prod_{i \in I}(T - z_i)$. Le numérateur de $\sum_{i \in I} \frac{1}{T - z_i}$ est donc multiple de G ; en déduire que G divise $f'(T)$. Montrer que $f'(T) \neq 0$ mais que $f''(T) = 0$; en déduire que $f'(T)$ est le carré d'un polynôme $f_1(T)$ de degré au plus $\lfloor (w-1)/2 \rfloor$. En déduire que $w \geqslant 2r + 1$ puis que la distance minimale de C est au moins $2r + 1$. Comparer avec la distance obtenue dans la question précédente.

(8) Programmer l'algorithme de recherche de couples (P, Q) tels que $PB \equiv Q \pmod{A}$, où $\deg(P), \deg(Q) < \frac{1}{2}\deg(B)$.

(9) Programmer le décodage dans le cas du code de Goppa de l'énoncé, voire pour celui indiqué plus haut.