Autour de la factorisation des polynômes

Martin Weimann

Le 14 juin 2024

LMNO, Université de Caen Normandie

- 1. Factorisation bivariée et singularités
- 2. Factorisation univariée sur les corps locaux
- 3. Factorisation bivariée et géométrie torique

Facile

$$(-2y + x^{2} - x + 3) (3xy - y + 2x + 1)$$

$$=$$

$$-6xy^{2} + 2y^{2} + 3x^{3}y - 4x^{2}y + 6xy - 5y + 2x^{3} - x^{2} + 5x + 3$$

Moins facile

$$-6xy^{2} + 2y^{2} + 3x^{3}y - 4x^{2}y + 6xy - 5y + 2x^{3} - x^{2} + 5x + 3$$

$$= (-2y + x^{2} - x + 3)(3xy - y + 2x + 1)$$

Le cas dense

• $f \in k[x,y]$ de degré total d

(k un corps effectif)

ullet $O(d^\omega)=\mathsf{coût}$ de la multiplication dans $\mathcal{M}_d(k)$

 $(2 < \omega < 3)$

• $O(d) = O(d^{1+o(1)})$

Théorème (Lecerf, 2006)

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

Lifting et recombinaisons :

ullet Réduction au cas f(0,y) séparable degré d

(changement de coordonnées)

• Factorisation de f(0, y)

(factorisation univariée)

ullet Factorisation de $f \mod (x^{2d})$

(lemme de Hensel)

Recombinaisons des facteurs modulaires.

(algèbre linéaire)

Objectif

Tenir compte d'indicateurs de complexité plus fins que le degré total.

1. Factorisation bivariée et singularités

Problème des recombinaisons

Suppose $k=\bar{k}$ pour simplifier.

$$\begin{cases} f(x,y) = F_1(x,y) \cdots F_s(x,y) \\ f(0,y) = (y-\alpha_1) \cdots (y-\alpha_d) & \text{supposé séparable.} \end{cases}$$

Recombinaisons: Cherche $\mu_i = (\mu_{ij}) \in \{0,1\}^d$ tels que

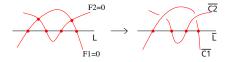
$$F_i(0,y) = \prod_{i=1}^d (y - \alpha_j)^{\mu_{ij}}, \ i = 1, \dots, s.$$



$$\implies \begin{cases} \mu_1 = (1, 0, 1, 0, 1) \\ \mu_2 = (0, 1, 0, 1, 0) \end{cases}$$

Normalisation

- ullet Facteurs de $f(x,y) \leftrightsquigarrow$ composantes C_1,\ldots,C_s de la courbe $C\subset \mathbb{P}^2$ de f.
- Facteurs de $f(0,y) \iff$ composantes de $Z=C\cap L$, où L droite de \mathbb{P}^2 .
- ullet $\pi:\overline{C} o C$ normalisation
- $\overline{Z} = \pi^{-1}Z \simeq Z.$



$$H^0(\mathcal{O}_{\overline{C}}) \simeq H^0(\mathcal{O}_{\overline{C}_1}) \oplus \cdots \oplus H^0(\mathcal{O}_{\overline{C}_s}) \simeq k^s$$

$$H^0(\mathcal{O}_{\overline{Z}}) \quad \simeq \quad H^0(\mathcal{O}_{\{p_1\}}) \oplus \cdots \oplus H^0(\mathcal{O}_{\{p_d\}}) \quad \simeq \quad k^d$$

Lemme

 (μ_1,\ldots,μ_s) est la base échelonnée réduite de l'image du morphisme de restriction

$$H^0(\mathcal{O}_{\overline{C}}) \stackrel{r}{\longrightarrow} H^0(\mathcal{O}_{\overline{Z}})$$

Faisceau dualisant et résidus

Proposition (W 2013)

On a une suite exacte

$$0 \longrightarrow H^0(\mathcal{O}_{\overline{C}}) \stackrel{r}{\longrightarrow} H^0(\mathcal{O}_{\overline{Z}}) \stackrel{R}{\longrightarrow} H^0(\Omega_{\overline{C}}(\overline{Z}))^{\vee} \longrightarrow H^0(\Omega_{\overline{C}})^{\vee} \longrightarrow 0$$

où
$$R(\lambda_1,\ldots,\lambda_d):\omega\mapsto\sum_{i=1}^n\operatorname{res}_{p_i}(\lambda_i\omega).$$

Preuve

Dualité de Serre, formule d'adjonction, théorème des résidus.

Corollaire

Etant donnée une k-base de $H^0(\Omega_{\overline{C}}(\overline{Z})) \, / \, H^0(\Omega_{\overline{C}})$, on factorise f sur k en $O(d^\omega)$.

Exemple:
$$f(x,y) = y^5 - xy^3 - xy^2 - 3y^3 + 2xy + x^2 - 2y$$

- f(0,y) = (y-2)(y-1)y(y+1)(y+2).
- On calcule $H^0(\Omega_{\overline{C}}(\overline{Z})) \, / \, H^0(\Omega_{\overline{C}}) \simeq \langle y, y^2 1, y^3 \rangle_k$. Donc s = 2.

On obtient

$$R = \frac{1}{24} \begin{pmatrix} 2 & -4 & 0 & 4 & -2 \\ 3 & 0 & -6 & 0 & 3 \\ -8 & -4 & 0 & 4 & 8 \end{pmatrix} \quad \Rightarrow \quad ker(R) = \langle (1,0,1,0,1), (0,1,0,1,0) \rangle.$$

D'où $f=F_1F_2$ avec :

- $F_1(0,y) = (y-2)y(y+2)$
- $F_2(0,y) = (y-1)(y+1)$.



Y a plus qu'à...

$$f(0,y) = F_1(0,y) \times F_2(0,y) \stackrel{\text{Hensel}}{\Longrightarrow} f(x,y) = (y^3 - 4y - x)(y^2 - 1 - x).$$

Clôture intégrale et conducteur

- ullet $\mathcal{C}\subset\mathbb{A}^2$ la courbe affine de f, supposée réduite.
- $k[\mathcal{C}] = k[x,y]/(f)$ l'anneau de fonctions et $k(\mathcal{C})$ l'anneau des fractions.
- ullet $\overline{k[\mathcal{C}]}$ la clôture intégrale de $k[\mathcal{C}]$ dans $k(\mathcal{C})$.

(normalisation affine)

Lemme

Supposons f séparable, unitaire de degré d en y. Le **conducteur**

$$\mathcal{I} := \{ g \in k[\mathcal{C}], \ g \, \overline{k[\mathcal{C}]} \, \subset \, k[\mathcal{C}] \}$$

est un k[x]-module libre de rang d (idéal de $\overline{k[C]}$).

Conducteur et factorisation

Définition

On dit qu'une k[x]-base (g_1, \ldots, g_d) de \mathcal{I} est **réduite** (pour le degré total) si

$$deg(\sum \lambda_i g_i) = \max deg(\lambda_i g_i) \quad \forall \ \lambda_i \in k[x].$$

Proposition (W. 2024, d'après Böhm et al. 2015 + Bauch 2015)

Considérons $L = \mathbb{P}^2 \setminus \mathbb{A}^2$ (recombinaisons à l'infini) et supposons $\operatorname{Sing}(C) \subset \mathbb{A}^2$.

Soit (q_1, \ldots, q_d) une base réduite de \mathcal{I} . Alors

$$\forall n \in \mathbb{N}, \qquad H^0(\Omega_{\overline{C}}(n\overline{Z})) = \langle g_i x^j, \deg(g_i x^j) \le d - 3 + n \rangle_k.$$

Corollaire

Calcul d'une k[x]-base réduite du conducteur $\stackrel{O(d^\omega)}{\Longrightarrow}$



Factorisation de f.

Calcul de la clôture intégrale

Delta-invariant

$$\Delta(C) = p_a(C) - g(C) = \frac{(d-1)(d-2)}{2} - g(C),$$

 $\Delta(C) = 0 \iff C \text{ lisse.}$

- ullet Coût du calcul du radical de $\mathrm{Disc}_y(f)$:
 - ightharpoonup D(d) $\subset O^{\sim}(d^3)$

(algorithme déterministe)

ightharpoonup $\mathrm{D}(d)\subset O^{\widetilde{}}(d^2)$ si $k=\mathbb{F}_q$

(algo probabiliste, Villard 2023)

Théorème (Poteaux-W. 2024)

Supposons $\operatorname{Car}(k)=0$ ou $\operatorname{Car}(k)>d$. On calcule en

$$\mathrm{D}(d) + O^{\widehat{\ }}(d\Delta) \subset O^{\widehat{\ }}(d^3)$$

une k[x]-base triangulaire de la clôture intégrale $\overline{k[\mathcal{C}]}$ (normalisation affine).

Preuve : stratégie locale-globale

$$\textbf{Notations}: \quad A = k[x] \quad \text{ et } \quad B = \overline{k[\mathcal{C}]}.$$

- Pour chaque $p \mid \operatorname{Disc}_y(f)$:
 - Factorisation rapide de $f\in \hat{A}_p[y]$ à précision p-adique optimale (Montes 2000 + Poteaux-W. 2022)
 - lacktriangle Déduit une A_p -base triangulaire de $B\otimes A_p$ (Okutsu 1983, Guardia-Nart-Montes 2006, Stainsby 2016)
- Recollement des A_p -bases en une A-base triangulaire de B. (restes chinois, Okutsu 1983).

Base réduite du conducteur

Travail en cours (Darkaoui-Simon-W., en s'appuyant sur Neiger-Xuan 2017)

Calcul d'une k[x]-base **réduite** du conducteur en $O(\Delta d^{\omega-1})$.

Corollaire (Conjecturé en 2010)

Supposons $\operatorname{Car}(k)=0$ ou >d et supposons $\operatorname{Sing}(C)\subset \mathbb{A}^2$. Factorisation déterministe en

$$D(d) + O^{\tilde{}}(\Delta d^{\omega-1}) \subset O^{\tilde{}}(d^{\omega+1}).$$

ightarrow Améliore les algos actuels, d'autant plus que C est peu singulière.

Exemple : Complexité $O(d^\omega)$ pour une courbe nodale sur \mathbb{F}_q avec O(d) noeuds.

Ouvertures

Objectif (Darkaoui-Simon-W.)

- Courbes nodales en $O(d^3)$.
- 2 Le cas des courbes singulières à l'infini.
- **3** Espaces $\mathcal{L}(D)$ de Riemann-Roch en $O^*(d^{\omega-1}(\Delta + \deg(D)))$. (améliore Abelard-Berardini-Couvreur-Lecerf 2022).

Objectif (Poteaux-W.)

Il faut ajouter $O(\Delta^2)\subset O(d^4)$ en petite caractéristique résiduelle. Très agaçant...

Problème : factorisation sur les corps locaux plus coûteuse.

2. Factorisation univariée sur les corps locaux

Résultat principal

- ullet (A,v) un anneau de valuation discrète complet de corps résiduel k.
- ullet Exemples : A=k[[t]] ou $A=\mathbb{Z}_p$ (et $k=\mathbb{F}_p$)
- Complexité = nombre d'opérations dans k.

Théorème (Poteaux-W. 2022, variante rapide de Montes 2000)

Soit $f \in A[x]$ séparable de degré d et $\delta = v(\operatorname{Disc}(f))$.

- Facteurs irréductibles de f à précision v-adique $n \geq \delta$:
 - ightharpoonup O(dn) si Car(k) = 0 ou Car(k) > d
 - $ightharpoonup O(dn+\delta^2)$ sinon.
- Test d'irréductibilité de f :
 - $ightharpoonup O^{\sim}(\delta)$ si $\operatorname{Car}(k) \nmid d$
 - $ightharpoonup O^{\sim}(\delta^2)$ sinon.

En deux mots

- Algorithme Round 4 de Zassenhauss (1986) : problèmes de gestion de précision.
- On se base plutôt sur l'algorithme OM de Montes (2000).
- S'inspire des travaux de Ore (1928), MacLane (1936) et Okutsu (1983) :
 - \rightarrow polygones ϕ -adiques, opérateurs résiduels.
- Reformalisé par Nart et al. (2020) et Spivakovski et al. (2022) dans le contexte plus général des corps henséliens:
 - valuations augmentées, algèbres graduées, polynômes clés (MacLane-Vaquié, 2007).

L'algorithme OM (sans frais)

Suppose f unitaire. Calculs menés avec précision v-adique δ .

Algorithme (Montes + Hensel μ -adique)

Factorisation (f, μ) :

- Si $R_{\mu}(f)$ irréductible, retourne f.
- $R_{\mu}(f) = P_1^{n_1} \cdots P_r^{n_r} \in k_{\mu}[z]$
- $f = F_1 \cdots F_r$
- Pour i = 1, ..., r:
 - ightharpoonup Calcule $\phi_i \in A[x]$ tel que $R_{\mu}(\phi_i) = P_i$
 - lacksquare Calcule les pentes λ_{ij} de $\mathcal{N}^+_{\mu,\phi_i}(F_i)$
 - Actualise $\mu_{ij} = [\mu, \phi_i, \lambda_{ij}]$
- Retourne $\bigcup_{i,j}$ Factorisation (F_i, μ_{ij}) .

 μ la valuation de Gauss

f irréductible

Factorisation résiduelle

Lemme de Hensel µ-adique

Lemme de Hensel μ -adique

Polynô me clé

Polygone ϕ_i -adique

Valuation augmentée

Exemple (Kuo)

$$f = (x^2 - t^3)^2 - t^7 \in \mathbb{Q}[[t]][x]$$

Réductible ou irréductible ?

L'orateur sonde l'audience...

 $f = (x^2 - t^3)^2 - t^7 \in \mathbb{Q}[[t]][x].$

$$f = (x^2 - t^3)^2 - t^7 \in \mathbb{Q}[[t]][x].$$

$$\mu(t) = 1$$
, $\mu(x) = 3/2$, $\mu(\phi) = 7/2$

avec corps résiduel $k_{\mu}=\mathbb{Q}$

$$f = (x^2 - t^3)^2 - t^7 \in \mathbb{Q}[[t]][x].$$

$$\mu(t) = 1$$
, $\mu(x) = 3/2$, $\mu(\phi) = 7/2$

avec corps résiduel $k_{\mu} = \mathbb{Q}$.

• On a $f = \phi^2 - t^7$, avec $\mu(\phi^2) = \mu(t^7) = 7$.

$$f = (x^2 - t^3)^2 - t^7 \in \mathbb{Q}[[t]][x].$$

$$\mu(t) = 1$$
, $\mu(x) = 3/2$, $\mu(\phi) = 7/2$

avec corps résiduel $k_{\mu} = \mathbb{Q}$.

- On a $f = \phi^2 t^7$, avec $\mu(\phi^2) = \mu(t^7) = 7$.
- On déduit :

$$R_{\mu}(f) = \mathbf{z^2} - \mathbf{1} = (z - 1)(z + 1) \quad \overset{\text{Montes}}{\Longrightarrow} \quad f = F_1 F_2 \in \mathbb{Q}\left[\begin{bmatrix} t \end{bmatrix} \right] \left[x \right]$$

$$f = (x^2 - t^3)^2 - t^7 \in \mathbb{Q}[[t]][x].$$

$$\mu(t) = 1$$
, $\mu(x) = 3/2$, $\mu(\phi) = 7/2$

avec corps résiduel $k_{\mu} = \mathbb{Q}$

- On a $f = \phi^2 t^7$, avec $\mu(\phi^2) = \mu(t^7) = 7$.
- On déduit :

$$R_{\mu}(f) = \mathbf{z}^2 - \mathbf{1} = (z - 1)(z + 1) \quad \stackrel{\text{Montes}}{\Longrightarrow} \quad f = F_1 F_2 \in \mathbb{Q}[[t]][x]$$

• Hensel μ -adique :

$$F_1 = \underbrace{x^2 - t^3 - t^2 x}_{\mu = 7/2} + \underbrace{\cdots}_{\mu > 7/2}$$
 $F_2 = \underbrace{x^2 - t^3 + t^2 x}_{\mu = 7/2} + \underbrace{\cdots}_{\mu > 7/2}.$

$$f = (x^2 - t^3)^2 - t^7 \in \mathbb{Q}[[t]][x].$$

$$\mu(t) = 1, \quad \mu(x) = 3/2, \quad \mu(\phi) = 7/2$$

avec corps résiduel $k_{\mu} = \mathbb{Q}$

- On a $f = \phi^2 t^7$, avec $\mu(\phi^2) = \mu(t^7) = 7$.
- On déduit :

$$R_{\mu}(f) = \frac{z^2}{1} - \frac{1}{1} = (z - 1)(z + 1) \xrightarrow{\text{Montes}} f = F_1 F_2 \in \mathbb{Q}[[t]][x]$$

• Hensel μ -adique :

$$F_1 = \underbrace{x^2 - t^3 - t^2 x}_{\mu = 7/2} + \underbrace{\cdots \cdots}_{\mu > 7/2} \qquad F_2 = \underbrace{x^2 - t^3 + t^2 x}_{\mu = 7/2} + \underbrace{\cdots \cdots}_{\mu > 7/2}.$$

• Indices de ramification $e_1=e_2=2$ et degrés résiduels $f_1=f_2=1$

Contributions (variante rapide, 2022)

- lacktriangle Lemme de Hensel μ -adique.
- 2 Diviser pour régner : précision $2\delta/d \leadsto$ moitié des facteurs
- lacktriangle Racines approchées (Abhyankhar-Moh) \Rightarrow polynômes clés optimaux si $\operatorname{Car}(k) \nmid d$.
- Evaluation dynamique (Lecerf-v.d. Hoeven 2020).

Proposition (Poteaux-W. 2024)

Il suffit de travailler à précision $\delta_{\mathrm{tame}} \leq \delta$.

Exemple: $f = x^2 - xt^N + t \in \mathbb{F}_2[[t]][x]$, on obtient $\delta_{tame} = 1$ tandis que $\delta = N$.

Travail en cours (Poteaux-W.)

Si Car(k) divise d: remplacer racines approchées par calcul détendu.

Quelques résultats en lien avec la factorisation locale

Courbes algébriques planes:

► Factorisation bivariée via une fibre critique

(W. 2017)

ightharpoonup Séries de Puiseux en $O(d\delta)$

(Poteaux-W. 2020)

 \blacktriangleright Genre en $O^{\tilde{}}(d^3)$

(Poteaux-W. 2020)

Corps de nombres et corps de fonctions:

(Poteaux-W. 2024)

- Invariants d'Okutsu-Zariski en $O(d\Delta)$
- Base intégrale d'un idéal fractionnaire en $O^{\sim}(d\Delta + h(I))$
- Corps henséliens:

(Alberich-Guardia-Nart-Poteaux-Roé-W., 2023)

- ▶ Valuation rang un: factorisation si Car(k) = 0 ou > d.
- ▶ Valuation quelconque: irréductibilité si $Car(k) \nmid d$.
- ► Corps valués : extensions de valuations et chaînes de MacLane-Vaquié.

3. Factorisation bivariée et géométrie torique

C'est bientôt fini...



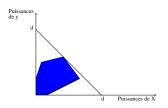
Polygone de Newton

Définition

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

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

Polynôme de facette : $f_{\Lambda} = \sum_{(i,j) \in \Lambda} c_{ij} x^i y^j$ (quasi-homogène).



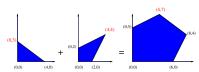
A degré fixé, plusieurs polygones

⇒ Meilleur indicateur de complexité.

$$f_1 = 1 - 2x^4 + y^3 - xy$$

$$f_2 = 3 - x^2 + xy^2 - 2x^4y^4 + y^2$$

$$f_1f_2 = 3 + 2x^6 + 4x^8y^4 - 2x^4y^7 + y^5 + \cdots$$



$$\mathrm{N_{f_1f_2}} = \mathrm{N_{f_1}} + \mathrm{N_{f_2}}$$
 (Ostrowski)

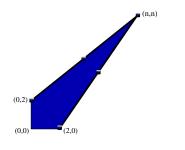
Résultat principal

Définition

f est non dégénéré si $0 \in N_f$ et si les polynômes de facettes extérieurs sont séparables.

Théorème (W. 2010)

Suppose $k \subset \mathbb{C}$. Factorisation des polynômes non dégénérés en $O(\operatorname{Vol}(\operatorname{N}_f)^\omega)$ plus le coût des factorisations des polynômes de facettes extérieurs.



- Approche dense :
 - $O(n^{\omega+1})$ et 1 facto univariée degré 2n
- Approche polygone : $O(n^{\omega})$ et 2 factos univariées de degré 2.

Stratégie torique

Compactification torique X de \mathbb{A}^2 telle que :

- ullet Facettes extérieures de $N_f \longleftrightarrow {\sf Composantes}$ du bord $B = X \setminus \mathbb{A}^2$.
- Factorisation de facettes \longleftrightarrow Décomposition de $C \cap B$, où $C \subset X$ courbe de f.



Stratégie : Recombinaisons des développements de Taylor (jets) à l'infini torique.

Précision et recombinaisons

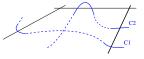
- Décomposition recherchée : $C = C_1 + \cdots + C_s$
- Précisions des calculs : $D=2\operatorname{div}_{\infty}(f)$
- Développements de Taylor : $C \cap D = \sum_{P} \gamma_{P} \in \operatorname{Div}(D)$.

Théorème (W. 2010)

Toute k-combinaison des γ_P qui s'étend à $\mathrm{Div}(X)\otimes k$ est une k-combinaison des $C_i\cap D$.



~→



Preuve

Théorème de Gao-Ruppert, formes logarithmiques, cohomologie des variétés toriques.

Extension des diviseurs (théorème d'osculation)

Théorème (W. 2010)

Soit $D \subset X$ de support B. On a une suite exacte

$$0 \to \operatorname{Pic}(X) \to \operatorname{Pic}(D) \overset{\alpha}{\to} H^0(X, \Omega^2_X(D))^\vee \to 0$$

où $\alpha(\gamma)$ associe à une 2-forme une somme de résidus.



Preuve

Suite exponentielle, dualité de Serre, cohomologie $\bar{\partial}$ de Dolbeault, courants résiduels.

Algorithme $(V = Vol(N_f) \text{ et } D = 2 \operatorname{div}_{\infty}(f).)$

- Calcul $C \cap D$ et construction matrice en O(dV)
- Recombinaisons en $O(Vr^{\omega-1})$, r nombre facteurs facettes
- Equations des C_i en $O(V^{\omega})$

Bernstein-Kushnirenko

$$h^0(\Omega^2_X(D)) = O(V)$$

Algèbre linéaire brute force

Peut mieux faire (merci HDR)

Théorème (W. 2024, non publié)

On peut atteindre **sur tout corps parfait k** la complexité

$$O^{\widehat{\ }}(Vr^{\omega-1})\subset O^{\widehat{\ }}(d^{\omega+1})$$

conjecturée dans mon mémoire (ouverture 3.3.4).

Preuve

- Transformation de N_f via $SL_2(\mathbb{Z})$ tel que $\operatorname{Vol}(N_f) pprox d_x d_y$
- (Berthomieux-Lecerf 2012)

ullet Factorisation rapide dans k[[x]][y]

(Poteaux-W. 2022)

• Recombinaisons des dérivées logarithmiques dans le cas critique

(W. 2017)

Finie la géométrie algébrique complexe (snif).

Conclusion

- ullet Approche singularités (cas unitaire) : $O(\Delta d^{\omega-1}) \subset O(d^{\omega+1})$
- ullet Approche polygone de Newton : $O(Vr^{\omega-1}) \subset O(d^{\omega+1})$
- Approche mixte?

On introduit le delta-invariant torique

$$\Delta' = \underbrace{\text{genre arithmétique torique}}_{\text{points entiers intérieurs au polygone}} - \text{genre géométrique} \qquad \Delta' \leq \min(\Delta, \mathbf{V})$$

Factorisation en
$$O(\Delta' r^{\omega-1})$$
 ?

Problème

Tenir compte du polygone de Newton lors du calcul du conducteur.

Quelques contributions dont je n'ai pas parlé

- Théorèmes type Abel-inverse torique (thèse, 2008)

 Courants résiduel, variétés toriques, analyse complexe
- Gonalité des courbes algébriques (Schicho-Schreyer-W., 2013)
 Syzygies des courbes canoniques
- Polynômes de discriminant minimaux (Simon-W., 2018)
 G-réduction des courbes planes
- Le lieu flex des hypersurfaces projectives (Busé-D'Andréa-Sombra-W., 2020)
 Résultants multivariés