Factorisation bivariée convexe-dense

Martin Weimann

7 février 2025

Séminaire de Théorie des Nombres de Bordeaux

1. Motivations, résultats, exemples.

2. Factorisation dans $\mathbb{K}((x))[y]$ relative à une valuation augmentée.

3. Application à la factorisation bivariée convexe-dense.

1. Motivations, résultats, exemples.

Factorisation dense

- $f \in \mathbb{K}[x,y]$ de degré total d ($\mathbb{K}$ un corps effectif)
- Taille de l'entrée $\approx d^2$
- $O(d^\omega) =$ coût de la multiplication dans $\mathcal{M}_d(\mathbb{K})$ $(2 \leq \omega \leq 3)$

Théorème (Lecerf, 2007)

Factorisation déterministe dans $\mathbb{K}[x,y]$ en $\tilde{O}(d^{\omega+1})$ plus une facto univariée de degré d.

Lifting et recombinaisons :

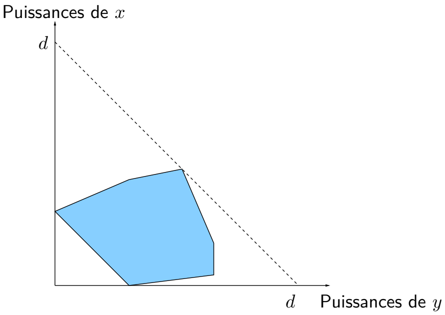
- Réduction au cas $f(0,y)$ séparable degré d (changement de coordonnées)
- Factorisation de $f(0,y)$ (factorisation univariée)
- Factorisation de $f \mod (x^{2d})$ (lemme de Hensel)
- Recombinaisons des facteurs modulaires (algèbre linéaire)

Polygone de Newton

Définition

Le polygone de Newton de $f = \sum c_{ij} x^j y^i \in \mathbb{K}[x,y]$ est l'enveloppe convexe de son support :

$$\mathrm{N}_f = \mathrm{Conv}((i,j) \in \mathbb{N}^2,\ c_{ij} \neq 0).$$



Taille de l'entrée (formule de Pick):

$$\boxed{\mathrm{Card}(N_f \cap \mathbb{Z}^2) \approx \mathrm{Vol}(N_f)}$$

Meilleur indicateur de complexité.

Factorisation convexe-dense

Théorème (Berthomieux et Lecerf, 2011)

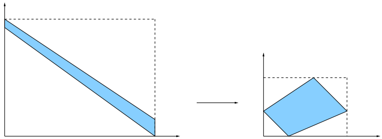
Suppose $V = \mathrm{Vol}(N_f) > 0$. Factorisation déterministe dans $\mathbb{K}[x,y]$ de complexité

$$\tilde{O}(V^{\frac{\omega+1}{2}}) \subset \tilde{O}(d^{\omega+1})$$

plus une facto univariée de degré $O(V^{\frac{1}{2}}) \subset O(d)$.

- Calcule $\tau \in \mathrm{Aut}(\mathbb{Z}^2)$ tel que le "rectangle englobant" $R \supset \tau(N_f)$ vérifie

$$\boxed{\mathrm{Vol}(R) = \mathcal{O}(V)} \qquad (V \text{ est invariant par } \mathrm{Aut}(\mathbb{Z}^2))$$



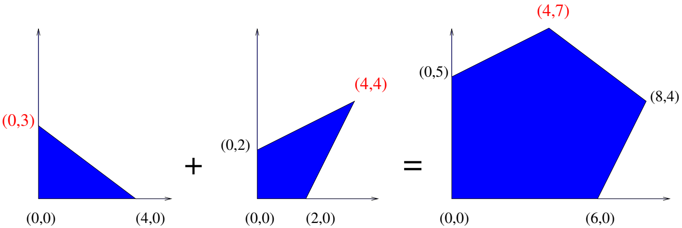
- Factorise $\tau(f)$ avec un algorithme dense et déduit la factorisation de f.

Fin de l'histoire ?

Théorème d'Ostrowski

- $g = 1 - 2x^4 + \mathbf{y^3} - xy$
- $h = 3 - x^2 + xy^2 - 2\mathbf{x^4 y^4} + y^2$
- $gh = 3 + 2x^6 + 4x^8y^4 - 2\mathbf{x^4 y^7} + y^5 + \cdots$

$$\boxed{\mathrm{N}_{gh} = \mathrm{N}_g + \mathrm{N}_h}$$



L'approche convexe-dense classique ne profite pas de ces contraintes combinatoires...

Longueur entière inférieure.

- $\Lambda = \Lambda(f)$ le **bord inférieur** de N_f.
- Longueur entière (inférieure) :

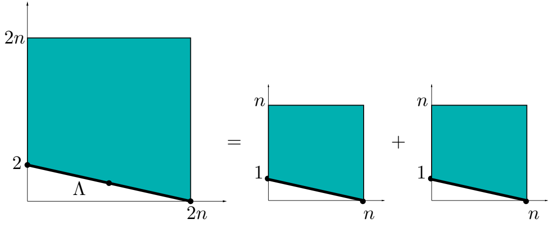
$$\boxed{r(f) := \mathrm{Card}(\Lambda \cap \mathbb{Z}^2) - 1}$$

$$\boxed{\Lambda(gh) = \Lambda(g) + \Lambda(h)}$$

$$\Downarrow$$

$$\boxed{r(gh) = r(g) + r(h)}$$

- $\boldsymbol{r(f)}$ **majore le nombre de facteurs irréductibles de** $\boldsymbol{f}$ **dans** $\mathbb{K}((x))[y]$**.**



$$r(f) = 2$$

$$\Downarrow$$

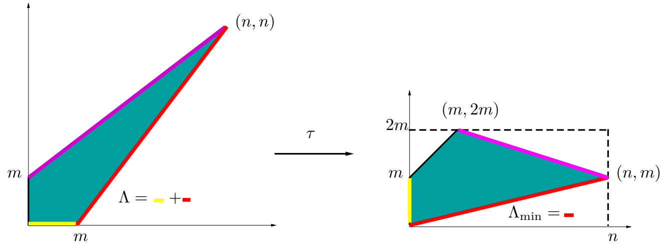
Au plus deux facteurs !

Longueur entière minimale.

- L'action de $\mathrm{Aut}(\mathbb{Z}^2)$ préserve le volume et la longueur entière des arêtes.

$$r_0(f) := \min(r(\tau(f)),\, \tau \in \mathrm{Aut}(\mathbb{Z}^2))$$

$$r_0(f) \le r(f) \le d$$



$r(f) = m + \gcd(m, n)$ $\qquad$ $r_0(f) = \gcd(m, n)$

- **Majore le nombre de facteurs irréductibles de volume positif**
- **Tient compte du théorème d'Ostrowski.**
- **Facile à calculer (W. 2024).**

Résultat principal

- Pour chaque arête $E \subset \Lambda$, on note $f_E = \sum_{(i,j)\in E\cap\mathbb{Z}^2} c_{ij}x^j y^i$
- f_E est un polynôme **quasi-homogène**.

Définition

- *f est **non dégénéré** si $y^{-\operatorname{ord}_y(f_E)} f_E \in \mathbb{K}(x)[y]$ est séparable pour tout $E \subset \Lambda$.*
- *f est **minimalement non dégénéré** s'il existe $\tau \in \operatorname{Aut}(\mathbb{Z}^2)$ tel que $r(\tau(f)) = r_0(f)$ et tel que $\tau(f)$ est non dégénéré.*

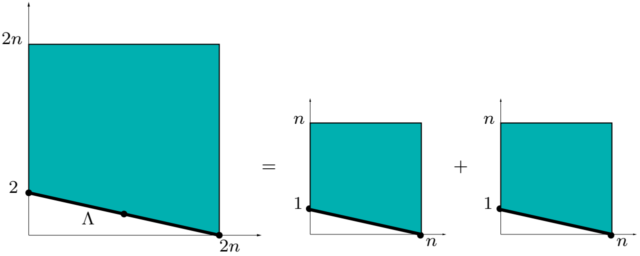
Théorème (W. 2024)

Soit $f \in \mathbb{K}[x,y]$ minimalement non dégénéré. Factorisation déterministe de complexité

$$\tilde{O}(V\, r_0^{\omega-1}) \subset \tilde{O}(V^{\frac{\omega+1}{2}})$$

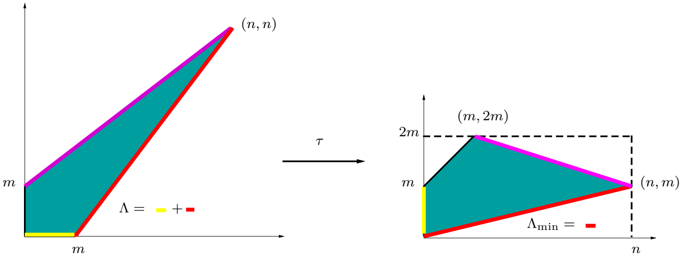
*plus des facto univariées de degré total r_0. **Complexité quasi-lineaire si $r_0 = \mathcal{O}(1)$**.*

Exemple 1



- Algo denses ou convexe-denses : $\tilde{\mathcal{O}}(n^{\omega+1})$ et une facto univariée degré $2n$.
- Nouvel algo (si f non dégénéré) : $\tilde{\mathcal{O}}(n^2)$ et une facto univariée degré 2.

Exemple 2



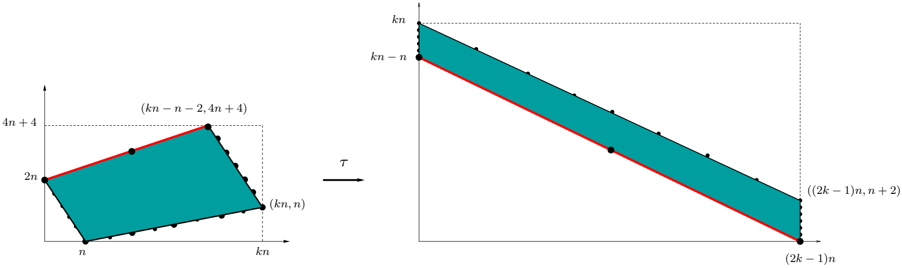
$r(f) = m + \gcd(m, n)$ $\qquad$ $r_0(f) = \gcd(m, n)$

- Algo dense : $\tilde{O}(n^{\omega+1})$ et une facto univariée degré n.
- Algo convexe-dense : $\tilde{O}(Vm^{\omega-1})$ et une facto univariée degré $2m$, où $V = nm$.
- Nouvel algo : $\tilde{O}(Vg^{\omega-1})$ et une facto univariée degré g, où $\boldsymbol{g = gcd(m, n)}$.

Remarque

Il existe ici deux configurations de longueur minimale $r_0(f)$ (bord rouge ou bord violet).

Exemple 3



- Algo dense ou convexe-dense : $\tilde{O}(V^{\omega+1})$ et une facto univariée degré $O(n)$.
- Nouvel algo : $\tilde{O}(V)$ et une facto univariée degré 2.

Remarque

Minimiser la longueur entière inférieure augmente ici le volume du rectangle englobant.

Stratégie

- Déterminer τ tel que $r(\tau(f))$ minimal. Remplacer f par $\tau(f)$.
- Factoriser f dans $\mathbb{K}((x))[y]$ relativement à une **valuation augmentée** induite par N_f.
- Recombiner les facteurs analytiques en facteurs rationnels (algèbre linéaire).

2. Factorisation dans $\mathbb{K}((x))[y]$ relativement à une valuation augmentée

Valuation augmentée

- Soit $\lambda \in \mathbb{Q}$. On définit :

$$v_\lambda : \mathbb{K}((x))[y] \longrightarrow \mathbb{Q}, \qquad v_\lambda\left(\sum c_{ij}x^j y^i\right) := \min\left(j + i\lambda,\ c_{ij} \neq 0\right).$$

- L'application v_λ induit une **valuation** sur $\mathbb{K}((x))(y)$ qui étend la valuation x-adique :

$$v_\lambda(y) = \lambda$$

$$v_\lambda\left(\sum c_i(x) y^i\right) = \min\left(\mathrm{val}_x(c_i) + i\lambda,\ c_i \neq 0\right).$$

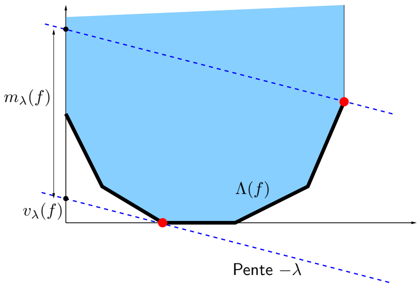
- Pour $\lambda = 0$, on obtient la **valuation de Gauss** v_0.

Le λ-défaut

- Soit $f \in \mathbb{K}((x))[y]$. Le **$\boldsymbol{\lambda}$-défaut** de f est

$$\boxed{m_\lambda(f) = \max_{(i,j)\in\Lambda(f)} (j + i\lambda) - v_\lambda(f)}$$

- On a $m_\lambda(f) \geq 0$ avec égalité si et seulement si $\Lambda(f)$ a une seule pente $-\lambda$.



$$\boxed{m_\lambda(gh) \geq \max(m_\lambda(g), m_\lambda(h))}$$

$$\boxed{m_\lambda(gh) \leq m_\lambda(g) + m_\lambda(h)}$$

Factorisation v_λ-adique

- Soit $f \in \mathbb{K}((x))[y]$ unitaire non dégénéré.
- Soit $f = f_1 \cdots f_s$ sa factorisation irréductible.

Théorème (W. 2024)

Etant donné $\sigma \geq m_\lambda(f)$, on peut calculer $f_1^*, \ldots, f_s^* \in \mathbb{K}(x)[y]$ unitaires tels que

$$v_\lambda(f - f_1^* \cdots f_s^*) - v_\lambda(f) > \sigma$$

et tels que

$$v_\lambda(f_i - f_i^*) - v_\lambda(f_i) > \sigma - m_\lambda(f)$$

en temps quasi-linéaire

$$\tilde{\mathcal{O}}(\sigma \deg(f))$$

plus des factorisations univariées dont la somme des degrés est $r(f)$.

Preuve (1)

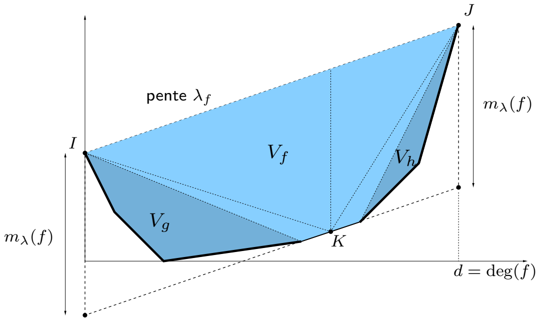
- Multiplication bivariée **convexe-dense** quasi-linéaire (Hoeven-Lebreton-Schost 2013).
- Déduit division et Hensel multifacteurs $v_{\boldsymbol{\lambda}}$**-adiques** quasi-linéaires.
- Puis algo récursif **diviser pour régner** :

Algorithme $\Big(\texttt{Facto}(f, \lambda, \sigma)\Big)$

1. *$L \leftarrow$ Hensel$(f, \lambda, \sigma + m_\lambda(f))$* *($v_\lambda$-adique, multifacteurs)*
2. *Si $\Lambda(f)$ a pour seule pente λ, retourne L.* *(facto complète car f non dégénéré)*
3. *Soit $g \in L$ de pentes $< \lambda$ et $h \in L$ de pentes $> \lambda$:*
   - (i) *Calcule les pentes moyennes λ_g, λ_h.*
   - (i) *Calcule les précisions σ_g, σ_h.*
   - (ii) *Retourne $L \setminus \{g, h\} \cup$ Facto$(g, \lambda_g, \sigma_g) \cup$ Facto(h, λ_h, σ_h).*

Preuve (2)

- $\texttt{Hensel}(f, \lambda_f, \sigma_f) = g \times h \times f_1 \times \cdots \times f_k$. **($\boldsymbol{\lambda_f}$ pente moyenne)**
- Si $V_f := \mathrm{Vol}(\Lambda(f)) = 0$, alors $g = h = 1$, c'est fini. **(une seule pente)**
- Sinon, appels récursifs sur g, h :



Pente moyenne $\implies$ $\boxed{V_g + V_h \leq \dfrac{V_f}{2}}$ $\implies$ **Diviser pour régner.** $\square$

3. Application à la factorisation convexe-dense dans $\mathbb{K}[x, y]$

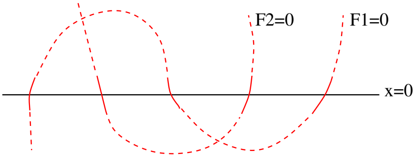
Problème des recombinaisons

- $f \in \mathbb{K}[x,y]$ séparable et unitaire en y (pour simplifier).

$$f = f_1 \cdots f_r \;\in\; \mathbb{K}[[x]][y] \qquad \xrightarrow{??} \qquad f = F_1 \cdots F_s \;\in\; \mathbb{K}[x,y]$$

- **Recombinaisons:** Trouver $v_i = (v_{ij}) \in \{0,1\}^r$ tels que

$$F_i = f_1^{v_{i1}} \cdots f_r^{v_{ir}}, \;\; i = 1, \ldots, s.$$



$$\Longrightarrow \quad \begin{cases} v_1 = (1,0,1,0,1) \\ v_2 = (0,1,0,1,0) \end{cases}$$

Algébre linéaire

- Les vecteurs v_i forment la base échelonnée réduite du sous-espace vectoriel

$$V := \langle v_1, \ldots, v_s \rangle \subset \mathbb{K}^r$$

qu'ils engendrent sur $\mathbb{K}$. On cherche les équations de $V \subset \mathbb{K}^r$.

Lemme (dérivées logarithmiques)

On note $\hat{f}_j = f/f_j$ et $\hat{F}_i = F/F_i$. Soit $\mu \in \mathbb{K}^r$. On a

$$\mu \in V \iff \sum_{i=1}^{r} \mu_i \hat{f}_i \partial_y f_i \in \left\langle \hat{F}_1 \partial_y F_1, \ldots, \hat{F}_s \partial_y F_s \right\rangle_{\mathbb{K}}.$$

- **Point clé : il suffit de considérer des troncations des $\hat{f}_i \partial_y f_i \in \mathbb{K}[[x]][y]$.**

v_λ-troncations et résidus

- Soit $\lambda \in \mathbb{Q}$. On associe à $\mu \in \mathbb{K}^r$ le polynôme v_λ-tronqué

$$\boxed{G_\mu := \sum_{i=1}^{r} \mu_i \left[\hat{f}_i \partial_y f_i\right]^{d_\lambda} \in \mathbb{K}[x,y]}$$

- La précision d_λ est donnée par le **λ-degré de f** (si $\lambda = 0$, on a $d_\lambda = \deg_x(f)$).

Proposition (Lecerf 2007, W. 2013, W. 2024)

Considérons les résidus de G_μ / f aux racines $y_1, \ldots, y_d$ de f :

$$\rho_k := \frac{G_\mu(x, y_k)}{\partial_y f(x, y_k)} \in \overline{\mathbb{K}(x)}.$$

***Si f est non dégénéré**, alors $\mu \in V$ si et seulement si $\rho_k \in \overline{\mathbb{K}}$ pour tout $k = 1, \ldots, d$.*

La matrice des recombinaisons

- Suppose $\mathrm{Char}(\mathbb{K}) = 0$. Alors $\rho_k \in \overline{\mathbb{K}}$ si et seulement si $\rho'_k = 0$. On a

$$\rho'_k(x) = \frac{H_\mu(x, y_k)}{\partial_y f(x, y_k)^3}, \qquad H_\mu \in \mathbb{K}[x, y].$$

- On a $\rho'_1 = \cdots = \rho'_d = 0$ si et seulement si f **divise** $\boldsymbol{H_\mu}$ dans $\mathbb{K}(x)[y]$.

$$\Longrightarrow \quad \textbf{Equations linéaires de } V \subset \mathbb{K}^r.$$

Proposition (W. 2024, difficultés : division v_λ-adique non unitaire, caractéristique positive)

Si f est non dégénéré, *il existe $\phi : \mathbb{K}^r \to \mathbb{K}^N$ linéaire telle que $V = \ker(\phi)$, avec*

$$N \leq 3d(d_\lambda(f) - v_\lambda(f))).$$

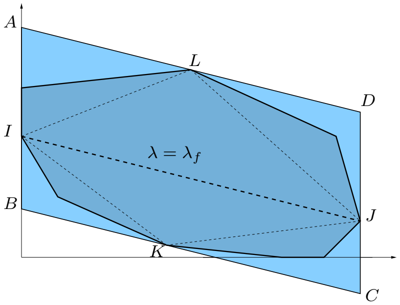
On peut calculer la matrice de ϕ en temps quasi-linéaire $\tilde{\mathcal{O}}(rN)$.

Le bon choix de λ

Lemme

Soit $V = \mathrm{Vol}(N_f)$. *Si on choisit* λ ***la pente moyenne*** *de* $\Lambda(f)$, *on a*

$$V \leq d(d_\lambda(f) - v_\lambda(f)) \leq 2V.$$



$$\boxed{d(d_\lambda(f) - v_\lambda(f)) = \mathrm{Vol}(ABCD)}$$

- I, J **points extrémaux** de $\Lambda(f)$
- $K \in N_f \cap (BC)$ et $L \in N_f \cap (AD)$

$$\boxed{\mathrm{Vol}(IKJL) \leq V \leq \mathrm{Vol}(ABCD)}$$

$\boldsymbol{\lambda}$ **pente moyenne** $\Longrightarrow$ $\boldsymbol{(IJ)//(BC)}$ $\Longrightarrow$ $\boxed{\mathrm{Vol}(ABCD) = 2\,\mathrm{Vol}(IKJL)}$

Conclusion

Algorithme

1. *Calcule $\tau \in \mathrm{Aut}(\mathbb{Z}^2)$ tel que $\tau(N_f)$ de longueur entière r minimale* *(négligeable)*
2. *Si $\tau(f)$ non dégénéré :* $\mathcal{O}(r)$
   - (i) *Factorise $\tau(f)$ dans $\mathbb{K}[[x]][y]$ à λ_f-précision $\mathcal{O}(V/d)$* $\tilde{\mathcal{O}}(V)$
   - (ii) *Recombinaisons (matrice et base réduite du noyau)* $\tilde{\mathcal{O}}(Vr) + \mathcal{O}(Vr^{\omega-1})$
   - (iii) *Déduit factorisation de $\tau(f)$, puis de f* $\tilde{\mathcal{O}}(V)$

Complexité totale : $\boxed{\tilde{\mathcal{O}}(Vr) + \mathcal{O}(Vr^{\omega-1})}$ $\square$

Remarque (cas dégénéré)

- Si $\tau(f)$ dégénéré, factorisation rapide dans $\mathbb{K}[[x]][y]$ plus délicate. (Poteaux-W. 2022)
- Et les recombinaisons peuvent nécessiter une précision $\Omega(V)$ (W. 2014)
- Autres options : changer de τ ou utiliser Berthomieux-Lecerf, en fonction de N_f.