Université Bordeaux 1
Mathématiques

Préparation à l'agrégation
Année 2009–2010

Factorisation de polynômes sur des corps finis

Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. Vous êtes laissé(e) libre d'organiser votre discussion comme vous l'entendez. Il vous est conseillé de mettre en lumière vos connaissances à partir du fil conducteur constitué par le texte. Le jury demande que la discussion soit accompagnée d'exemples traités sur ordinateur. Il est souhaitable que vous organisiez votre présentation comme si le jury n'avait pas connaissance du texte. Le jury aura néanmoins le texte sous les yeux pendant votre exposé.

1. Introduction

La factorisation est l'un des points où l'analogie entre nombres entiers et polynômes se rompt. Par exemple, en caractéristique nulle, on peut trouver la partie sans facteurs carrés d'un polynôme (c'est-à-dire le produit de ses facteurs irréductibles) en utilisant la notion de dérivée, et en caractéristique positive, on peut aménager ce procédé. De plus, la notion de degré, la structure d'algèbre dont est muni l'ensemble de polynômes sur un corps, fournissent des outils importants pour la résolution du problème.

Nous allons voir deux algorithmes. Le premier utilise trois étapes : la factorisation en un produit de polynômes sans facteurs carrés, la factorisation en degrés distints, puis la factorisation en degrés égaux (algorithme de Cantor-Zassenhaus). La seconde utilise d'abord une factorisation en produit de polynômes sans facteurs carrés, puis un algorithme de factorisation dû à Berlekamp, qui utilise de l'algèbre linéaire.

2. Factorisation en degrés distincts

Ce paragraphe décrit une factorisation de polynômes sans facteurs carrés en un produit de polynômes de degrés distincts. On utilise le théorème suivant.

Théorème 2.1. *Pour tout $d \geqslant 1$, $x^{q^d} - x \in \mathbb{F}_q[x]$ est le produit de tous les polynômes unitaires irréductibles de $\mathbb{F}_q[x]$ dont le degré divise d.*

Définition 2.2. La décomposition en degrés distincts d'un polynôme non constant $f \in \mathbb{F}_q[x]$ est la suite $(g_1, \ldots, g_s)$ de polynômes, où g_i est le produit de tous les polynômes unitaires irréductibles de degré i qui divisent f, avec $g_s \neq 1$.

Exemple. $x^2 + x, x^4 + x^3 + x + 2$ est la décomposition en degrés distincts de $f = x(x+1)(x^2+1)(x^2+x+2) \in \mathbb{F}_3[x]$.

Pour effectuer la factorisation en degrés distincts d'un polynôme f sans facteurs carrés, on peut définir les éléments de $R = \mathbb{F}_q[x]/(f)$, pour $i \geqslant 0$: $h_i = x^{q^i}$, $f_0 = f$, $g_i = (h_i - x, f_{i-1})$, $f_i = f_{i-1}/g_i$, jusqu'à ce que $f_i = 1$. On pose alors $s = i$ et la décomposition cherchée est $(g_1, \ldots, g_s)$.

Théorème 2.3. *Cet algorithme fonctionne, et utilise au plus $O(sn^2 \log(q))$ opérations dans $\mathbb{F}_q$.*

Remarquons qu'on peut arrêter l'algorithme dès que $\deg f_i < 2(i+1)$, parce-que tous les facteurs irréductibles de f_i ont un degré supérieur ou égal à $i+1$, et donc dans ce cas, f_i est irréductible.

3. Factorisation en degrés égaux (algorithme de Cantor-Zassenhaus)

Maintenant, voyons la factorisation en degrés égaux, pour factoriser les polynômes produits par la factorisation en degrés distincts. L'algorithme décrit ici ne fonctionne que si q est impair.

Lemme 3.1. *Soit q une puissance d'un nombre premier impair, et soit $S = (\mathbb{F}_q^*)^2$ l'ensemble des carrés de $\mathbb{F}_q$. Alors S est un sous-groupe de $\mathbb{F}_q^*$ d'ordre $(q-1)/2$, égal à $\operatorname{Ker}\varphi$, où φ est l'homomorphisme de groupes de $\mathbb{F}_q^*$ dans $\{-1,1\}$ qui à a associe $a^{(q-1)/2}$.*

Soit f un polynôme unitaire de $\mathbb{F}_q[x]$ de degré n, et soit d un diviseur de n, tels que tous les facteurs irréductibles de f ont degré d. On veut trouver ces facteurs irréductibles. Il y en a $r = n/d$. On écrit $f = f_1 \dots f_r$, où pour tout i, f_i est un polynôme unitaire irréductible de degré r de $\mathbb{F}_q[x]$. On peut supposer que $r \geqslant 2$, car sinon f est irréductible. Grâce au théorème chinois, on sait qu'il existe un isomorphisme d'algèbres

$$\chi\colon R \longrightarrow \mathbb{F}_q[x]/(f_1) \times \dots \mathbb{F}_q[x]/(f_r) = R_1 \times \dots \times R_r,$$

chaque R_i étant une extension algébrique de $\mathbb{F}_q$ de degré d, donc un corps fini de cardinal q^d. Pour tout élément a de $\mathbb{F}_q$, on note $\chi_i(a)$ l'image de a dans R_i. Si l'on trouve un polynôme a tel que certains $\chi_i(a)$ sont nuls et d'autres non, alors (a, f) est un diviseur non trivial de f.

Soit $e = (q^d-1)/2$. Pour tout élément α de R_i^*, $\alpha^e \in \{\pm 1\}$, chacune des deux possibilités ayant la même probabilité d'arriver. Si on choisit $a \in \mathbb{F}_q[x]$, de façon aléatoire, avec une loi de probabilité uniforme, premier à f de degré strictement inférieur à n, alors les $\chi_i(a)$ sont des éléments aléatoires avec des lois de probabilité uniformes indépendantes de $\mathbb{F}_{q^d}^*$, et $\varepsilon_i = \chi_i(a^e) \in R_i$ est égal à 1 ou -1, chacun avec une probabilité de $1/2$. Ainsi,

$$\chi([a^e - 1]_f) = (\varepsilon_1 - 1, \dots \varepsilon_r - 1),$$

et $a^e - 1$ décompose f, sauf si $\varepsilon_1 = \dots = \varepsilon_r$, ce qui arrive avec probabilité $2^{-r+1} \leqslant 1/2$.

On procède de la façon suivante. On choisit $a \in \mathbb{F}_q[x]$ de degré inférieur strictement à n au hasard. Si $a \in \mathbb{F}_q$, on retourne : « Erreur ».

Ensuite, on pose $g_1 = \operatorname{pgcd}(a, f)$. Si $g_1 \neq 1$, on retourne g_1 : c'est un facteur non trivial de f.

On calcule $b = a^{(q^d-1)/2} \bmod f$.

On calcule $g_2 = \operatorname{pgcd}(b-1, f)$. Si $g_2 \neq 1$ et $g_2 \neq f$, alors on retourne g_2. Sinon, on retourne « Erreur ».

Théorème 3.2. *Cet algorithme de Cantor-Zassenhaus répond « Erreur » avec une probabilité inférieure à $2^{1-r} \leqslant 1/2$, où $r = n/d \geqslant 2$, ou sinon donne un facteur non trivial de f. Il se fait en au plus $O(dn^2 \log(q))$ opérations dans $\mathbb{F}_q$.*

Ainsi, si l'on fait tourner l'algorithme k fois, la probabilité de ne pas trouver de facteurs est inférieure à $2^{(1-r)k} \leqslant 2^{-k}$.

Cet algorithme donne 2 facteurs. Si on veut juste un facteur irréductible, on peut appliquer l'algorithme récursivement sur le plus petit facteur. Habituellement, on veut les r facteurs irréductibles, et donc on applique l'algorithme récursivement sur tous les facteurs.

Théorème 3.3. *Par cette méthode, on factorise un polynôme de degré $n = rd$ avec r facteurs irréductibles de degré d avec un nombre d'opérations de $O(dn^2 \log q \log r)$ en moyenne.*

Pour montrer cela, on peut illustrer la méthode par un arbre. Les noeuds de l'arbre sont des facteurs de f. La racine est f et les facteurs irréductibles sont les feuilles. Si l'algorithme de Cantor-Zassenhaus répond « Erreur », alors le noeud correspondant a exactement un enfant avec le même polynôme. Sinon, il a deux enfants qui contiennent les deux facteurs trouvés. Le produit sur tous les noeuds à un niveau de l'arbre est égal à f, donc la somme des degrés correspondants est n. Le coût en un noeud de degré m est $O(dm^2 \log q)$. Donc, le coût total à un niveau donné est de $O(dn^2 \log q)$.

Montrons maintenant que la profondeur moyenne de l'arbre est en $O(\log r)$. Soient g et g' deux facteurs irréductibles de f. La probabilité que l'algorithme de Zassenhaus sépare g et g' est supérieure à $1/2$ (s'ils n'ont pas été séparés auparavant). Donc, la probabilité pour que g et g' ne soient pas encore séparés à la profondeur k de l'arbre est au plus 2^{-k}. C'est valable pour tout couple de facteurs irréductibles de f. Comme il y a $(r^2 - r)/2 \leqslant r^2$ tels couples, la probabilité p_k que tous les facteurs irréductibles ne sont pas séparés à la profondeur k de l'arbre est au plus $r^2 2^{-k}$. p_k est en fait la probabilité pour que l'arbre soit de profondeur supérieure ou égale à k, et $p_{k-1} - p_k$ est la probabilité pour que l'arbre soit de profondeur exactement k. Donc la profondeur en moyenne de l'arbre est égale à $\sum_{k \geqslant 1} k(p_{k-1} - p_k) = \sum_{k \geqslant 0} p_k$. Pour $k < s = \lceil 2 \log_2 r \rceil$, on utilise le fait que $p_k \leqslant 1$ et pour $k \geqslant s$ le fait que $p_k \leqslant r^2 2^{-k}$ pour montrer que cette moyenne est inférieure ou égale à $s + 2$, qui est en $O(\log r)$.

4. Un algorithme complet de factorisation

Soit f un polynôme qui n'est pas nécessairement sans facteurs carrés. On peut déterminer sa partie sans facteurs carrés, par un algorithme décrit dans le paragraphe suivant.

Mais on peut aussi directement appliquer directement les algorithmes décrits dans le paragraphe précédent. Ces algorithmes donnent la factorisation en facteurs irréductibles de la partie sans facteur carrée de f. Ensuite, il suffit de chercher la valuation de f pour chacun de ces facteurs irréductibles.

Voyons le coût en opérations dans $\mathbb{F}_q$. Il est dominé par $n^3 \log q$ pour la factorisation en degrés distincts. Ensuite, on applique l'algorithme de Cantor-Zassenhaus aux différents facteurs $g_1, \ldots, g_s$ trouvés, respectivement de degrés $m_1, \ldots, m_s$. Chacune de ces

applications coûte au plus $O(im_i^2 \log q \log(m_i/i))$ opérations dans $\mathbb{F}_q$. Comme

$$i \log(m_i/i) = m_i \frac{\log(m_i/i)}{m_i/i} \leqslant m_i,$$

on trouve que le coût total est en $O(n^3 \log q)$. Le pas final, qui trouve les valuations des facteurs irréductibles, a un coût inférieur, donc en tout, l'algorithme est en $O(n^3 \log q)$.

5. Factorisation sans facteurs carrés

Soit F un corps *parfait* arbitraire. Nous nous intéressons dans ce paragraphe à la façon de réduire le problème de la factorisation d'un polynôme au problème de la factorisation d'un polynôme sans facteurs carrés.

Écrivons la factorisation en facteurs irréductibles d'un polynôme f de $F[x]$: $f = \prod_{i=1}^r f_i^{e_i}$, où les f_i sont deux à deux non associés et les e_i strictement positifs. La partie sans facteurs carrés de f est égale à $\prod_{i=1}^r f_i$. De plus,

$$f' = \sum_{i=1}^r e_i \frac{f}{f_i} f_i'.$$

Alors on peut voir que pour tout i, $f_i^{e_i-1}$ divise f', et que de plus, $f_i^{e_i}$ ne divise f' que si $e_i f_i' = 0$. Ainsi, en caractéristique nulle, la partie sans facteur carré de f est f/u, où $u = \mathrm{pgcd}(f, f')$, alors qu'en caractéristique p, ce quotient f/u est égal à $v = \prod_{p \nmid e_i} f_i$. Alors, $u/\mathrm{pgcd}(u, v^n) = \prod_{p \mid e_i} f_i^{e_i}$. On est donc ramené à calculer la racine $p^{\text{ème}}$ de ce polynôme, puis à procéder de façon récursive.

6. Algorithme de Berlekamp

Cet algorithme de factorisation utilise l'algèbre linéaire. Soit $f \in \mathbb{F}_q[x]$ un polynôme unitaire irréductible de degré $n > 0$, et soit $R = \mathbb{F}_q[x]/(f)$. Alors R est une $\mathbb{F}_q$-algèbre de dimension n, et l'application σ de R dans R qui à a associe a^q est $\mathbb{F}_q$-linéaire. Soit $\beta = \sigma - \mathrm{id}$. Alors β est également $\mathbb{F}_q$-linéaire. On va encore utiliser l'isomorphisme d'algèbres

$$\chi \colon R \longrightarrow \mathbb{F}_q[x]/(f_1) \times \cdots \times \mathbb{F}_q[x]/(f_r) = R_1 \times \cdots \times R_r.$$

Soit $\mathcal{B} = \mathrm{Ker}\, \beta$. $\chi(\mathcal{B})$ est égal à $\mathbb{F}_q \times \cdots \times \mathbb{F}_q = \mathbb{F}_q^r$ (c'est un abus de notation : c'est en fait égal au produit des images de $\mathbb{F}_q$ dans $\mathbb{F}_q[x]/(f_i)$).

Soit Q la matrice de σ dans la base de R formée par les images de $1, x, \ldots, x^{n-1}$ dans R. L'algorithme de Berlekamp détermine dans un premier temps une base $b_1, \ldots, b_r$ de $\mathcal{B}$, en utilisant le pivot de Gauss. Notons que f est irréductible si et seulement si le rang de $Q - I$ est égal à $n - 1$. On va supposer à partir de maintenant que q est impair. Soit $b = \sum_{i=1}^r c_i b_i$ un élément de $\mathcal{B}$ choisi au hasard, où les c_i sont des éléments de $\mathbb{F}_q$. On emploi la même idée que pour la factorisation en degrés égaux. Si aucun f_i ne divise b, alors pour tout i, $b^{(q-1)/2} \equiv \pm 1 \bmod f_i$, et chacune des deux possibilités apparaît avec probabilité $1/2$, et ce de façon indépendante pour tout i. L'algorithme suivant donne un facteur non trivial de f, ou bien retourne « Erreur ».

On calcule $g_1 = \text{pgcd}(b, f)$. Si $g_1 \neq 1$, on termine l'algorithme : g_1 est un facteur de f.

On calcule $a = b^{(q-1)/2}$.

On calcule $g_2 = \text{pgcd}(a - 1, f)$. Si $g_2 \neq 1$ et $g_2 \neq f$, alors on retourne g_2, sinon, on retourne « Erreur ».

Théorème 6.1. *Cet algorithme répond « Erreur » avec une probabilité inférieure à* $1/2$*, ou sinon donne un facteur non trivial de* f*. Il utilise au plus* $O(n^3 + n^2 \log q)$ *opérations dans* $\mathbb{F}_q$*.*

Si l'on veut une factorisation complète de f, on se contente de calculer une base de $\mathcal{B}$ une fois pour toute, puis on applique le reste de l'algorithme récursivement à g et f/g, où g est le facteur trouvé. Une analyse semblable à celle correspondant à l'algorithme de factorisation en degrés égaux montre que le coût en moyenne est de $O(n^3 + n^2 \log q)$ opérations dans $\mathbb{F}_q$.

Référence. Modern computer algebra (Von zur Gathen et Gerhard).