Factorisation des polynômes à plusieurs variables

Journées Nationales de Calcul Formel 2013

Grégoire Lecerf

CNRS UMR 7161, LABORATOIRE D'INFORMATIQUE

CAMPUS DE L'ÉCOLE POLYTECHNIQUE, PALAISEAU, FRANCE

Introduction

- La factorisation des polynômes est une question centrale depuis les années 70 en calcul formel.
- Les sous-algorithmes nécessaires pour la factorisation sont nombreux.
- La recherche en factorisation à donné lieu à plusieurs avancées :
  - LLL,
  - utilisation du principe de transposition en algèbre linéaire,
  - « pas de bébé, pas de géant » pour le calcul du polynôme minimal dans une algèbre,
  - composition modulaire, etc.
- L'utilisation de la factorisation intervient principalement en intégration symbolique, calcul symbolique, thèorie des nombres, géométrie algébrique, etc.

Calculabilité – résultats négatifs

Définition.

Un corps est effectif si ses éléments peuvent être représentés avec l'alphabet $\{0, 1\}$ et ses opérations élémentaires ($+$, $-$, $\times$, $\div$, $=$) sont calculables avec une machine de Turing.

Théorème. Frohlich, Shepherdson, 1955

Il existe des corps effectifs $\mathbb{K}$ pour lesquels la décomposition en irréductibles des polynômes de $\mathbb{K}[x]$ n'est pas calculable.

Démonstration.

Soit $\lambda : \mathbb{N}^* \to \mathbb{N}^*$ une fonction injective calculable.

Soit p_i le i-ième nombre premier, $\mathbb{K} := \mathbb{Q}(\sqrt{p_{\lambda(1)}}, \sqrt{p_{\lambda(2)}}, \sqrt{p_{\lambda(3)}}, \ldots)$.

Factoriser $x^2 - p_n$ dans $\mathbb{K}[x]$ est équivalent à tester $n \in \lambda(\mathbb{N}^*)$.

λ peut être construite de sorte à ce que ce test soit indécidable, en utilisant le fait que la terminaison d'un programme est indécidable.

Calculabilité – résultats positifs

Définition.

Un corps $\mathbb{K}$ est explicitement finiment engendré sur un corps $\mathbb{F}$ lorsqu'il est donné par le corps des fractions de $\mathbb{F}[x_1, ..., x_n]/\mathfrak{P}$, où $\mathfrak{P}$ est un idéal premier de $\mathbb{F}[x_1, ..., x_n]$ donné par un ensemble fini de polynômes de $\mathbb{F}[x_1, ..., x_n]$.

Théorème.

Si $\mathbb{K}$ est explicitement finiment engendré sur son sous-corps premier $\mathbb{F}$, alors la factorisation dans $\mathbb{K}[x_1, ..., x_n]$ est calculable.

Kronecker, 1882

Hermann, 1926

van der Waerden, 1930

Fröhlich et Shepherdson, 1955

Seidenberg, 1970-1978

Richman, 1981

Plan du cours

1. Modèle de calcul et complexité
2. Factorisation séparable
3. Polynômes à une variable sur un corps fini
4. Polynômes à une variable sur les nombres rationnels
5. Polynômes à deux variables
6. Polynômes à plusieurs variables

Chapitre 1.

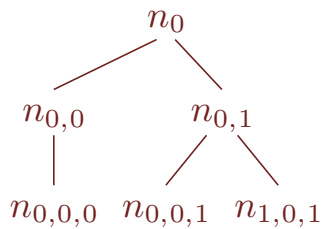
Modèle de calcul et complexité

Arbre binaire

Définition.

Un arbre binaire est un graphe acyclique orienté dont tous les nœuds sauf un, appelé la racine, a un parent et au plus deux fils.

Exemple.

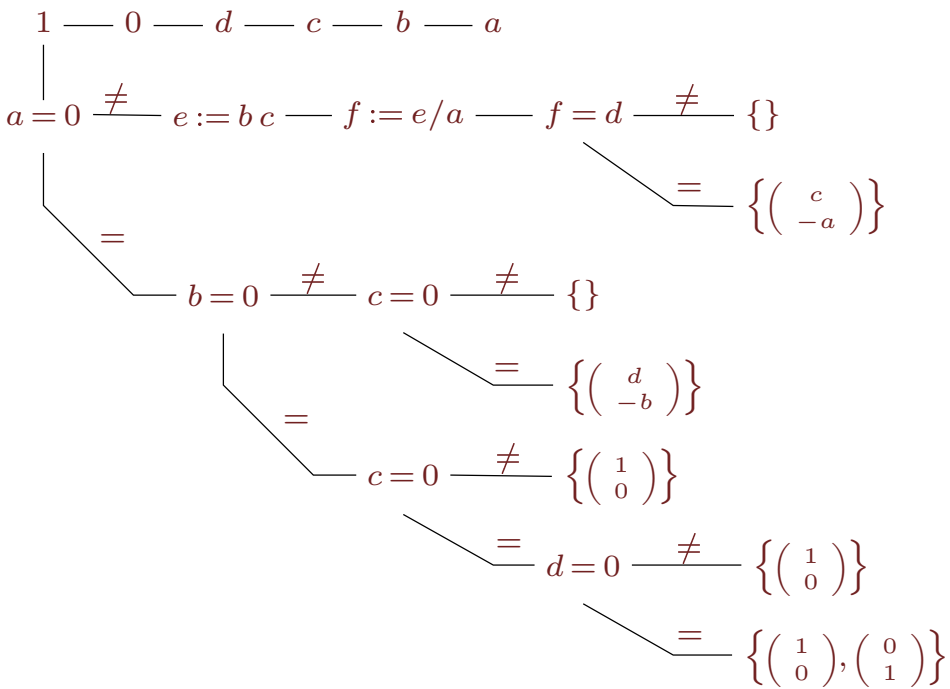


Définition.

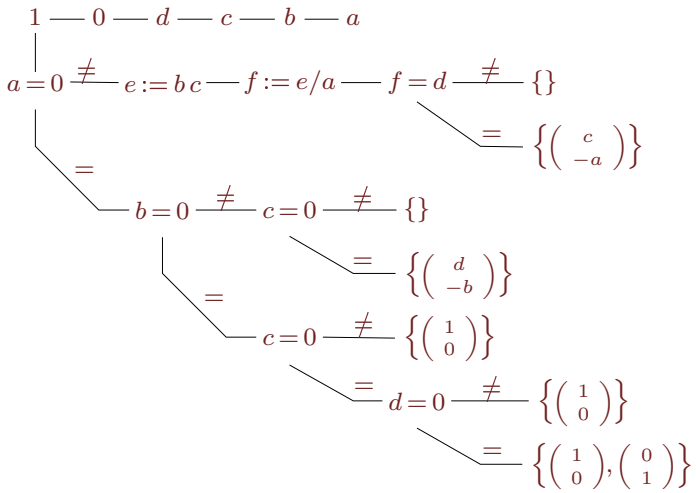
$u \prec v \Leftrightarrow u$ est le grand-$\cdots$-grand-parent de v.

Syntaxe d'un arbre de calcul

Exemple du calcul du noyau d'une matrice de la forme $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$:



Sémantique d'un arbre de calcul



$\mathbb{A} := \mathbb{Q}$, entrée $e := \begin{pmatrix} a & c \\ b & d \end{pmatrix} := \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$, chemin T_e, fonctions d'évaluation α et β :

	a	b	c	d	0	1	$a = 0$	$e := b\,c$	$f := e/a$	$f = d$
nœud de calcul	1	2	2	4	0	1		4	4	
nœud de branchement							faux			vrai

La valeur de sortie est $\left\{\begin{pmatrix} 2 \\ -1 \end{pmatrix}\right\}$.

Fonction de coût

$\mathbb{A}$: une structure algébrique

Ω : l'ensemble des opérations élémentaires $(-, +, \times, ...)$

P : l'ensemble des prédicats $(=, \neq, <, ...)$

Définition.

Une fonction de coût est une fonction de $\Omega \cup P$ dans $\mathbb{N}$.

Définition.

Le coût d'un nœud de sortie v est la somme des coûts des nœuds sur le chemin menant de la racine à v.

Définition.

Si f et g sont deux fonctions de $\mathbb{N}$ dans $\mathbb{R}_+$ définies au voisinage de l'infini.

$f(n) \in O(g(n)) \Leftrightarrow \exists\ N$ et C telles que $f(n) \leqslant C\, g(n)$ pout tout $n \geqslant N$.

$f(n) \in \tilde{O}(g(n)) \Leftrightarrow f(n) \in g(n) \log_2 (3 + g(n))^{O(1)}$.

Opérations élémentaires sur les polynômes

Définition.

Si $\mathbb{A}$ est un anneau, la représentation dense des polynômes de $\mathbb{A}[x]$ consiste à stocker un polynôme de degré d comme le vecteur de ses $d+1$ coefficients du degré 0 au degré d.

Proposition.

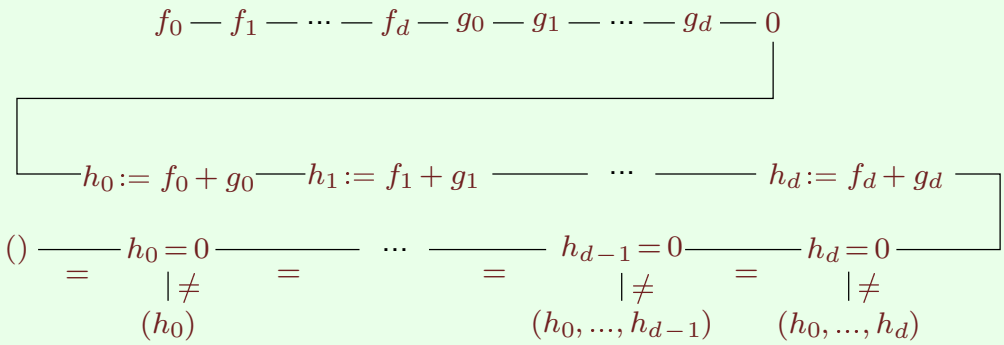
Il existe une constante σ telle que, pour tout anneau $\mathbb{A}$, il existe une famille d'arbres de calcul $(S_d)_{d\in\mathbb{N}}$ sur $\mathbb{A}$ telle que pour deux polynômes f et g de $\mathbb{A}[x]$ de degré au plus $d \geqslant 0$, l'arbre S_d évalué sur les entrées f et g calcule la somme $f+g$, avec une fonction de coût total associée $d \mapsto c(T_d)$ bornée par $\sigma\, d$.

D'un façon moins formelle, nous dirons que la somme de deux polynômes s'effectue en temps linéaire.

Somme de deux polynômes

Démonstration.

Nous pouvons prendre l'arbre de calcul suivant pour S_d :



Algorithme

Définition.

Un algorithme est juste une description en langage naturel de la construction de familles d'arbres de calcul.

Exemple.

Algorithme : somme de deux polynômes

Entrée. $f = \sum_{i=0}^{m} f_i x^i$ et $g = \sum_{i=0}^{n} g_i x^i$.

Sortie. $h := f + g$.

1. Pour i de 0 à $\max(m, n)$ calculer $h_i := f_i + g_i$.
2. Retourner $h = \sum_{i=0}^{\max(m,n)} h_i x^i$.

Produit de deux polynômes

Proposition.

Il existe une constante μ telle que, pour tout anneau $\mathbb{A}$, il existe une famille d'arbres de calcul $(M_d)_d$ telle que pour deux polynômes f et g de $\mathbb{A}[x]$ de degré au plus d, l'arbre M_d évalué sur les entrées f et g calcule le produit fg, avec une fonction de coût total associée $d \mapsto c(M_d)$ bornée par $\mu\, d^2$.

Algorithme : produit de deux polynômes

Entrée. $f = \sum_{i=0}^{m} f_i\, x^i$ et $g = \sum_{i=0}^{n} g_i\, x^i$.

Sortie. $h := fg$.

1. Si $f = 0$ ou $g = 0$ alors retourner $h := 0$.
2. Pour i de 0 à $m+n$ initialiser $h_i := 0$.
3. Pour i de 0 à m, pour j de 0 à n, calculer $h_{i+j} := h_{i+j} + f_i\, g_j$.

Autres opérations usuelles sur les polynômes

Notation.

M: $\mathbb{N} \to \mathbb{N}$, borne le coût de l'algorithme choisi pour calculer le produit de deux polynômes à coefficients dans un anneau commutatif unitaire.

Nous supposerons que M satisfait les propriétés suivantes :

$$\mathsf{M}(d)/d \text{ est croissante, } \mathsf{M}(m\,d) \leqslant m^2\,\mathsf{M}(d) \text{ pour tout } m \geqslant 1.$$

Proposition.

En degré d, les opérations suivantes coûtent $O(\mathsf{M}(d)\log d)$ opérations dans le corps des coefficients : p.g.c.d étendu, résultant, évaluation, interpolation, réductions simultanées, restes chinois.

Opérations élémentaires sur les matrices

Notation.

$\omega \in]2, 3]$, multiplier deux matrices de taille $n \times n$ sur un anneau commutatif coûte $O(n^\omega)$ opérations d'anneau (c'est à dire $+, -, \times$).

Proposition.

En taille $n \times n$, sur un corps, les opérations suivantes coûtent $O(n^\omega)$: déterminant, inverse, forme échelonnée réduite.

Définition.

matrice échelonnée réduite en colonnes :

- toutes ses colonnes non nulles sont toutes à gauche de ses colonnes nulles,
- le premier coefficient non nul d'une colonne non nulle, appelé le pivot de la colonne, est toujours strictement plus bas que le pivot de la colonne à sa gauche,
- les pivots valent 1, tous les autres coefficients dans la ligne d'un pivot sont nuls.

Chapitre 2.

Factorisation séparable

Séparabilité

Notation.

$\mathbb{A}$, anneau factoriel

p, caractéristique de $\mathbb{A}$

$\mathbb{L}$, corps des fractions de $\mathbb{A}$

F, polynôme de $\mathbb{A}[x]$ de degré $d \geqslant 1$

$\mathcal{B} := \{1, p, p^2, p^3, ...\}$ si $p > 0$, et $\mathcal{B} := \{1\}$ si $p = 0$

Définition.

$F \in \mathbb{A}[x]$ est dit séparable s'il n'a aucune racine multiple dans la clôture algébrique $\bar{\mathbb{L}}$ de $\mathbb{L}$.

Exemple. Si $p = 0$, tout polynôme sans carré est séparable.

Exemple. Si $\mathbb{A} = \mathbb{F}_3(t)$, alors $F(t, x) = 1 + t + x^3$ n'est pas séparable.

Décomposition séparable

Définition.

La décomposition séparable d'un polynôme primitif $F \in \mathbb{A}[x] \setminus \mathbb{A}$, notée $\mathrm{sep}(F)$, est l'ensemble des triplets $(G_1,\ q_1,\ m_1),\ \ldots,\ (G_s,\ q_s,\ m_s)$ de $\mathbb{A}[x] \times \mathcal{B} \times \mathbb{N}^*$ vérifiant les propriétés suivantes :

- $(\boldsymbol{S_1})$. $F(x) = \prod_{i=1}^{s} G_i^{m_i}(x^{q_i})$,
- $(\boldsymbol{S_2})$. les $G_i(x^{q_i})$ sont premiers entre eux deux à deux,
- $(\boldsymbol{S_3})$. les m_i ne sont pas divisibles par p,
- $(\boldsymbol{S_4})$. les G_i sont primitifs et séparables de degré au moins 1,
- $(\boldsymbol{S_5})$. les couples (q_i, m_i) sont deux à deux distincts.

Théorème.

Tout polynôme primitif F de $\mathbb{A}[x]$ admet une unique décomposition séparable (à permutation et unités près dans $\mathbb{A}$).

Démonstration.

Les racines de G_i sont celles de F de multiplicité $q_i\, m_i$.

Exemples

```
Mmx] use "factorix";
     x == polynomial (0, 1);
```

```
Mmx] F == (x^9 + x^3 + 1)^2 * (x^4 - 1)
```

$$x^{22} - x^{18} + 2\,x^{16} + 2\,x^{13} - 2\,x^{12} + x^{10} - 2\,x^9 + 2\,x^7 - x^6 + x^4 - 2\,x^3 - 1$$

```
Mmx] separable_factorization F
```

$$(x^4 - 1)\,(x^9 + x^3 + 1)^2$$

```
Mmx] S == separable_factorization (F mod modulus 3)
```

$$(x^3 + x^2 + x + 1)\,((x^3)^2 + x^3 + 2)^2\,(x + 2)^7$$

```
Mmx] [ [factor g, ideg g, mul g] | g in S ]
```

$$[[x^3 + x^2 + x + 1, 1, 1], [x^2 + x + 2, 3, 2], [x + 2, 1, 7]]$$

Algorithme de Musser

Algorithme de Musser

Entrée. un polynôme primitif $F \in \mathbb{A}[x]$ de degré $d \geqslant 1$.

Sortie. la liste L des facteurs séparables de F de la forme $(G, 1, m)$, et un polynôme C qui est le produit des autres facteurs séparables de F.

1. Initialiser L à la liste vide et i à l'entier 1.
2. Calculer $C := \gcd(F, F')$ et $G := F/C$.
3. Tant que $\deg(G) \geqslant 1$ faire :
   a) calculer $P := \gcd(C, G)$ et $C := G/P$,
   b) si $\deg(G) > \deg(P)$ alors adjoindre $(G/P, 1, i)$ à L,
   c) $G := P$, et $i := i + 1$.
4. Retourner L et C.

Démonstration.

F_0 le facteur de F composé des racines de multiplicité qui ne sont pas multiples de p.
$F_1 := F/F_0$. Notons $(G_1, 1, m_1), ..., (G_s, 1, m_s) := \mathrm{sep}(F_0)$.

$$F'(x) = F_1(x) \sum_{i=1}^{s} m_i G_i'(x) G_i^{m_i-1}(x) \frac{F_0(x)}{G_i^{m_i}(x)}$$

À l'étape 2, nous avons $C = F_1 \prod_{i=1}^{s} G_i^{m_i-1}$, et $G = \prod_{i=1}^{s} G_i$.
À la première étape de la boucle : $P = \prod_{i=1, m_i \geqslant 2}^{s} G_i$, $C = F_1 \prod_{i=1, m_i \geqslant 2}^{s} G_i^{m_i-2}$.
À la deuxième étape de la boucle : $P = \prod_{i=1, m_i \geqslant 3}^{s} G_i$, $C = F_1 \prod_{i=1, m_i \geqslant 3}^{s} G_i^{m_i-3}$...

Algorithme naïf de factorisation séparable

Algorithme : décomposition séparable (Gianni, Trager, 1996)

Entrée :. un polynôme primitif $F \in \mathbb{A}[x]$ de degré $d \geqslant 1$.

Sortie :. la décomposition séparable de F.

1. Appeler l'algorithme de Musser pour obtenir l'ensemble $L = \{(G_1, 1, m_1), ..., (G_r, 1, m_r)\}$ des facteurs séparables de F contenant toutes les racines de F de multiplicité non divisible par p, et le facteur F_1 restant de F.
2. Calculer $\tilde{F}_1$ défini par $\tilde{F}_1(x^p) = F_1(x)$.
3. Appeler récursivement le présent algorithme pour obtenir la décomposition séparable $\tilde{L} = \{(G_{r+1}, q_{r+1}, m_{r+1}), ..., (G_s, q_s, m_s)\}$ de $\tilde{F}_1$.
4. Retourner $\{(G_1, 1, m_1), ..., (G_r, 1, m_r), (G_{r+1}, p\,q_{r+1}, m_{r+1}), ..., (G_s, p\,q_s, m_s)\}$.

Proposition.

L'algorithme est correct. Si $\mathbb{A}$ est un corps, alors son coût est borné par $O(d\,\mathsf{M}(d)\log d)$.

Démonstration.

$F(x) = G_1^{m_1}(x) \cdots G_r^{m_r}(x)\,\tilde{F}_1(x^p)$.

Algorithme de Yun revisité

Lemme.

Supposons $p > 0$, et soit F un polynôme primitif de $\mathbb{A}[x]$. Il existe des polynômes primitifs S_0 et S_1 de $\mathbb{A}[x]$, uniques à des unités près de $\mathbb{A}$, avec les propriétés suivantes :

- les facteurs irréductibles de S_0 sont séparables de multiplicité au plus $p-1$,
- $F(x) = S_0(x)\, S_1(x^p)$.

Exemple. Lorsque $\mathbb{A} := \mathbb{F}_3$ et $F := x^2\,(x+1)^3\,(x+2)^4 = x^9 + 2\,x^8 + 2\,x^3 + x^2$, nous avons $S_0 = (x+2)\,x^2$ et $S_1 = (x+1)\,(x+2)$.

Exemple. Lorsque $\mathbb{A} := \mathbb{F}_3[t]$ et $F := (x+2\,t)^7\,(x^3+2\,t)^3\,(x^6+t)$, nous avons $S_0 = x + 2\,t$ et $S_1 = (x^2+t)\,(x+2\,t^3)^2\,(x+2\,t)^3$.

Algorithme de Yun revisité

Algorithme de Yun

Entrée. un polynôme primitif $F \in \mathbb{A}[x]$ de degré $d \geqslant 1$.

Sortie. $\mathrm{sqr}(S_0)$ et S_1.

1. Poser $l := 1$ et initialiser L avec la liste vide.
2. Calculer $U := \gcd(F, F')$, $V := F/U$, et $W := F'/U$.
3. Tant que $\deg(V) \geqslant 1$ faire :
   a. Calculer $H := \gcd(V, W - V')$, $W = (W - V')/H$, et $V := V/H$.
   b. Si $\deg(H) \geqslant 1$ alors adjoindre (H, l) à L.
   c. Incrémenter l de 1.
4. Calculer $S_0 := \prod_{(H,l)\in L} H^l$.
5. Calculer F/S_0 et S_1 défini par $S_1(x^p) = (F/S_0)(x)$.
6. Retourner L et S_1.

Proposition.

L'algorithme est correct. Si $\mathbb{A}$ est un corps, alors il effectue $O(\mathsf{M}(d)\log d)$ opérations dans $\mathbb{A}$.

Algorithme rapide de factorisation séparable

Algorithme : factorisation séparable rapide

Entrée. un polynôme primitif $F \in \mathbb{A}[x]$ de degré d.

Sortie. $\mathrm{sep}(F)$.

1. Calculer $\mathrm{sqr}(S_0)$ et S_1 avec l'algorithme de Yun.
2. Utiliser récursivement le présent algorithme pour calculer $\mathrm{sep}(S_1)$.
3. Fusionner $\mathrm{sqr}(S_0)$ et $\mathrm{sep}(S_1)$ de sorte à obtenir $\mathrm{sep}(F)$.

Théorème. Lecerf, 2008

L'algorithme est correct. Si $\mathbb{A}$ est un corps, alors il effectue $O(\mathsf{M}(d)\log d)$ opérations dans $\mathbb{A}$.

- La difficulté est dans l'étape 3 de fusion.
- Lorsque $\mathbb{A}$ est un corps parfait, on retrouve un algorithme connu (Modern Computer Algebra, exercise 14.30).

Polynômes à deux variables

Notation.

$F \in \mathbb{K}[t][x]$, de degrés partiels d_t et d_x.

Théorème. Lecerf, 2008

Si $\mathbb{K}$ contient au moins $d_t\,(2\,d_x+1)+1$ éléments, alors $\mathrm{sep}(F)$ peut être calculé avec au plus $O(d_x\,(d_x\,\mathsf{M}(d_t)\log d_t + d_t\,\mathsf{M}(d_x)\log d_x)$ ou $\tilde{O}(d_t\,d_x^2)$ opérations dans $\mathbb{K}$.

Théorème. Lecerf, 2008

Si $|\mathbb{K}| \gg d_t\,d_x$, la décomposition séparable de $F \in \mathbb{K}[t][x]$ peut être calculée au moyen de $O(d_x\,\mathsf{M}(d_t)\log(d_t) + d_t\,\mathsf{M}(d_x)\log(d_x))$ ou $\tilde{O}(d_t\,d_x)$ opérations dans $\mathbb{K}$ en moyenne.

- La technique probabiliste est essentiellement la même que pour le p.g.c.d.

Déflation

Définition.

Le degré d'inséparabilité de F, noté $\mathrm{ideg}(F)$, est le plus grand $q \in \mathcal{B}$ tel que $F \in \mathbb{A}[x^q] \setminus \mathbb{A}[x^{pq}]$.

Si $F \in \mathbb{A}[x] \setminus \mathbb{A}$, le polynôme déflaté de F est $\tilde{F}$ défini par $\tilde{F}(x^{\mathrm{ideg}(F)}) := F(x)$.

Notation.

$\mathcal{Q}$, l'ensemble des puissances q-ièmes des irréductibles de $\mathbb{A}[x] \setminus \mathbb{A}$ pour $q \in \mathcal{B}$.

$\mathcal{S}$, l'ensemble des polynômes séparables irréductibles de $\mathbb{A}[x] \setminus \mathbb{A}$.

Proposition.

$$\begin{aligned} \Phi \colon \mathbb{A}[x] \setminus \mathbb{A} &\to (\mathbb{A}[x] \setminus \mathbb{A}[x^p]) \times \mathcal{B} \\ F &\mapsto (\tilde{F}, \deg^i(F)) \end{aligned}$$

Φ est une bijection qui envoie $\mathcal{Q}$ surjectivement sur $\mathcal{S} \times \mathcal{B}$.

Calcul de Φ^{-1}

Algorithme : calcul de Φ^{-1}

Entrée . $(G, q) \in \mathcal{S} \times \mathcal{B}$.

Sortie . $(H, h) \in \mathbb{A}[x] \times \mathcal{B}$ avec H irréductible tel que $H^h = \Phi^{-1}(G, q)$.

1. Poser $\tilde{G} := G$ et $h := 1$.
2. Tant que $\tilde{G}(x^p)$ est une puissance p-ième et tant que $h < q$ faire :
   Remplacer $\tilde{G}$ par la racine p-ième de $\tilde{G}(x^p)$ et multiplier h par p.
3. Retourner $(\tilde{G}(x^{q/h}), h)$.

Lemme.

L'algorithme est correct et coûte $O(\deg(G) \log_p q)$ extractions de racines p-ièmes de $\mathbb{A}$.

Exemple. Si $\mathbb{A}$ est un corps parfait alors $\Phi^{-1}(F, q)$ est la racine q-ième de $F(x^q)$.

Exemple. Si $\mathbb{A} = \mathbb{F}_3[t]$, alors $\Phi^{-1}(1 + t^3 + x, 9)$ alors l'algorithme retourne $1 + t + x^3$ et 3, puisque $(1 + t + x^3)^3 = 1 + t^3 + x^9$.

Réduction de la factorisation au cas séparable

Algorithme

Entrée. un polynôme primitif $F \in \mathbb{A}[x]$ de degré $d \geqslant 1$.

Sortie. $\mathrm{irr}(F)$.

1. Calculer la décomposition séparable $\mathrm{sep}(F)$ de F.
2. Pour chaque $(G, q, m) \in \mathrm{sep}(F)$ calculer la décomposition irréductible G.
3. Retourner

$$\bigcup_{(G,q,m)\in \mathrm{sep}(F)} \{(H(x^{q/h}), h\, m) |\ H^h := \Phi^{-1}(\bar{G}, q),$$

pour chaque facteur irréductible $\bar{G}$ de $G\}$.

Proposition.

L'algorithme est correct. Si $\mathbb{A}$ est un corps, alors il effectue des factorisations irreducibles de polynômes séparables de $\mathbb{A}[x]$ dont la somme des degrés est au plus d, ainsi que $O(\mathsf{M}(d) \log d)$ opérations arithmétiques dans $\mathbb{A}$ et $O(d)$ extractions de racines p-ièmes dans $\mathbb{A}$.

Chapitre 3.

Polynômes à une variable sur un corps fini

Introduction

Les premières techniques connues remontent aux travaux de Gauss (1798), Galois (1830), et Arwins (1918). Les premiers algorithmes performants sont dus à Berlekamp (1970), Cantor et Zassenhaus (1981).

```
Mmx] use "factorix";
     x == polynomial (0, 1);
     f == (x^9 + x^3 + 1)^2 * (x^4 - 1)
```

$$x^{22} - x^{18} + 2\,x^{16} + 2\,x^{13} - 2\,x^{12} + x^{10} - 2\,x^9 + 2\,x^7 - x^6 + x^4 - 2\,x^3 - 1$$

```
Mmx] f mod modulus 3
```

$$x^{22} + 2\,x^{18} + 2\,x^{16} + 2\,x^{13} + x^{12} + x^{10} + x^9 + 2\,x^7 + 2\,x^6 + x^4 + x^3 + 2$$

```
Mmx] irreducible_factorization (f mod modulus 3)
```

$$(x+1)\,(x^2+1)\,(x^2+x+2)^6\,(x+2)^7$$

Résidus

Notation.

$\mathbb{K}$, un corps de caractéristique $p>0$. Pour simplifier, on suppose $p\neq 2$.
$\mathbb{F}$, un sous-corps fini de $\mathbb{K}$ de cardinal χ.
Soit f séparable de degré d dans $\mathbb{K}[x]$, de racines $\varphi_1,\ldots,\varphi_d$ et de facteurs irréductibles $f_1,\ldots,f_r$.

Proposition.

Soit $g\in\mathbb{K}[x]$ de degré au plus $d-1$.

. $g(\varphi_i)/f'(\varphi_i)\in\mathbb{F}$, pour tout $i\in\{1,\ldots,d\}$.

$\Leftrightarrow$. $g^{\chi}-(f')^{\chi-1}\,g\in(f)$ (méthode de Berlekamp).

$\Leftrightarrow$. $g\in\left\langle f_1'\,\hat{f}_1,\ldots,f_r'\,\hat{f}_r\right\rangle_{\mathbb{F}}$ où $\hat{f}_i:=f/f_i$.

Démonstration.

Posons $\rho_i:=g(\varphi_i)/f'(\varphi_i)\in\bar{\mathbb{K}}$, $\dfrac{g}{f}=\displaystyle\sum_{i=1}^{d}\frac{\rho_i}{x-\varphi_i}$.

- $(g^{\chi}-(f')^{\chi-1}\,g)(\varphi_i)=(f')^{\chi}(\varphi_i)\,(\rho_i^{\chi}-\rho_i)$
- $\dfrac{\lambda_1 f_1'\,\hat{f}_1+\cdots+\lambda_r f_r'\,\hat{f}_r}{f}=\sum_{i=1}^{r}\lambda_i\dfrac{f_i'}{f_i}=\sum_{i=1}^{r}\sum_{f_i(\varphi)=0}\dfrac{\lambda_i}{x-\varphi}$

D'une base des résidus aux facteurs

Algorithme

Entrée. $f \in \mathbb{F}_q[x]$ séparable, et une base $g_1, ..., g_r$ de $\langle f_1' \hat{f}_1, ..., f_r' \hat{f}_r \rangle_{\mathbb{F}_q}$.

Sortie. les facteurs irréductibles $f_1, ..., f_r$ de f.

1. Si $r = 1$ alors retourner f.
2. Choisir des éléments c_1, ..., c_r dans $\mathbb{F}_q$ à l'aide d'un générateur aléatoire, et calculer $g := c_1\, g_1 + \cdots + c_r\, g_r$.
3. Si $h_1 := \gcd(f, g)$ n'est pas constant alors aller à l'étape 6.
4. Calculer $h := (g/f')^{\frac{q-1}{2}} \bmod f$.
5. Si $h_1 := \gcd(f, h-1)$ est constant alors retourner à l'étape 2.
6. Calculer $h_2 := f/h_1$.
7. Calculer une base $g_{1,1}, ..., g_{r_1,1}$ des $g_i/h_2 \bmod h_1$ pour $i \in \{1, ..., r\}$.
8. Calculer une base $g_{1,2}, ..., g_{r_2,2}$ des $g_i/h_1 \bmod h_2$ pour $i \in \{1, ..., r\}$.
9. Retourner la réunion des facteurs obtenus par l'appel récursif avec $h_1, g_{1,1}, ..., g_{r_1,1}$, d'une part, puis $h_2, g_{1,2}, ..., g_{r_2,2}$ d'autre part.

Proposition.

L'algorithme est correct et nécessite au plus $O(d\, r^{\omega-1} \log r + (r + \log d + \log q)\, \mathsf{M}(d) \log r)$ ou $\tilde{O}(d^\omega + d \log q)$ opérations dans $\mathbb{F}_q$ en moyenne.

Algorithme de Berlekamp

Algorithme de Berlekamp

Entrée. $f \in \mathbb{F}_q[x]$ séparable de degré $d \geqslant 1$.

Sortie. les facteurs irréductibles $f_1, ..., f_r$ de f.

1. Calculer, dans la base $1, x, ..., x^{d-1}$, la matrice B de l'endomorphisme de Frobenius $\alpha \mapsto \alpha^q$ dans $\mathbb{F}_q[x]/(f)$.
2. Calculer une base $\rho_1, ..., \rho_r$ du noyau de B.
3. Calculer $g_i = \rho_i f' \bmod f$ pour $i \in \{1, ..., r\}$.
4. Appeler l'algorithme précédent avec $f, g_1, ..., g_r$ et retourner la factorisation obtenue.

Proposition.

L'algorithme est correct et utilise en moyenne $\tilde{O}(d^\omega + d \log q)$ opérations dans $\mathbb{F}_q$.

Itérés de Frobenius

Définition.

La suite des itérés de Frobenius $(\Phi_i)_{i \geqslant 0}$, relative à f définie par $\Phi_i = x^{q^i} \bmod f$.

- D'une façon naïve $\Phi_0, \ldots, \Phi_d$ peuvent être calculés en utilisant $O(d\,\mathsf{M}(d)\log q)$ opérations dans $\mathbb{F}_q$.

Proposition. Gathen, Shoup, 1992

Une fois Φ_1 connu, $\Phi_0, \ldots, \Phi_d$ peuvent être calculés avec $O(\mathsf{M}(d)^2 \log^2 d)$ opérations dans $\mathbb{F}_q$.

Démonstration.

L'évaluation de Φ_i en $\Phi_1, \ldots, \Phi_i$ modulo f donne $\Phi_{i+1}, \ldots, \Phi_{2i}$.

Décomposition par degré des facteurs

Algorithme

Entrée. f séparable, de degré $d \geqslant 1$.

Sortie. la décomposition $e_1, ..., e_d$ par degré des facteurs irréductibles de f.

1. Pour chaque i de 1 à d :
   calculer $e_i := \gcd(\Phi_i - x, f)$ puis remplacer f par f/e_i.
2. Retourner $e_1, ..., e_d$.

Proposition. Gathen, Shoup, 1992

L'algorithme est correct et nécessite $O(\mathsf{M}(d)\ (\mathsf{M}(d)\ \log^2 d + \log q))$ ou $\tilde{O}(d^2 + d \log q)$ opérations dans $\mathbb{F}_q$.

Démonstration.

$x^{q^i} - x$ est le produit de tous les facteurs irréductibles unitaires de $\mathbb{F}_q[x]$ dont le degré divise i.

Par la proposition précédente nous obtenons un coût total en

$O(\mathsf{M}(d) \log q + \mathsf{M}(d)^2 \log^2 d + d\, \mathsf{M}(d) \log d)$.

Séparation des facteurs de même degré

Algorithme

Entrée. f séparable ayant tous ses facteurs irréductibles de degré d/r.

Sortie. la décomposition en irréductibles $f_1, ..., f_r$.

1. Si $r = 1$ alors retourner f.
2. Répéter :
   a) Choisir un polynôme h de degré au plus $d-1$ d'une façon aléatoire.
   b) Calculer $f_1 := \gcd(f, h)$. Si f_1 n'est pas constant alors aller à l'étape 3.
   c) Calculer $g := h^{\frac{q^{d/r}-1}{2}} \bmod f$.
   d) Calculer $f_1 := \gcd(f, g-1)$.
   e) Si f_1 n'est pas constant alors aller à l'étape 3.
3. Calculer $f_2 := f/f_1$ et appeler récursivement la fonction sur f_1 et f_2 et retourner la réunion des facteurs.

Proposition. Gathen, Shoup, 1992

L'algorithme est correct et effectue $\tilde{O}(d^2 + d \log q)$ opérations dans $\mathbb{F}_q$.

Conclusion

Théorème. Gathen, Shoup, 1992

Un polynôme de degré d dans $\mathbb{F}_q[x]$ peut être factorisé avec un coût moyen dans $\tilde{O}(d^2 + d \log q)$.

Théorème. Kaltofen, Shoup, 1998

Un polynôme de degré d dans $\mathbb{F}_q[x]$ peut être factorisé avec un coût moyen dans $\tilde{O}(d^{1,815} \log q)$.

Théorème. Kedlaya, Umans, 2008

Si f, g, h sont dans $\mathbb{F}_q[x]$ de degrés au plus d, alors $g \circ h \bmod f$ peut être calculé avec un coût binaire $\tilde{O}(d \log q)$.

Corollaire de [Kaltofen, Shoup, 1998]. Kedlaya, Umans, 2008

Un polynôme de degré d dans $\mathbb{F}_q[x]$ peut être factorisé avec un coût moyen binaire dans $\tilde{O}((d^{1,5} + d \log q) \log q)$.

Défi 1. Implémenter un algorithme de composition modulaire de sorte à observer un temps quasi-linéaire et à être plus efficace que les autres implémentations.

Problème ouvert 2. Existe-il un algorithme de composition modulaire de coût quasi-linéaire pour tout corps $\mathbb{K}$?

Problème ouvert 3. Existe-il un algorithme de factorisation dans $\mathbb{F}_q[x]$ en temps polynomial ?

Chapitre 4.

Polynômes à une variable sur les nombres rationnels

Introduction

Théorème.

Soit $\mathbb{A}$ un anneau factoriel de corps de fractions $\mathbb{K}$. Un polynôme primitif f de $\mathbb{A}[x]$ est irréductible dans $\mathbb{A}[x]$ si, et seulement si, il est irréductible dans $\mathbb{K}[x]$.

```
Mmx] use "factorix"; type_mode? := true;
```

```
Mmx] irreducible_factorization (3^96 - 1)
```

$5\,7\,13\,17\,41\,73\,97\,193\,577\,769\,6481\,76801\,21523361\,24127552321\,2^7$:
Vector(Irreducible_factor(Integer))

```
Mmx] probable_irreducible_factorization (3^96 - 1)
```

$5\,7\,13\,17\,41\,73\,97\,193\,577\,769\,6481\,76801\,21523361\,24127552321\,2^7$:
Vector(Irreducible_factor(Integer))

```
Mmx] x == polynomial (0 :> Integer, 1 :> Integer)
```

x: Polynomial(Integer)

```
Mmx] irreducible_factorization (15 * (x^2 - 1))
```

$3\,5\,(x-1)\,(x+1)$: Vector(Irreducible_factor(Polynomial(Integer)))

```
Mmx] x == polynomial (0 :> Rational, 1 :> Rational)
```

x: Polynomial(Rational)

```
Mmx] irreducible_factorization (15 * (x^2 - 1))
```

$15\,(x-1)\,(x+1)$: Vector(Irreducible_factor(Polynomial(Rational)))

Algorithme naïf

Notation.

Soit f un polynôme séparable et primitif de $\mathbb{Z}[x]$ de degré d.

Notons $\|f\|_\infty := \max_{i\in\{0,\dots,d\}} |f_i|$.

Soit g est un facteur propre de f de degré au plus $m \leqslant d-1$: $\forall i \in \{0,\dots,m\}$, $g(i)$ divise $f(i)$.

1. Évaluer f en tous les points de $\{0,\dots,m\}$.
2. Énumérer tous les vecteurs $(b_0,\dots,b_m)$ de $\mathbb{Z}^{m+1}$ tels que b_i divise $f(i)$ pour tout $i \in \{0,\dots,m\}$.
3. Pour chaque tel vecteur $(b_0,\dots,b_m)$, interpoler le polynôme g de degré au plus m tel que $g(i) = b_i$ pour tout $i \in \{0,\dots,m\}$. Si g est dans $\mathbb{Z}[x] \setminus \mathbb{Z}$ et divise f alors c'est un facteur de f.
4. Si aucun facteur de f n'est trouvé à l'étape précédente alors f est irréductible.

Le coût de cette méthode dans le pire des cas est exponentiel.

Borne sur la taille des coefficients

Proposition.

Soit f un polynôme séparable primitif de $\mathbb{Z}[x]$ de degré d, et soit g un facteur propre de f de degré $m \leqslant d-1$. Alors $\|g\|_\infty \leqslant (m+1)\,(d+1)\,m^{d+2m}\,\|f\|_\infty$.

Démonstration.

À partir de la formule d'interpolation de Lagrange

$$g(x) = \sum_{i=0}^{m} g(i) \prod_{j=0,\, j\neq i}^{m} \frac{x-j}{i-j},$$

nous obtenons la majoration grossière suivante :

$$\|g\|_\infty \leqslant \left(\max_{i\in\{0,\dots,m\}} |g(i)| \right) \left\| \sum_{i=0}^{m} \prod_{j=0,\, j\neq i}^{m} (x+j) \right\|_\infty \leqslant (m+1)\,m^{2m} \max_{i\in\{0,\dots,m\}} |g(i)|.$$

La conclusion provient de $\max_{i\in\{0,\dots,m\}} |g(i)| \leqslant \max_{i\in\{0,\dots,m\}} |f(i)| \leqslant (d+1)\,m^d\,\|f\|_\infty$.

Théorème. Mignotte, 1974

Si g est un facteur de f de degré m, alors $\|g\|_\infty \leqslant \sqrt{d+1}\,2^m\,\|f\|_\infty$.

Lemme de Newton-Hensel

Lemme.

Si $\mathfrak{g} \in \mathbb{A}[x]$ divise f modulo I et que $\mathrm{lc}(\mathfrak{g}) = 1$, alors il existe un unique polynôme $\mathfrak{G}$ congru à $\mathfrak{g}$ modulo I, unitaire et divisant f modulo I^2.

Démonstration.

Posons $\mathfrak{h} := f/\mathfrak{g}$, et $\mathfrak{u} = \mathfrak{h}^{-1} \bmod \mathfrak{g}$.

Nous cherchons $\mathfrak{G}$ et $\mathfrak{H}$ tels que : $\mathfrak{G} = \mathfrak{g} \bmod I$, $\mathfrak{H} = \mathfrak{h} \bmod I$, $f = \mathfrak{G}\,\mathfrak{H} \bmod I^2$.

Àpartir de $f = \mathfrak{g}\,\mathfrak{h} + \mathfrak{g}\,(\mathfrak{H} - \mathfrak{h}) + \mathfrak{h}\,(\mathfrak{G} - \mathfrak{g}) \bmod I^2$.

$\mathrm{rem}(f, \mathfrak{g}) = \mathrm{rem}(\mathfrak{h}\,(\mathfrak{G} - \mathfrak{g}), \mathfrak{g}) \bmod I^2$.

$\mathfrak{G} = \mathfrak{g} + \mathrm{rem}(\mathfrak{u}\,f, \mathfrak{g}) \bmod I^2$.

Comme $f' = \mathfrak{g}'\,\mathfrak{h} + \mathfrak{g}\,\mathfrak{h}'$, alors $\mathfrak{h} = f'/\mathfrak{g}' \bmod \mathfrak{g}$ et nous obtenons la formule

$$\mathfrak{G} - \mathfrak{g} = \frac{\mathfrak{g}'}{f'}\, f \bmod \mathfrak{g} \bmod I^2.$$

Remontée de Newton-Hensel

Algorithme

Entrée. $f \in \mathbb{A}[x]$, et $\mathfrak{f}_1, \ldots, \mathfrak{f}_s$ unitaires dans $(\mathbb{A}/I)[x]$ tels que $f = \mathrm{lc}(f)\, \mathfrak{f}_1 \cdots \mathfrak{f}_s$ dans $(\mathbb{A}/I)[x]$.

Sortie. $\mathfrak{F}_1, \ldots, \mathfrak{F}_s$ unitaires dans $(\mathbb{A}/I^2)[x]$ tels que $f = \mathrm{lc}(f)\, \mathfrak{F}_1 \cdots \mathfrak{F}_s$ dans $(\mathbb{A}/I^2)[x]$ et $\mathfrak{F}_i = \mathfrak{f}_i \bmod I$ pour tout i.

1. Si $s = 1$ retourner $f/\mathrm{lc}(f)$.
2. Calculer $f \bmod \mathfrak{f}_1, \ldots, f \bmod \mathfrak{f}_s$ et $f' \bmod \mathfrak{f}_1, \ldots, f' \bmod \mathfrak{f}_s$ modulo I^2.
3. Calculer $\mathfrak{r}_1 = \mathfrak{f}_1' \frac{f}{f'} \bmod \mathfrak{f}_1, \ldots, \mathfrak{r}_s = \mathfrak{f}_s' \frac{f}{f'} \bmod \mathfrak{f}_s$ modulo I^2.
4. Retourner $\mathfrak{f}_1 + r_1, \ldots, \mathfrak{f}_s + r_s$.

Proposition.

Soient $\mathbb{A} = \mathbb{Z}$ et $I = (p)$ avec p premier. À partir d'une décomposition $f = \mathrm{lc}(f)\, \mathfrak{f}_1 \cdots \mathfrak{f}_s$ modulo p, avec des $\mathfrak{f}_i$ unitaires, nous pouvons calculer la décomposition $f = \mathrm{lc}(f)\, \mathfrak{F}_1 \cdots \mathfrak{F}_s$ modulo p^σ telle que $\mathfrak{F}_i = \mathfrak{f}_i \bmod p$ pour tout i, en temps $O(\mathsf{I}(\sigma \log p)\, \mathsf{M}(d) \log d)$.

Proposition.

Soient $\mathbb{K}$ un corps, $\mathbb{A} = \mathbb{K}[t]$ et $I = (t)$. À partir d'une décomposition $f = \mathrm{lc}(f)\, \mathfrak{f}_1 \cdots \mathfrak{f}_s$ modulo t, avec des $\mathfrak{f}_i$ unitaires, nous pouvons calculer la décomposition $f = \mathrm{lc}(f)\, \mathfrak{F}_1 \cdots \mathfrak{F}_s$ modulo t^σ telle que $\mathfrak{F}_i = \mathfrak{f}_i \bmod t$ pour tout i, en temps $O(\mathsf{M}(\sigma)\, \mathsf{M}(d) \log d)$.

Recombinaison des facteurs p-adiques

```
Mmx] use "factorix";
     p == modulus 5;
     F == polynomial (-1, 0, 0, 0, 1)
```

$x^4 - 1$

```
Mmx] irreducible_factorization (F mod p)
```

$(x+2)\,(x+4)\,(x+1)\,(x+3)$

```
Mmx] Fp == polynomial (p_adic (z, p) | z in @F)
```

$(1+O(p^{10}))\,x^4 + O(p^{10})\,x^3 + O(p^{10})\,x^2 + O(p^{10})\,x + 4 + 4\,p + 4\,p^2 + 4\,p^3 + 4\,p^4 + 4\,p^5 + 4\,p^6 + 4\,p^7 + 4\,p^8 + 4\,p^9 + O(p^{10})$

```
Mmx] v == irreducible_factorization (Fp)
```

$((1+O(p^{10}))\,x + 1 + O(p^{10}))\,((1+O(p^{10}))\,x + 3 + 3\,p + 2\,p^2 + 3\,p^3 + p^4 + 2\,p^6 + p^7 + 4\,p^8 + p^9 + O(p^{10}))\,((1+O(p^{10}))\,x + 2 + p + 2\,p^2 + p^3 + 3\,p^4 + 4\,p^5 + 2\,p^6 + 3\,p^7 + 3\,p^9 + O(p^{10}))\,((1+O(p^{10}))\,x + 4 + 4\,p + 4\,p^2 + 4\,p^3 + 4\,p^4 + 4\,p^5 + 4\,p^6 + 4\,p^7 + 4\,p^8 + 4\,p^9 + O(p^{10}))$

```
Mmx] g == factor v[1] * factor v[2]
```

$$(1+O(p^{10}))\,x^2+O(p^{10})\,x+1+O(p^{10})$$

```
Mmx] polynomial (@map (z :-> integer (z[0,10]), [@g]))
```

$$x^2+1$$

Cas le pire de la recherche exhaustive

Définition.

Soit p_i le i-ième nombre premier pour $i \geqslant 1$. Le n-ième polynôme de Swinnerton-Dyer est défini par

$$S_n(x) = \prod \left(x \pm \sqrt{2} \pm \sqrt{3} \pm \sqrt{5} \pm \cdots \pm \sqrt{p_n}\right),$$

où le produit est pris sur les 2^n possibilités de signes $+$ et $-$.

```
Mmx] use "factorix"
```

```
Mmx] f == swinnerton_dyer_polynomial 3
```

$x^8 - 40\,x^6 + 352\,x^4 - 960\,x^2 + 576$

```
Mmx] irreducible_factorization (f mod modulus 2)
```

x^8

```
Mmx] irreducible_factorization (f mod modulus 3)
```

$(x^2 + 1)^2\,x^4$

```
Mmx] irreducible_factorization (f mod modulus 5)
```

$$(x^2+2)^2\,(x^2+3)^2$$

```
Mmx] irreducible_factorization (f mod modulus 7)
```

$$(x^2+x+6)\,(x^2+6\,x+3)\,(x^2+6\,x+6)\,(x^2+x+3)$$

```
Mmx] irreducible_factorization (f mod modulus 11)
```

$$(x^2+7\,x+2)\,(x^2+4\,x+2)\,(x^2+2\,x+10)\,(x^2+9\,x+10)$$

```
Mmx] irreducible_factorization f
```

$$x^8-40\,x^6+352\,x^4-960\,x^2+576$$

Algorithme de Lenstra, Lenstra, Lovász

Théorème. Lenstra, Lenstra, Lovász, 1982

Si $f \in \mathbb{Z}[x]$ est un polynôme primitif de degré d alors sa décomposition irréductible peut être calculée en temps polynomial en d et $\log \| f \|_\infty$.

1. Choisir un nombre premier p ne divisant ni $\mathrm{lc}(f)$ ni $\mathrm{disc}(f)$ en temps polynomial tel que $p \in \tilde{O}(d \log \| f \|_2)$.
2. Calculer un facteur $\mathfrak{f}$ de f dans $(\mathbb{Z}/p\,\mathbb{Z})[x]$ en temps polynomial en d et p.
3. Remonter un facteur $\mathfrak{F}$ de f dans $\mathbb{Z}/p^\sigma\,\mathbb{Z}[x]$ unitaire à une précision σ définie à l'aide de la borne de Mignotte.
4. Soit $l := \deg(\mathfrak{f})$, pour $n = d - 1$, nous calculons une base réduite du réseau engendré par les d lignes de la matrice carrée suivante :

$$L := \begin{pmatrix} p^\sigma & & & & & \\ & \ddots & & & & \\ & & p^\sigma & & & \\ \mathfrak{F}_0 & \cdots & \mathfrak{F}_{l-1} & 1 & & \\ & \ddots & & \ddots & \ddots & \\ & & \mathfrak{F}_0 & \cdots & \mathfrak{F}_{l-1} & 1 \end{pmatrix}.$$

5. Le premier vecteur de cette base réduite représente un polynôme g de degré au plus n tel que $g = q\,\mathfrak{F} + p^\sigma\, r$, avec $r \in \mathbb{Z}[x]$ de degré au plus $l-1$, et $q \in \mathbb{Z}[x]$ de degré au plus $n-l$.
   Si la norme de g est trop grande, alors f est irréductible.
   Sinon nous pouvons construire un facteur propre de f qui est divisible par $\mathfrak{F}$ modulo p^σ.

Exemple

```
Mmx] use "factorix";
     p == 7;
     f == polynomial (-1, 0, 0, 0, 0, 0, 1)
```

$x^6 - 1$

```
Mmx] fp == polynomial (p_adic (z, modulus p) | z in @f)
```

$(1 + O(p^{10}))\, x^6 + O(p^{10})\, x^5 + O(p^{10})\, x^4 + O(p^{10})\, x^3 + O(p^{10})\, x^2 + O(p^{10})\, x + 6 + 6\, p + 6\, p^2 + 6\, p^3 + 6\, p^4 + 6\, p^5 + 6\, p^6 + 6\, p^7 + 6\, p^8 + 6\, p^9 + O(p^{10})$

```
Mmx] h == factor (irreducible_factorization (fp)[1])
```

$(1 + O(p^{10}))\, x + 5 + 2\, p + 3\, p^3 + 6\, p^4 + 4\, p^5 + 4\, p^7 + 2\, p^8 + 3\, p^9 + O(p^{10})$

```
Mmx] s == 10; l == deg h; d == deg f;
```

```
Mmx] L == vertical_join (
       [ if i=j then p^s else 0 | j in 0..d || i in 0..l ],
       [ (0 | j in 0..i), (integer (h[j][0,s]) | j in 0..l+1),
         (0 | j in 0..d-l-i-1) || i in 0..d-l ])
```

$$\begin{bmatrix} 282475249 & 0 & 0 & 0 & 0 & 0 \\ 135967277 & 1 & 0 & 0 & 0 & 0 \\ 0 & 135967277 & 1 & 0 & 0 & 0 \\ 0 & 0 & 135967277 & 1 & 0 & 0 \\ 0 & 0 & 0 & 135967277 & 1 & 0 \\ 0 & 0 & 0 & 0 & 135967277 & 1 \end{bmatrix}$$

```
Mmx] L == row_lll L
```

$$\begin{bmatrix} -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \\ 5498 & -3681 & -1818 & 5498 & -3680 & -1818 \\ -3680 & -1818 & 5498 & -3681 & -1818 & 5498 \end{bmatrix}$$

```
Mmx] g == [ polynomial (@row (L, i)) | i in 0..4 ]
```

$[x^3 - 1, x^3 + x^2 + x, x^4 - x, x^5 - x^2]$

```
Mmx] f1 == gcd (g[0], gcd (g[1], gcd (g[2], g[3])))
```

$x^2 + x + 1$

```
Mmx] f rem f1
```

0

```
Mmx] f quo f1
```

$x^4 - x^3 + x - 1$

Calcul des racines complexes

Notation.

Soit $f = \sum_{i=0}^{d} f_i\, x^i \in \mathbb{C}[x]$, unitaire de degré d, $\bar{f} := \sum_{i=0}^{d} \overline{f_i}\, x^i$, $\mathrm{rev}(d, f) := \sum_{i=0}^{d} f_{d-i}\, x^i$, et

$$\mathtt{B}_f(x, y) := \frac{\mathrm{rev}(d, \bar{f})(x)\,\mathrm{rev}(d, f)(y) - f(x)\,\bar{f}(y)}{1 - x\,y} = \sum_{0 \leqslant i,j < d} b_{i,j}\, x^i\, y^j.$$

Nous notons $B_f := (b_{i,j})_{i,j}$ la matrice symétrique de taille $d \times d$ des $b_{i,j}$.

Théorème. Schur-Cohn

Si $f \in \mathbb{C}[x]$ est unitaire de degré d, alors la signature de B_f est égale à la différence $\pi_+(f) - \pi_-(f)$, où $\pi_+(f)$ (resp. $\pi_-(f)$) représente le nombre de racines de f incluses dans le disque ouvert $B(0,1)$ (resp. hors du disque fermé $\bar{B}(0,1)$).

Proposition.

Soit f un polynôme de $\mathbb{Z}[x]$ sans carré de degré d. Il existe un algorithme permettant de déterminer si f admet un zéro dans $B(0,1)$ en temps polynomial en d et $\log \|f\|_\infty$.

Théorème.

Soit f un polynôme de $\mathbb{Z}[x]$ séparable de degré d. Le calcul d'une approximation d'un zéro de f dans $\mathbb{C}$ à une distance au plus $\varepsilon := 2^{-\sigma} < 1$ peut se faire en temps $(d \log(\|f\|_\infty/\varepsilon))^{O(1)}$.

Approximant algébrique

Algorithme de Kannan, Lenstra et Lovász (1984)

Entrée. $f \in \mathbb{Z}[x]$, séparable et primitif de degré $d \geqslant 1$, et un entier $m \leqslant d-1$.

Sortie. un facteur irréductible de f de degré au plus m s'il existe et sinon rien.

1. Poser $M := d^{d+2}\,\|f\|_2$, $c := 2^{(3/2)d^2+2d-1}\,M^{3m}$, $\varepsilon = 2^{-(2d^2+3d+4d\log_2 M)}$.
2. Calculer β telle qu'il existe une racine α de f avec $|\beta-\alpha| \leqslant \varepsilon/(2\,n\,\|f\|_2^n)$.
3. Pour i de 0 à m faire :

   Calculer $\tilde{\alpha}_i$ comme approximation de β^i avec $\left\lceil -\frac{1}{2}\log\varepsilon \right\rceil$ bits après la virgule.
4. Construire le réseau $\tilde{L}_c$ formé à partir des lignes de la matrice suivante :

$$\begin{pmatrix} 1 & & & c\,\mathrm{Re}(\tilde{\alpha}_0) & c\,\mathrm{Im}(\tilde{\alpha}_0) \\ & 1 & & c\,\mathrm{Re}(\tilde{\alpha}_1) & c\,\mathrm{Im}(\tilde{\alpha}_1) \\ & & \ddots & \vdots & \vdots \\ & & 1 & c\,\mathrm{Re}(\tilde{\alpha}_m) & c\,\mathrm{Im}(\tilde{\alpha}_m) \end{pmatrix}$$

5. Appeler l'algorithme de réduction de base LLL. Notons $\tilde{v}$ le premier vecteur de la base réduite.
6. Si $\|\tilde{v}\|_2 \leqslant 2\,M^2$ alors retourner le polynôme correspondant.

Exemple

```
Mmx] use "lattiz"; type_mode? := true;
```

```
Mmx] f == polynomial (6 :> Integer, 0, -5, 0, 1)
```

$x^4 - 5\,x^2 + 6$: Polynomial(Integer)

```
Mmx] N z == z - evaluate (f, z) / evaluate (derive f, z);
```

```
Mmx] a == N N N N N 1.0
```

1.41421356237303701652: Floating

```
Mmx] c == 10^5
```

100000: Integer

```
Mmx] L == [ 1, 0, c;
            0, 1, as_integer trunc (c * a )]
```

$\begin{bmatrix} 1 & 0 & 100000 \\ 0 & 1 & 141421 \end{bmatrix}$: Matrix(Integer)

```
Mmx] row_lll L
```

$$\begin{bmatrix} -239 & 169 & 149 \\ 99 & -70 & 530 \end{bmatrix} : \text{Matrix(Integer)}$$

```
Mmx] L == [ 1, 0, 0, c;
            0, 1, 0, as_integer trunc (c * a );
            0, 0, 1, as_integer trunc (c * a^2)]
```

$$\begin{bmatrix} 1 & 0 & 0 & 100000 \\ 0 & 1 & 0 & 141421 \\ 0 & 0 & 1 & 199999 \end{bmatrix} : \text{Matrix(Integer)}$$

```
Mmx] R == row_lll L
```

$$\begin{bmatrix} -2 & 0 & 1 & -1 \\ -129 & 169 & -55 & 204 \\ -14 & -239 & 176 & 205 \end{bmatrix} : \text{Matrix(Integer)}$$

```
Mmx] g == polynomial (@row (R, 0)[0,3])
```

$x^2 - 2$: Polynomial(Integer)

```
Mmx] f rem g
```

0: Polynomial(Rational)

```
Mmx] f div g
```

$x^2 - 3$: Polynomial(Rational)

Dérivée logarithmique

Notation.

$\mathfrak{F}_1, \ldots, \mathfrak{F}_s$, les facteurs p-adiques unitaires de f.

$\forall i \in \{1, \ldots, r\}$, $\exists \mu_i \in \{0,1\}^s$ tel que $f_i = \mathrm{lc}(f_r)\, \mathfrak{F}_1^{\mu_{i,1}} \cdots \mathfrak{F}_s^{\mu_{r,s}}$.

$$f\,\frac{f_i'}{f_i} = \mu_{i,1}\, f\,\frac{\mathfrak{F}_1'}{\mathfrak{F}_1} + \cdots + \mu_{i,s}\, f\,\frac{\mathfrak{F}_r'}{\mathfrak{F}_r}.$$

Notons $\sigma \in \mathbb{N}$ la précision connue pour les facteurs p-adiques.

Soit $\mathfrak{G}_i$ la pré-image de $f\,\frac{\mathfrak{F}_1'}{\mathfrak{F}_1}$ dans $\mathbb{Z}[x]$, telle que $\mathfrak{G}_i = f\,\frac{\mathfrak{F}_i'}{\mathfrak{F}_i} \bmod p^\sigma$.

Il existe un entier $c \in \mathbb{Z}$ tel que $f\,\frac{f_i'}{f_i} = \mu_{i,1}\,\mathfrak{G}_1 + \cdots + \mu_{i,s}\,\mathfrak{G}_s + c\,p^\sigma$.

La borne de Mignotte permet de déterminer un entier τ tel que $\left\| f\,\frac{f_i'}{f_i} \right\|_\infty < p^\tau$.

Si $\mathfrak{a} = \sum_{i \geqslant 0} a_i\, p^i$ est un nombre p-adique, nous notons $[\mathfrak{a}]_\tau^\sigma := \sum_{i=\tau}^{\sigma-1} a_i\, p^{i-\tau} \in \mathbb{N}$.

Si $\mathfrak{Q} = \sum_{i=0}^{d} \mathfrak{Q}_i\, x^i \in \mathbb{Z}_p[x]$ alors notons, par extension, $[\mathfrak{Q}]_\tau^\sigma := \sum_{i=0}^{d} [\mathfrak{Q}_i]_\tau^\sigma\, x^i \in \mathbb{N}[x]$.

Si $\sigma > \tau$ nous obtenons finalement des polynômes δ_i et ε_i dans $\mathbb{Z}[x]$, de degré au plus $d-1$, tels que $\|\delta_i\|_\infty \leqslant s+1$, $\|\varepsilon_i\|_\infty \leqslant s+2$ et

$$\mu_{i,1}\,[\mathfrak{G}_1]_\tau^\sigma + \cdots + \mu_{i,s}\,[\mathfrak{G}_s]_\tau^\sigma + p^{\sigma-\tau}\,\delta_i = \varepsilon_i.$$

On considère le réseau L engendré par les lignes de la matrice suivante :

$$\begin{pmatrix} 1 & & [\mathfrak{G}_{1,0}]_\tau^\sigma & \cdots & [\mathfrak{G}_{1,d-1}]_\tau^\sigma \\ & \ddots & \vdots & & \vdots \\ & & 1 & [\mathfrak{G}_{s,0}]_\tau^\sigma & \cdots & [\mathfrak{G}_{s,d-1}]_\tau^\sigma \\ & & & p^{\sigma-\tau} & & \\ & & & & \ddots & \\ & & & & & p^{\sigma-\tau} \end{pmatrix}.$$

$(\mu_{i,1}, \ldots, \mu_{i,s}, \varepsilon_{i,0}, \ldots, \varepsilon_{i,d-1})$ est un vecteur de « petite norme » dans L.

- van Hoeij, 2002
- Belabas, van Hoeij, Klüners et Steel, 2009
- Novocin, 2008
- A. Novocin et M. van Hoeij, 2009
- W. Hart, M. van Hoeij et A. Novocin, 2011

Exemple

```
Mmx] use "factorix"; p == modulus 9973;
     f == swinnerton_dyer_polynomial 2 * swinnerton_dyer_polynomial 3
```

$$x^{12} - 50\,x^{10} + 753\,x^8 - 4520\,x^6 + 10528\,x^4 - 6720\,x^2 + 576$$

```
Mmx] irreducible_factorization (f mod p)
```

$$(x^2 + 3391\,x + 1)\,(x^2 + 6582\,x + 342)\,(x^2 + 6582\,x + 1)\,(x^2 + 3391\,x + 342)\,(x^2 + 3391\,x + 9623)\,(x^2 + 6582\,x + 9623)$$

```
Mmx] f_p == polynomial (p_adic (z, p) | z in @f);
     facts_p == map (factor, irreducible_factorization (f_p));
```

```
Mmx] G == [(f_p div facts_p[i]) * derive facts_p[i] | i in 0..#facts_p];
```

```
Mmx] tau == 3; sigma == 4; s == #G; d == deg f - 1;
     L == horizontal_join (
       [ if i = j then 1 else 0 | j in 0..s || i in 0..s ],
       [ integer (G[i][j][tau, sigma]) | j in 0..d || i in 0..s ])
```

```
Mmx] L == vertical_join (L, horizontal_join (
      [ 0 | j in 0..s || i in 0..d ],
      [ if i = j then p^(sigma-tau) else 0 | j in 0..d || i in 0..d ]))
```

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 5606 & 4827 & 8343 & 6630 & 265 & 7406 & 1791 & 3859 & 4151 & 3109 & 1623 \\
0 & 1 & 0 & 0 & 0 & 0 & 1819 & 5145 & 9473 & 3342 & 1849 & 2566 & 4693 & 6113 & 1184 & 6863 & 1623 \\
0 & 0 & 1 & 0 & 0 & 0 & 8153 & 5145 & 499 & 3342 & 8123 & 2566 & 5279 & 6113 & 8788 & 6863 & 8349 \\
0 & 0 & 0 & 1 & 0 & 0 & 2331 & 9972 & 432 & 0 & 4201 & 9972 & 8109 & 0 & 3247 & 9972 & 1623 \\
0 & 0 & 0 & 0 & 1 & 0 & 4366 & 4827 & 1629 & 6630 & 9707 & 7406 & 8181 & 3859 & 5821 & 3109 & 8349 \\
0 & 0 & 0 & 0 & 0 & 1 & 7641 & 9972 & 9540 & 0 & 5771 & 9972 & 1863 & 0 & 6725 & 9972 & 8349 \\
0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9973
\end{bmatrix}$$

```
Mmx] R == row_lll L
```

$$\begin{bmatrix}
-1 & -1 & -1 & 1 & -1 & 1 & 1 & 0 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 0 & 1 \\
0 & 0 & 0 & -1 & 0 & -1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 0 & 1 & 2 & 1 \\
39 & -81 & 85 & -37 & -35 & 37 & 147 & -4 & 136 & -4 & 95 & -4 & -32 & -4 & -86 & -4 & -234 \\
-30 & 90 & -33 & 59 & 87 & -58 & 134 & -58 & 244 & -57 & -194 & -58 & 13 & -57 & -24 & -58 & 173 \\
-15 & 58 & -87 & -11 & -14 & 10 & -144 & 30 & -67 & 29 & 196 & 30 & -127 & 29 & -297 & 30 & 260 \\
121 & -52 & 151 & 48 & -22 & -49 & 210 & -98 & -9 & -99 & 154 & -98 & 170 & -99 & -71 & -98 & 133 \\
-84 & 248 & -241 & 79 & 91 & -80 & 56 & -6 & -35 & -7 & 106 & -6 & -131 & -7 & 53 & -6 & -12 \\
56 & 50 & -28 & 89 & -34 & -87 & -311 & -24 & 184 & -22 & 54 & -24 & -131 & -22 & 371 & -24 & -27 \\
-105 & 145 & -119 & 7 & 131 & -8 & -26 & -25 & -142 & -26 & -70 & -25 & 445 & -26 & -33 & -25 & -26 \\
142 & -9 & -81 & -27 & -232 & 26 & 53 & 91 & -38 & 90 & -101 & 91 & -194 & 90 & -113 & 91 & -146 \\
-102 & -288 & 171 & 343 & -15 & -344 & -302 & 118 & 91 & 117 & -17 & 118 & -4 & 117 & -125 & 118 & -348 \\
240 & -339 & -542 & -120 & 383 & -23 & -108 & 488 & 111 & -599 & -52 & -193 & -68 & 531 & 173 & -377 & -31 \\
-75 & -422 & -341 & -72 & 43 & -547 & 33 & -523 & 73 & 415 & 195 & -171 & -22 & -667 & 40 & 217 & 8 \\
586 & -176 & -161 & -416 & 488 & -376 & 73 & 467 & 70 & 593 & -215 & -709 & 218 & 128 & -91 & -192 & 27 \\
351 & -487 & -247 & 678 & 535 & 309 & -169 & 655 & 297 & 413 & -86 & -52 & -82 & -757 & 7 & -38 & -105 \\
972 & 155 & -212 & -157 & 886 & 62 & 192 & -1114 & -158 & 878 & 24 & 1036 & 20 & 49 & -99 & 6 & 72 \\
561 & -287 & -368 & 231 & 443 & 706 & 31 & -608 & -9 & -394 & -131 & -464 & 86 & 70 & 24 & 1508 & 56
\end{bmatrix}$$

```
Mmx] R[0,0,2,s]
```

$$\begin{bmatrix}
-1 & -1 & -1 & 1 & -1 & 1 \\
0 & 0 & 0 & -1 & 0 & -1
\end{bmatrix}$$

```
Mmx] Hp == facts_p[3] * facts_p[5]
```

$$(1 + O(p^{10}))\, x^4 + O(p^{10})\, x^3 + (9963 + 9972\, p + 9972\, p^2 + 9972\, p^3 + 9972\, p^4 + 9972\, p^5 + 9972\, p^6 + 9972\, p^7 + 9972\, p^8 + 9972\, p^9 + O(p^{10}))\, x^2 + O(p^{10})\, x + 1 + O(p^{10})$$

```
Mmx] reconstruct u == {
       x == integer u[0,3];
       if x > 9973^3 quo 2 then x - 9973^3 else x; };
```

```
Mmx] g == polynomial (@map (reconstruct, [@Hp]))
```

$x^4 - 10\,x^2 + 1$

```
Mmx] f rem g
```

0

```
Mmx] f div g
```

$x^8 - 40\,x^6 + 352\,x^4 - 960\,x^2 + 576$

Défi

L'algorithme PSLQ conçu par Ferguson et Bailey au début des années 90 permet de calculer une relation entière non triviale de petite taille entre plusieurs nombres (entiers ou décimaux en fixant la précision souhaitée) ou bien de prouver qu'il n'en existe pas d'une norme inférieure à une valeur donnée en entrée de l'algorithme.

```
Mmx] use "lattiz"
```

```
Mmx] pslq ([100, 150, 200], 5)
```

$[1, -2, 1]$

Défi 4. Sachant que les relations μ_i qui interviennent dans le problème de factorisation ne font intervenir que des 0 et des 1, est-il possible de tirer parti de PSLQ pour obtenir une meilleure borne de complexité, ou bien de meilleures performances pratiques ?

Chapitre 4.

Polynômes à deux variables

Introduction

Notation.

$F(x,y) \in \mathbb{K}[x,y]$, de degrés partiels d_x et d_y, tel que

$$\text{(N)} \quad \begin{cases} \deg\left(F(0,y)\right) = d_y, \\ \mathrm{Res}\left(F(0,y), \frac{\partial F}{\partial y}(0,y)\right) \neq 0, \\ F \text{ est primitif vu dans } \mathbb{K}[x][y]. \end{cases}$$

$\mathfrak{F}_1, ..., \mathfrak{F}_s$, les facteurs analytiques unitaires de F dans $\mathbb{K}[[x]][y]$.

$F_1, ..., F_r$, les facteurs rationnels F dans $\mathbb{K}[x,y]$.

$\forall i \in \{1, ..., r\}$, $\exists \mu_i \in \{0,1\}^s$ tel que $F_i = \mathrm{lc}(F_i) \prod_{j=1}^{s} \mathfrak{F}_j^{\mu_{i,j}}$.

Si $A = \sum_{i,j \geqslant 0} a_{i,j}\, x^i\, y^j \in \mathbb{K}[[x]][y]$, $[A]_k^l := \sum_{k \leqslant i \leqslant l-1, j \geqslant 0} a_{i,j}\, x^i\, y^j \in \mathbb{K}[x,y]$.

$$\hat{F}_i := \prod_{j=1, j\neq i}^{r} F_j = \frac{F}{F_i}, \qquad \hat{\mathfrak{F}}_i := \mathrm{lc}(F) \prod_{j=1, j\neq i}^{s} \mathfrak{F}_j = \frac{F}{\mathfrak{F}_i}.$$

Recherche exhaustive

```
Mmx] use "factorix";
     p == modulus 101; x == polynomial (0, 1);
     F == polynomial ((-x^2 - x^4) mod p, (2 + 2*x^2) mod p,
                          polynomial (-1) mod p,
                          polynomial (-2) mod p,
                          polynomial (1) mod p)
```

$$y^4 + 99\,y^3 + 100\,y^2 + (2\,x^2 + 2)\,y + 100\,x^4 + 100\,x^2$$

```
Mmx] set_variable_name (series (@(x mod p)), 'x);
     set_variable_name (polynomial series (@(x mod p)), 'y);
     Fs == polynomial (series (@z) | z in @F)
```

$$(1 + O(x^{10}))\,y^4 + (99 + O(x^{10}))\,y^3 + (100 + O(x^{10}))\,y^2 + (2 + 2\,x^2 + O(x^{10}))\,y + 100\,x^2 + 100\,x^4 + O(x^{10})$$

```
Mmx] fs == irreducible_factorization (Fs)
```

$$((1 + O(x^{10}))\,y + 50\,x^2 + 63\,x^4 + 82\,x^6 + 26\,x^8 + O(x^{10}))\,((1 + O(x^{10}))\,y + 99 + 51\,x^2 + 38\,x^4 + 19\,x^6 + 75\,x^8 + O(x^{10}))\,((1 + O(x^{10}))\,y + 100 + 50\,x^2 + 38\,x^4 + 82\,x^6 + 75\,x^8 + O(x^{10}))\,((1 + O(x^{10}))\,y + 1 + 51\,x^2 + 63\,x^4 + 19\,x^6 + 26\,x^8 + O(x^{10}))$$

```
Mmx] Gs == factor (fs[0]) * factor (fs[1])
```

$$(1+O(x^{10}))\,y^2+(99+O(x^{10}))\,y+x^2+O(x^{10})$$

```
Mmx] G == polynomial (Gs[i][0,4] | i in 0..#Gs)
```

$$y^2+99\,y+x^2$$

Temps polynomial

Dérivée logarithmique de la formule $F_i = \mathrm{lc}(F_i) \prod_{j=1}^{s} \mathfrak{F}_j^{\mu_{i,j}}$:

$$\frac{\frac{\partial F_i}{\partial y}}{F_i} = \sum_{j=1}^{s} \mu_{i,j} \frac{\frac{\partial \mathfrak{F}_j}{\partial y}}{\mathfrak{F}_j}, \text{ et donc } \hat{F}_i \frac{\partial F_i}{\partial y} = \sum_{j=1}^{s} \mu_{i,j} \hat{\mathfrak{F}}_j \frac{\partial \mathfrak{F}_j}{\partial y}.$$

Théorème. Belabas, van Hoeij, Klüners, Steel, 2009

Si $\sigma \geqslant d_x\,(2\,d_y - 1) + 1$, alors $\mu_1, \ldots, \mu_r$ forment la base échelonnée réduite de l'espace des solutions de

$$\left[\sum_{j=1}^{s} \ell_j \hat{\mathfrak{F}}_j \frac{\partial \mathfrak{F}_j}{\partial y} \right]_{d_x+1}^{\sigma} = 0.$$

Démonstration.

Soit $\ell_1, ..., \ell_s$ une solution. Posons $G := \left[\sum_{j=1}^{s} \ell_j \hat{\mathfrak{F}}_j \frac{\partial \mathfrak{F}_j}{\partial y} \right]_0^{d_x+1} \in \mathbb{K}[x, y]$.

Soit $R(x) := \mathrm{Res}_y\Big(F(x, y), \ell_1 \frac{\partial F}{\partial y}(x, y) - G(x, y) \Big) \in \mathbb{K}[x]$, $\deg R \leqslant d_x\,(2\,d_y - 1)$.

$$\begin{aligned} R(x) &= \mathrm{lc}(F)^{d_y-1} \prod_{j=1}^{s} \mathrm{Res}_y\Big(\mathfrak{F}_j, \ell_1 \frac{\partial F}{\partial y}(x, y) - G(x, y) \Big) \\ &= \mathrm{lc}(F)^{d_y-1} \prod_{j=1}^{s} \mathrm{Res}_y\Big(\mathfrak{F}_j, (\ell_1 - \ell_j)\, \hat{\mathfrak{F}}_j \frac{\partial \mathfrak{F}_j}{\partial y}(x, y) \Big) + O(x^\sigma) = 0 + O(x^\sigma). \end{aligned}$$

Comme $\sigma > \deg(R)$ alors $R = 0$.

Donc $\prod_{j, \ell_j = \ell_1} \mathfrak{F}_j = \gcd\Big(F, \ell_1 \frac{\partial F}{\partial y}(x, y) - G(x, y) \Big)$.

Espace des résidus

- La méthode précédente demande une remontée de Newton-Hensel à la précision $d_x\,(2\,d_y - 1) + 1$.
- L'autre méthode que nous allons présenter demande une précision $d_x + 1$.

Notation.

$\mathfrak{G}_i := \left[\hat{\mathfrak{F}}_i \frac{\partial \mathfrak{F}_i}{\partial y}\right]_0^{d_x+1}$, pour tout $i \in \{1, ..., s\}$.

$\mathbb{K}[x, y]_{k,l}$ polynômes de degré au plus k en x et au plus l en y.

$\mathcal{L}_{\mathbb{F}} := \left\{(\ell_1, ..., \ell_s) \in \mathbb{F}^s \middle| \sum_{i=1}^s \ell_i\,\mathfrak{G}_i \in \left\langle \hat{F}_1 \frac{\partial F_1}{\partial y}, ..., \hat{F}_r \frac{\partial F_r}{\partial y} \right\rangle_{\mathbb{F}}\right\}$ où $\mathbb{F} \subseteq \mathbb{K}$.

Lemme.

Les vecteurs $\mu_1, ..., \mu_r$ forment la base échelonnée réduite de $\mathcal{L}_{\mathbb{F}}$.

Démonstration.

Comme $\hat{F}_i \frac{\partial F_i}{\partial y} \in \mathbb{K}[x, y]_{d_x, d_y - 1}$, on a

$$\hat{F}_i \frac{\partial F_i}{\partial y} = \left[\hat{F}_i \frac{\partial F_i}{\partial y}\right]_0^{d_x+1} = \left[\sum_{j=1}^s \mu_{i,j}\,\hat{\mathfrak{F}}_j \frac{\partial \mathfrak{F}_i}{\partial y}\right]_0^{d_x+1} = \sum_{j=1}^s \mu_{i,j}\,\mathfrak{G}_j \Longrightarrow \mu_i \in \mathcal{L}_{\mathbb{F}}.$$

La conclusion provient de l'égalité des dimensions.

Notation.

$G := \sum_{i=1}^{s} \ell_i \, \mathfrak{G}_i$, $\quad \frac{G}{F} = \sum_{i=1}^{d_y} \frac{\rho_i}{y - \phi_i}$, avec $\phi_i, \rho_i \in \bar{\mathbb{K}}[[x]]$.

Lemme.

Si $(\ell_1, ..., \ell_s) \in \mathcal{L}_{\mathbb{F}}$, alors $\rho_1, ..., \rho_{d_y}$ appartiennent tous à $\mathbb{F}$.

Réciproquement, si $\rho_1, ..., \rho_{d_y}$ appartiennent tous à $\bar{\mathbb{K}}$, alors $(\ell_1, ..., \ell_s) \in \mathcal{L}_{\mathbb{F}}$.

Démonstration.

Si $(\ell_1, ..., \ell_s) \in \mathcal{L}_{\mathbb{F}}$ alors G est une combinaison linéaire sur $\mathbb{F}$ des $\hat{F}_i \frac{\partial F_i}{\partial y}$.

Supposons que tous les ρ_i soient dans $\bar{\mathbb{K}}$.

$$\frac{G(0,y)}{F(0,y)} = \sum_{i=1}^{d_y} \frac{\rho_i(0)}{y - \phi_i(0)} = \sum_{j=1}^{s} \ell_j \frac{\frac{\partial \mathfrak{F}_j}{\partial y}(0,y)}{\mathfrak{F}_j(0,y)}$$

L'hypothèse (N) implique $\rho_i = \rho_i(0) = \ell_j$ dès que $\mathfrak{F}_j(0, \phi_i(0)) = 0$, d'où $G = \sum_{j=1}^{s} \ell_j \hat{\mathfrak{F}}_i \frac{\partial \mathfrak{F}_i}{\partial y}$.

Caractéristique zéro ou suffisamment grande

$$\begin{aligned}
\mathsf{D}: \quad & \mathbb{K}[x,y]_{d_x,d_y-1} \to \mathbb{K}[x,y]_{3d_x-1,3d_y-3} \\
& G \mapsto \left(\frac{\partial G}{\partial x}\frac{\partial F}{\partial y} - \frac{\partial G}{\partial y}\frac{\partial F}{\partial x}\right)\frac{\partial F}{\partial y} - \left(\frac{\partial^2 F}{\partial x\, y}\frac{\partial F}{\partial y} - \frac{\partial^2 F}{\partial y^2}\frac{\partial F}{\partial x}\right) G, \\
\mathsf{D}_{\mathbb{F}}: \quad & \mathbb{F}^s \to \mathbb{K}[x,y]_{d_x-1,2d_y-3} \times \mathbb{K}[x,y]_{3d_x-1,d_y-1} \\
& (\ell_1,\ldots,\ell_s) \mapsto \mathsf{D}\left(\sum_{i=1}^{s} \ell_i\, \mathfrak{G}_i\right).
\end{aligned}$$

Proposition.

Nous avons $\langle \mu_1, \ldots, \mu_r \rangle_{\mathbb{F}} \subseteq \ker(\mathsf{D}_{\mathbb{F}})$. Réciproquement, si $(\ell_1, \ldots, \ell_s)$ appartient à $\ker(\mathsf{D}_{\mathbb{F}})$ alors $\rho_1, \ldots, \rho_{d_y}$ appartiennent à $\bar{\mathbb{K}}[[x^p]]$. De plus, si $p = 0$ ou $p \geqslant d_x\,(2\,d_y - 1) + 1$ alors $\mu_1, \ldots, \mu_r$ est la base échelonnée réduite de $\ker(\mathsf{D}_{\mathbb{F}})$.

Démonstration.

$$\rho_i = \frac{G(x,\phi_i)}{\frac{\partial F}{\partial y}(x,\phi_i)} \Longrightarrow \rho_i' =$$

$$\frac{\left(\frac{\partial G}{\partial x}(x,\phi_i) + \Phi_i' \frac{\partial G}{\partial y}(x,\phi_i)\right)\frac{\partial F}{\partial y}(x,\phi_i) - \left(\frac{\partial^2 F}{\partial y^2}(x,\phi_i) + \phi_i' \frac{\partial^2 F}{\partial x\, y}(x,\phi_i)\right) G(x,\phi_i)}{\left(\frac{\partial F}{\partial y}(x,\phi_i)\right)^2}$$

Par ailleurs, $\phi_i' = -\frac{\partial F}{\partial x}(x,\phi_i) / \frac{\partial F}{\partial y}(x,\phi_i)$.

Résultats de complexité

Théorème. Lecerf, 2010

Si $\mathbb{K}$ contient au moins $2\,d_x\,d_y + d_x + 1$ éléments, alors la factorisation irréductible dans $\mathbb{K}[x,y]$ se réduit à une variable sur $\mathbb{K}$ en degré borné par $d_x + d_y$, plus

a) $O(d_x\,d_y^\omega)$ opérations arithmétiques dans $\mathbb{K}$, si $p = 0$ ou $p \geqslant d_x\,(2\,d_y - 1) + 1$;

b) $\tilde{O}(k\,d_x\,d_y^\omega)$ opérations arithmétiques dans $\mathbb{F}_p$, si $\mathbb{K} := \mathbb{F}_{p^k}$.

Théorème. Lecerf, 2010

Si $\mathbb{K}$ contient au moins $10\,d_x\,d_y$ éléments, alors la factorisation irréductible dans $\mathbb{K}[x,y]$ se réduit à une variable sur $\mathbb{K}$ en degré borné par $d_x + d_y$, plus

a) $O((d_x\,d_y)^{1,5})$ opérations en moyenne dans $\mathbb{K}$, si $p = 0$ ou $p \geqslant d_x\,(2\,d_y - 1) + 1$;

b) $\tilde{O}(k\,(d_x\,d_y)^{1,5})$ opérations en moyenne dans $\mathbb{F}_p$, si $\mathbb{K} := \mathbb{F}_{p^k}$.

Problème ouvert 5. Est-il possible d'améliorer l'exposant $1,5$ du théorème précédent ?

Petite cardinalité positive

Si $\mathbb{F}_q$ est trop petit pour appliquer les résultats précédents alors on peut construire $\mathbb{F}_{q^l}$ sous la forme $\mathbb{F}_q[z]/(\mu(z))$, avec μ irréductible de degré l.

Notons α une racine de μ dans $\mathbb{F}_{q^l}$.

En prenant $l \in O(\log_q(d_x\, d_y))$ suffisamment grand pour pouvoir factoriser F dans $\mathbb{F}_{q^l}[x]$ avec les algorithmes précédents, nous pouvons obtenir les facteurs irréductibles $\mathcal{F}_1, ..., \mathcal{F}_t$ de F dans $\mathbb{F}_{q^l}[x]$.

En prenant les préimages des coefficients des $\mathcal{F}_i$ dans $\mathbb{F}_q[z]$, nous construisons des polynômes $\mathsf{F}_i(x, y, z)$ de degré au plus $l-1$ en z, tels que $\mathcal{F}_i(x, y) = \mathsf{F}_i(x, y, \alpha)$.

Pour chaque $i \in \{1, ..., t\}$, nous pouvons calculer $F_i(x, y) := \mathrm{Res}_z(\mathsf{F}_i(x, y, z), \mu(z))$ qui est un facteur irréductible de F.

Chaque F_i peut être obtenu par évaluation/interpolation rapide en temps $\tilde{O}(\deg_x(F_i) \deg_y(F_i)\, l)$ opérations dans $\mathbb{F}_{q^l}$.

Au final le surcoût total reste un facteur borné par $\log^{O(1)}(d_x\, d_y)$.

Notes

- Remontée de Hensel et recherche exhaustive : Musser (1973), Wang & Rothschild (1975), Wang (1978), von zur Gathen (1984), Bernardin (1999), Shuhong Gao & Lauder (2000).
- Premiers algorithmes en temps polynomial : Kaltofen (1982), puis Lenstra, Kannan, Lovász, Chistov, Grigoriev, von zur Gathen.
- Premier algorithme en temps essentiellement quadratique : Gao (2003), Belabas & Klüners & Steel (2004).
- Premier algorithme en temps sous-quadratique : Bostan, Lecerf, Salvy, Schost, Wiebelt (2004).
- Remontée de Hensel et recombinaison en précision essentiellement optimale : Lecerf (2006).

Chapitre 6.

Polynômes à plusieurs variables

Réduction à une variable

Notation.

$$F \in \mathbb{K}[z_1, ..., z_n, y] \text{ tel que } (N) \begin{cases} \deg\left(F(0, ..., 0, y)\right) = d_y, \\ \mathrm{Res}\left(F(0, ..., 0, y), \frac{\partial F}{\partial y}(0, ..., 0, y)\right) \neq 0, \\ F \text{ est primitif vu dans } \mathbb{K}[z_1, ..., z_n][y]. \end{cases}$$

Algorithme

1. Factoriser le polynôme $F(0, ..., 0, y)$.
2. Remonter les facteurs de sorte à obtenir la factorisation de F dans $\mathbb{K}[[z_1, ..., z_n]][y]$ à la precision $(z_1, ..., z_n)^{d_z+1}$, où $\mathbb{K}[[z_1, ..., z_n]]$ représente l'algèbre des séries à n variables, et d_z est le degré total de F en les seules variables $z_1, ..., z_n$.
3. Résoudre le problème de recombinaison pour trouver les facteurs rationnels de F.

- Les méthodes du chapitre précédent peuvent se généraliser.
- La taille du système linéaire croît avec le nombre de monômes.

Points de Hilbert

Pour réduire la taille du système linéaire, de façon probabiliste nous pouvons procéder comme suit.

Définition.

Sous l'hypothèse (N), un point $(\alpha_1, ..., \alpha_n) \in \mathbb{K}^n$ est dit de Hilbert si, pour tout facteur irréductible F_i de F, le polynôme $F_i(\alpha_1 x, ..., \alpha_n x, y)$ est irréductible.

Lemme.

Sous l'hypothèse (N), si F est irréductible, alors $F(a_1 x, ..., a_n x, y)$ est irréductible dans $\mathbb{K}(a_1, ..., a_n)[x, y]$.

Démonstration.

Posons $G(a_1, ..., a_n, x, y) := F(a_1 x, ..., a_n x, y)$.
Il suffit de prouver que G est irréductible dans $\mathbb{K}[a_1, ..., a_n, x, y]$.
Les facteurs irréductibles $\mathfrak{F}_1, ..., \mathfrak{F}_s$ de F dans $\mathbb{K}[[z_1, ..., z_n]][y]$ sont en bijection avec ceux de G dans $\mathbb{K}(a_1, ..., a_n)[[x]][y]$ notés $\mathfrak{G}_1, ..., \mathfrak{G}_s$:

$\mathfrak{G}_i(x, y) = \mathfrak{F}_i(a_1 x, ..., a_n x, y)$.

Tout facteur irréductible de G dans $\mathbb{K}[a_1, ..., a_n, x, y]$ est nécessairement de la forme $H(a_1 x, ..., a_n x, y)$ avec $H \in \mathbb{K}[z_1, ..., z_n, y]$.
En remplaçant x par 1, le polynôme $H(a_1, ..., a_n, y)$ est un facteur de F.

Localisation des points de Hilbert

Théorème. Lecerf, 2013

Sous l'hypothèse (N), il existe un polynôme de $\mathbb{K}[a_1, ..., a_n] \setminus \{0\}$ de degré au plus $d_z\,(d_y - 1)\,(2\,d_y - 1)$ qui s'annule sur tout $\mathcal{H}(F)$.

Démonstration.

Il suffit de prouver le résultat en supposant F irréductible.
Supposons d'abord que $\alpha_1, ..., \alpha_n$ soient des indéterminées.
Alors $H(x,\, y) := F(\alpha_1\, x,\, ...,\, \alpha_n\, x,\, y) \in \mathbb{K}(\alpha_1,\, ...,\, \alpha_n)[x,\, y]$ est irréductible par le lemme précédent.
Notons $\mathfrak{H}_1(x, y), ..., \mathfrak{H}_s(x, y)$ les facteurs analytiques de H dans $\mathbb{K}(\alpha_1, ..., \alpha_n)[[x]][y]$.
En posant $\hat{\mathfrak{H}}_i := H/\mathfrak{H}_i$, et $\sigma := d_x\,(2\,d_y - 1) + 1$, le système linéaire suivant en les inconnues $\ell_1, ..., \ell_s$ a pour rang $s - 1$:

$$\left[\sum_{j=1}^{s} \ell_j\, \hat{\mathfrak{H}}_j\, \frac{\partial \mathfrak{H}_j}{\partial y}\right]_{d_x+1}^{\sigma} = 0.$$

Il existe par conséquent un mineur non nul $A \in \mathbb{K}[a_1, ..., a_n]$ de taille $s - 1$.
Si maintenant $\alpha_1, ..., \alpha_n$ sont des valeurs dans $\mathbb{K}$ telles que $A(\alpha_1, ..., \alpha_n) \neq 0$ alors les mêmes calculs restent valables et le système linéaire ainsi spécialisé reste de rang $s - 1$.
Pour chaque $j \geqslant 0$ et $k \geqslant 0$, le coefficient de $x^j\, y^k$ dans $\hat{\mathfrak{H}}_l\, \frac{\partial \mathfrak{H}_l}{\partial y}$ est un polynôme de degré au plus j. Le degré total de A est donc au plus $(s - 1)\, d_z\, (2\, d_y - 1)$.

Proportion des points de Hilbert

Corollaire.

Sous l'hypothèse (N), en notant p la caractéristique de $\mathbb{K}$, pour n'importe quel sous-ensemble non vide S de $\mathbb{K}$, nous avons les inégalités suivantes :

- $\dfrac{|\mathcal{H}(F)\cap S^n|}{|S|^n} \leqslant \dfrac{3\,d_z\,d_y}{|S|}$ si $p=0$ ou $p \geqslant d_z\,(2\,d_y-1)+1$,
- $\dfrac{|\mathcal{H}(F)\cap S^n|}{|S|^n} \leqslant \dfrac{d_z\,d_y \min\,(2\,d_y, p)}{|S|}$ si $p>0$.

Démonstration.

On utilise le lemme de Schwarz-Zippel.

Problème ouvert 6. Peut-on avoir une borne en $O(d_z\,d_y/|S|)$ dans tous les cas ?

Réduction à deux variables

Algorithme

Entrée. F satisfaisant l'hypothèse (N) et $(\alpha_1, ..., \alpha_n) \in \mathbb{K}^n$ un point de Hilbert pour F.

Sortie. les facteurs irréductibles $F_1, ..., F_r$ de F.

1. Calculer les facteurs irréductibles $H_1(x, y), ..., H_r(x, y)$ de $H(x, y) := F(\alpha_1\, x, ..., \alpha_n\, x, y)$.
2. Utiliser la remontée de Newton-Hensel pour calculer la factorisation de F.

Notation.

Supposons que, pour toutes les valeurs d et n, nous disposions d'arbres de calcul effectuant les additions et soustractions dans $\mathbb{K}[[z_1, ..., z_n]]/(z_1, ..., z_n)^d$ en temps linéaire, ainsi que le produit en temps au plus $\mathsf{S}(d, n)$.

Pour des raisons techniques nous supposons que S est super-additive en d, c'est à dire $\mathsf{S}(d_1, n) + \mathsf{S}(d_2, n) \leqslant \mathsf{S}(d_1 + d_2, n)$.

Résultats de complexité

Sous l'hypothèse (N), si $(\alpha_1, ..., \alpha_n)$ est un point de Hilbert pour F, alors l'algorithme effectue :

- la factorisation d'un polynôme à deux variables de degrés partiels d_z et d_y ;
- la remontée de Newton-Hensel peut se faire jusqu'en précision d_z au moyen de $O(\mathsf{S}(d_z, n)\,\mathsf{M}(d_y)\log d_y)$.

Théoreme. Lecerf, 2007

Si l'on dispose d'un produit de séries à plusieurs variables en temps quasi-linéaire, alors la réduction à deux variables est quasi-linéaire moyen à partir de 3 variables.

Théorème de Bertini-Hilbert

Pour tout triplet de points $(\alpha_1, ..., \alpha_n)$, $(\beta_1, ..., \beta_n)$ et $(\gamma_1, ..., \gamma_n)$ de $\mathbb{K}^n$, nous définissons le polynômes à deux variables x et y suivant :

$$P_{\alpha,\beta,\gamma} := P(\alpha_1\, x + \beta_1\, y + \gamma_1, ..., \alpha_n\, x + \beta_n\, y + \gamma_n).$$

Théorème. Bertini

Si P est irréductible, alors il existe un ouvert de Zariski de $(\mathbb{K}^n)^3$ tel que $P_{\alpha,\beta,\gamma}$ est irréductible pour chaque triplet $(\alpha_1, ..., \alpha_n), (\beta_1, ..., \beta_n), (\gamma_1, ..., \gamma_n)$ dans cet ouvert.

Définition.

Un triplet $(\alpha_1, ..., \alpha_n)$, $(\beta_1, ..., \beta_n)$ et $(\gamma_1, ..., \gamma_n)$ de $\mathbb{K}^n$ est un point de Bertini pour P si, pour tout facteur irréductible Q de P, le polynôme $Q(\alpha_1\, x + \beta_1\, y + \gamma_1, ..., \alpha_n\, x + \beta_n\, y + \gamma_n)$ est irréductible de même degré total que Q.

Théorème. Lecerf, 2008–2013

Soit S un sous-ensemble fini de $\mathbb{K}$. Si $P \in \mathbb{K}[v_1, ..., v_n]$ est séparable en au moins une variable et est de degré total $d \geqslant 1$, alors la proportion $\mathsf{B}(P, S)$ de triplets à coordonnées dans S qui ne sont pas des points de Bertini pour P est au plus

- $5\, d^2/|S|$ si la caractéristique p de $\mathbb{K}$ est nulle ou au moins $d\,(2\, d - 1) + 1$,
- $d^2 \min(2\, d, p + 1)/|S|$ si $p > 0$.

Notes historiques

Résultats quantitatifs sur Bertini-Hilbert. – en degré total d.

- Hilbert (1892) : le densité des points qui ne sont pas de Bertini tend vers 0 lorsque $|S| \to \infty$.
- Heintz & Sieveking (1981), Kaltofen (1982): première utilisation en calcul formel.
- von zur Gathen (1985): $9^{d^2}/|S|$.
- Bajaj, Canny, Garrity & Warren (1993): $d^4/|S|$ lorsque $\mathbb{K} = \mathbb{C}$.
- Kaltofen (1995): $2d^4/|S|$ lorsque $\mathbb{K}$ est parfait.
- Shuhong Gao (2003): $2d^3/|S|$ lorsque $p = 0$ ou $p \geq 2d^2$.
- Lecerf (2007): $\frac{23}{8}d^2/|S|$ lorsque $p = 0$ ou $p \geq d(d-1)+1$.

Représentation creuse

Une représentation creuse des polynômes de $\mathbb{K}[x_1, ..., x_n]$ consiste à stocker ceux-ci sous la forme d'une liste de termes non nuls.

Définition 7.

Le support d'un polynôme $F \in \mathbb{K}[x_1, ..., x_n]$, noté $\mathrm{supp}(F)$, est l'ensemble des exposants de ses monômes non nuls.

Si $F = \sum_{e \in \mathbb{N}^n} F_e \, x_1^{e_1} \cdots x_n^{e_n}$, alors $\mathrm{supp}(F) = \{e \in \mathbb{N}^n \mid F_e \neq 0\}$.

Définition 8.

La somme de Minkowski de deux sous-ensembles Q et R de $\mathbb{R}^n$, notée $Q + R$, est définie par $Q + R := \{e + f \mid (e, f) \in Q \times R\}$.

Définition 9.

Le polytope de Newton de $F \in \mathbb{K}[x_1, ..., x_n]$, noté $N(f)$, est l'enveloppe convexe dans $\mathbb{R}^n$ de $\mathrm{supp}(F)$. L'enveloppe convexe entière de F est l'ensemble des points de $\mathbb{Z}^n$ contenus dans $N(F)$.

Théorème. Ostrowski

Si F se factorise en $G\,H$ alors $N(F) = N(G) + N(H)$.

Support dense dans le polytope de Newton

Théorème. Berthomieu, Lecerf, 2012

Si S est un sous-ensemble fini normalisé de $\mathbb{Z}^2$ de cardinal σ, de taille convexe π, et inclus dans $[0, d_x] \times [0, d_y]$, alors nous pouvons calculer une application $U \in \mathrm{Aff}(\mathbb{Z}^2)$, ainsi que $U(S)$, tels que $U(S)$ est normalisé et contenu dans $[0, d'_x] \times [0, d'_y]$ avec $(d'_x + 1)\,(d'_y + 1) \leqslant 9\,\pi$, en utilisant $O(\sigma \log^2((d_x + 1)\,(d_y + 1)))$ opérations binaires.

Pour factoriser un polynôme on peut alors :

1. Calculer U comme dans le théorème.
2. Appliquer le changement de variables de U à F pour obtenir F^U.
3. Factoriser F^U en $F_1^U, \ldots, F_r^U$.
4. Appliquer U^{-1} aux F_i^U.

Polynômes lacunaires

Exemple. Si p est premier alors $F := x^p - 1 \in \mathbb{Q}[x]$ est composé de seulement deux monômes mais ses facteurs irréductibles sont $x - 1$ et $(x^p - 1)/x - 1$. Ce dernier est composé de p monômes.

Le calcul de facteurs de « petits degrés » fixés de polynômes à coefficients dans $\mathbb{Q}$ peut se faire en temps polynomial dans la taille binaire creuse (c'est à dire le total des tailles des coefficients et des exposants).

- H. W. Lenstra, Jr. (1997)
- Kaltofen & Koiran (2006)
- M. Avendaño & T. Krick & M. Sombra (2007)
- Leroux (2011)

Théorème. Kaltofen, Koiran, 2005

Supposons que nous disposions d'un algorithme de type Monte Carlo pour tester l'irréductibilité des polynômes de $\mathbb{F}_{2^m}[x, y]$ en temps polynomial en la taille binaire creuse, pour m au voisinage de l'infini. Alors il serait possible de factoriser les entiers en temps polynomial avec un algorithme de type Las Vegas.

Fin