Algorithmes pour la décomposition primaire des idéaux polynomiaux de dimension nulle donnés en évaluation.

Clémence Durvye.

UMR 8100 du CNRS

Laboratoire de mathématiques

Université de Versailles

Saint-Quentin-en-Yvelines

Problématique

Soit $\mathbb{K}$ un corps de caractéristique 0, de clôture algébrique $\bar{\mathbb{K}}$.

On cherche à résoudre un système algébrique **de dimension nulle**

$$f_1 = \cdots = f_s = 0, \; g \neq 0,$$

où $f_1, \ldots, f_s, g \in \mathbb{K}[x_1, \ldots, x_n]$.

$\rightsquigarrow$ applications en géométrie algébrique effective, robotique, etc.

Descriptions de l’ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Dimension et position de Noether
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

1. Localisation et intersection
2. Calcul du module localisé de courbe
3. Formes de Hermite et sommes de modules

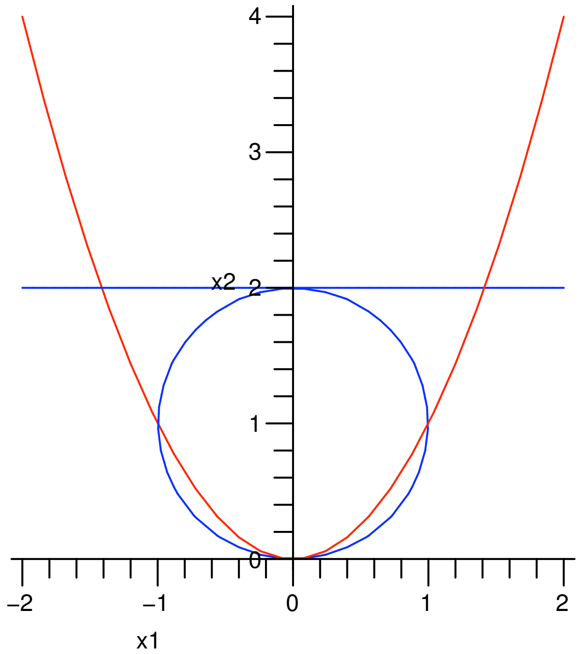
Conclusion

Représentation univariée : un exemple

$n = 2,\ \mathbb{K} = \mathbb{Q}$

L'ensemble des solutions du système

$$\begin{cases} f_1 = (x_1^2 + (x_2 - 1)^2 - 1)(x_2 - 2), \\ f_2 = x_2 - x_1^2 \end{cases}$$



est

$\{(0,0), (-1,1), (1,1), (-\sqrt{2},2), (\sqrt{2},2)\}$

que l'on peut décrire par

$$\begin{cases} x_1(x_1 - 1)(x_1 + 1)(x_1^2 - 2) = 0, \\ x_2 = x_1^2. \end{cases}$$

Algorithmes de calcul d'une représentation univariée

Entrée : $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$.
Sortie : une représentation univariée de l'ensemble des solutions du système $f_1 = \cdots = f_n = 0$ s'il est fini.

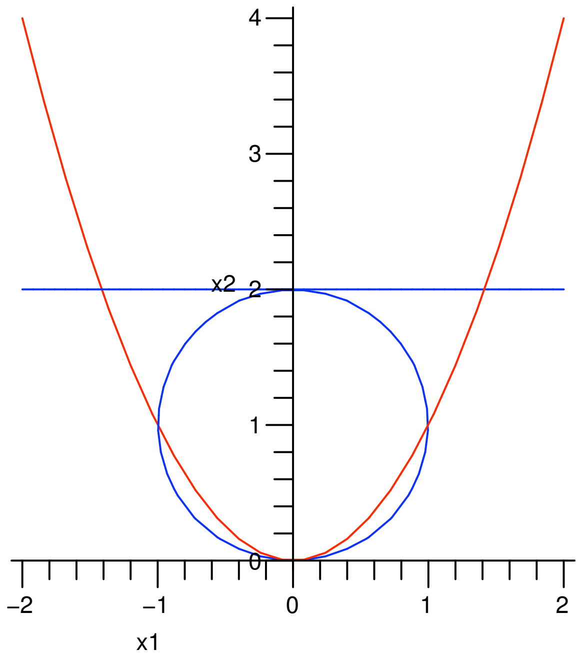
Deux familles d'algorithmes, liées à la représentation des polynômes de départ :

– algorithmes de réécriture : bases de Gröbner, algorithme *RUR* (*Maple 11*), résultants,...
– algorithmes par évaluation : travaux du groupe TERA (Giusti, Heintz, Pardo, Lecerf, Salvy,...), algorithme *Kronecker*, implementé en *Magma* (www.math.uvsq.fr/$\sim$lecerf)

$\rightsquigarrow$ Ce n'est qu'une description ensembliste.

$$f_1 = (x_1^2 + (x_2 - 1)^2 - 1)(x_2 - 2)$$
$$f_2 = (x_2 - x_1^2)$$

$$(f_1, f_2)$$
$$= (x_1^2(x_1 - 1)(x_1 + 1)(x_1^2 - 2), x_2 - x_1^2)$$
$$\neq (x_1(x_1 - 1)(x_1 + 1)(x_1^2 - 2), x_2 - x_1^2)$$



Descriptions de l’ensemble des solutions

1. Description ensembliste
2. Description algébrique :
   (a) point de vue global
   (b) point de vue local

Calcul de la description ensembliste

Calcul de la description algébrique

Conclusion

Idéaux primaires de dimension nulle

Remarque

Soit $g = \prod_{j=1}^{s}(x - p^{(j)})^{\nu_j} \in \bar{\mathbb{K}}[x]$. Alors

$$(g) = (x - p^{(1)})^{\nu_1} \cap \cdots \cap (x - p^{(s)})^{\nu_s}.$$

Définition

Un idéal $\mathcal{J}$ de $\mathbb{K}[x_1, \ldots, x_n]$ est dit de dimension nulle si $\{(p_1, \ldots, p_n) \in \bar{\mathbb{K}}^n,\ \forall f \in \mathcal{J},\ f(p_1, \ldots, p_n) = 0\}$ est fini.

Un idéal de dimension nulle $\mathcal{Q}$ de $\bar{\mathbb{K}}[x_1, \ldots, x_n]$ est dit primaire si $\{(p_1, \ldots, p_n) \in \bar{\mathbb{K}}^n,\ \forall f \in \mathcal{Q},\ f(p_1, \ldots, p_n) = 0\}$ contient exactement un point.

Décomposition primaire

Exemple Soit $g = \prod_{j=1}^{s}(x - p^{(j)})^{\nu_j} \in \bar{\mathbb{K}}[x]$.
Alors $(g) = (x - p^{(1)})^{\nu_1} \cap \cdots \cap (x - p^{(s)})^{\nu_s}$.

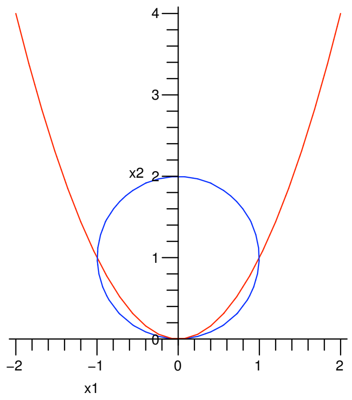
Théorème

Pour tout idéal de dimension nulle $\mathcal{I}$ de $\bar{\mathbb{K}}[x_1, \ldots, x_n]$, il existe un unique ensemble d'idéaux *primaires* $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_s\}$ tels que

$$\mathcal{I} = \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_s.$$

Exemple

$f_1 = x_1^2 + (x_2 - 1)^2 - 1,$
$f_2 = x_2 - x_1^2.$
$(f_1, f_2) = (x_1^2, x_2) \cap (x_1 - 1, x_2 - 1) \cap (x_1 + 1, x_2 - 1).$



Algorithmes de décomposition primaire

Entrée : une famille $f_1, \ldots, f_s$ de polynômes.
Sortie : une famille de générateurs de “chaque” idéal primaire.

Algorithmes

– [*Gianni, Trager, Zacharias 88*],
– [*Eisenbud, Huneke, Vasconcelos 92*],
– [*Shimoyama, Yokohama 94*],
– [*Decker, Greuel, Pfister 99*],
– [*Steel 05*], [*Gao, Wan, Wang 06*]
(caractéristique positive et corps finis),...

$\rightsquigarrow$ ces algorithmes procèdent par calcul de bases de Gröbner ;
$\rightsquigarrow$ les polynômes y sont représentés dans la base des monômes.

Descriptions de l'ensemble des solutions

1. Description ensembliste
2. Description algébrique :
   (a) point de vue global
   (b) point de vue local

Calcul de la description ensembliste

Calcul de la description algébrique

Conclusion

Algèbre locale

Pour $p = (p_1, \ldots, p_n) \in \bar{\mathbb{K}}^n$, on note $\bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]$ l'anneau des séries formelles en $x_1 - p_1, \ldots, x_n - p_n$ sur $\bar{\mathbb{K}}$.

Exemple

$\mathcal{I} = (\ x_1^2(x_1 - 1)(x_1 + 1),\ x_2 - x_1^2\ )$,

$\mathcal{I}\bar{\mathbb{K}}[[x_1, x_2]] = (x_1^2, x_2)$.

Définition L'algèbre locale de p comme racine de $\mathcal{I}$ est

$$\mathbb{D}_p = \bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]/(\mathcal{I}).$$

La multiplicité de p comme racine de $\mathcal{I}$ est la dimension de $\mathbb{D}_p$.

Exemple

$\mathbb{D}_{(0,0)} = \bar{\mathbb{K}}[[x_1, x_2]]/(x_1^2, x_2)$,

$\mathbb{D}_{(1,1)} = \bar{\mathbb{K}}[[x_1 - 1, x_2 - 1]]/(x_1 - 1, x_2 - 1)$.

Historique de la décomposition primaire : cas de la dimension nulle

Entrée : une famille $f_1, \ldots, f_s$ de polynômes.
Sortie : pour toute racine du système, les matrices de multiplication par les variables dans une base de son algèbre locale $\mathbb{D}_p$.

Algorithme Global
$\rightsquigarrow$ algèbre linéaire dans $\bar{\mathbb{K}}[x_1, \ldots, x_n]/(f_1, \ldots, f_s)$
(bases de Gröbner)
– [*Alonso, Becker, Roy, Wörmann 96*] ,...

Algorithmes Locaux (après le calcul d'une racine p du système)
$\rightsquigarrow$ élimination dans $\bar{\mathbb{K}}[[x_1 - p_1, \ldots, x_n - p_n]]$
(bases standard, ordres locaux)
– [*Mora 91*], [*Greuel, Pfister 96*]
$\rightsquigarrow$ dualité entre polynômes et opérateurs différentiels.
– [*Mourrain 96*], [*Dayton, Zeng 05*], [*Leykin 08* (dim. positive)]

Descriptions de l'ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

Conclusion

Résolution géométrique et “Kronecker” solver

1990–1999 Algorithmes probabilistes théoriques avec un coût polynomial en le degré géométrique pour calculer les racines isolées : Giusti, Hägele, Heintz, Matera, Montaña, Morais, Morgenstern, Pardo, Sabia, Smietanski.

1999–2001 Algorithmes pratiques et implantation : Aldaz, Bruno, Castaño, Hägele, Heintz, Llovet, Marchand, Martìnez, Matera, Wachenchauzer, [*Giusti, Lecerf, Salvy 01*], [*Magma Kronecker package*].

2001–2003 Généralisations pour le calcul de la décomposition équidimensionelle d’une variété : Jeronimo, Lecerf, Krick, Puddu, Sabbia, Sombra,...

2006 une preuve autonome, calcul des multiplicités des racines isolées sans coût supplèmentaire : [*Durvye, Lecerf, 2007*]

2007 Description algébrique des racines isolées : [*Durvye, 2008*]

Descriptions de l’ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

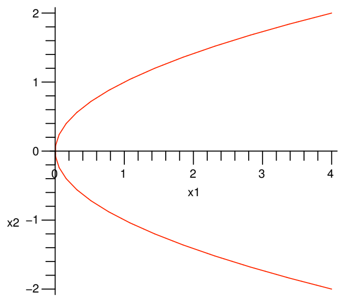
Calcul de la description algébrique

Conclusion

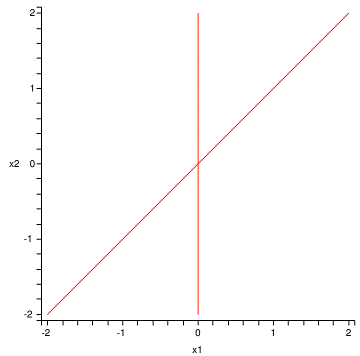
Position de Noether générale

Définition Soit $\mathcal{I}$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$.
$\mathcal{I}$ est dit en position de Noether générale (p.N.g.) s'il existe r t.q.

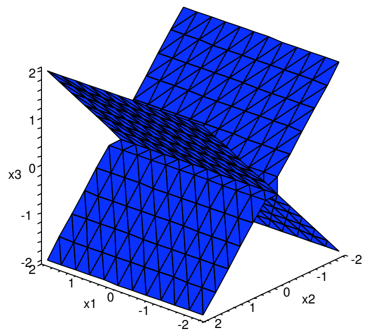
- $\mathbb{K}[x_1, \ldots, x_r] \cap \mathcal{I} = (0)$ (variables libres),
- $\forall\, j \in \{r+1, \ldots, n\}$, $\exists\, q \in \mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_r, x_j]$ tel que $\deg_{x_j}(q) = \deg(q)$ (variables liées).



$(x_2^2 - x_1)$



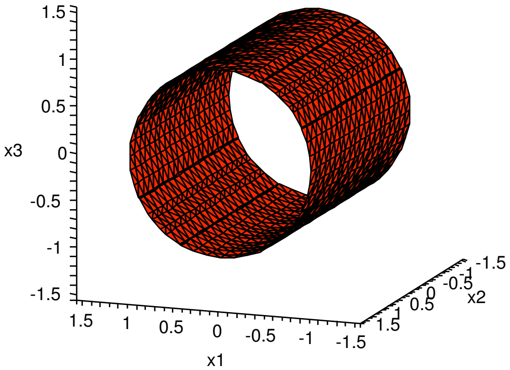
$(x_1 x_2 - x_1^2)$

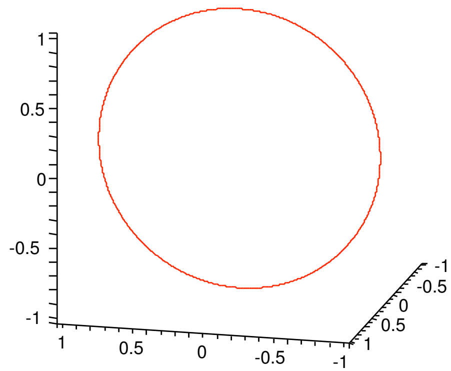


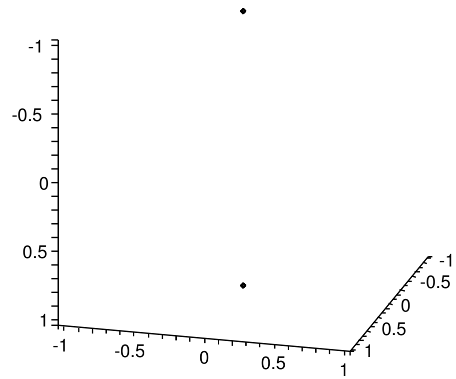
$(x_3^2 - x_2^2)$

$\rightsquigarrow$ r est alors la dimension de l'idéal.

Position de Noether et spécialisations







$$(x_3^2 + x_1^2 - 1) \qquad (x_3^2 + x_1^2 - 1) + (x_2) \qquad (x_3^2 + x_1^2 - 1) + (x_1, x_2)$$

Le $\mathbb{K}[x_1, \ldots, x_r]$-module $\mathbb{B}$

Soit $\mathcal{I}$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ en position de Noether générale, et soit

$$\mathbb{B} = \mathbb{K}[x_1, \ldots, x_r][x_{r+1}, \ldots, x_n]/\mathcal{I}.$$

Proposition

Le $\mathbb{K}[x_1, \ldots, x_r]$-module $\mathbb{B}$ est sans torsion si et seulement si $\mathcal{I}$ est r-équidimensionel (unmixed).

$\rightsquigarrow$ dans le cas d'une courbe équidimensionelle, $\mathbb{B}$ est un $\mathbb{K}[x_1]$-module libre de type fini.

Exemple

$\mathbb{K}[x_1, x_2]/(x_1^2 + (x_2 - 1)^2 - 1)$ est un $\mathbb{K}[x_1]$-module libre.

Descriptions de l’ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

Conclusion

Élément Primitif

Soit $\mathcal{I}$ en p.N.g. radical, et $\mathcal{I}' = \mathcal{I}\mathbb{K}(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$.

Définition

On dit que x_{r+1} est primitif pour $\mathcal{I}$ si ses puissances engendrent le $\mathbb{K}(x_1, \ldots, x_r)$-espace vectoriel

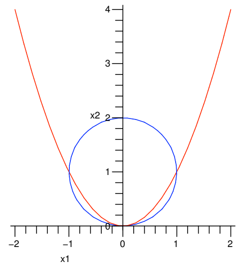
$$\mathbb{B}' = \mathbb{K}(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/\mathcal{I}'.$$

Propriété utile

Si $\mathcal{I}$ est un idéal de dimension nulle, et si x_1 est primitif pour $\mathcal{I}$, alors x_1 sépare les racines de $\mathcal{I}$.

Exemple

x_1 est primitif pour $\sqrt{(x_1^2 + (x_2 - 1)^2 - 1, x_2 - x_1^2)}$.



Représentations univariées

Soit $\mathcal{I}$ un idéal radical équidim. en p.N.g., d'élt primitif x_{r+1}.

$$\mathbb{B}' = \mathbb{K}(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/\mathcal{I}',$$

et q le polynôme minimal de x_{r+1} dans $\mathbb{B}'$.

Représentation univariée (RU)

$\exists! v_{r+2}, \ldots, v_n \in \mathbb{K}(x_1, \ldots, x_r)[x_{r+1}],\ \deg(v_j) \leq \deg(q) - 1$
tels que

$$\mathcal{I}' = (q(x_{r+1}), x_{r+2} - v_{r+2}(x_{r+1}), \ldots, x_n - v_n(x_{r+1})).$$

Représentation de Kronecker (RK) (aussi appelée RUR)
$\exists! w_{r+2}, \ldots, w_n \in \mathbb{K}(x_1, \ldots, x_r)[x_{r+1}],\ \deg(w_i) \leq \deg(q) - 1$
tels que

$$\mathcal{I}' = (q(x_{r+1}), q'(x_{r+1})x_{r+2} - w_{r+2}, \ldots, q'(x_{r+1})x_n - w_n).$$

Exemple

$$\left\{\begin{array}{ll} f_1 = & (x_2-1)^2+(x_1+2x_2+4x_3)^2+1 \\ f_2 = & x_3^2-x_2^2 \end{array}\right.$$

Représentation univariée (RU) pour x_2

$$q = x_2^4 + \frac{(84-88x_1)}{185} x_2^3 + \frac{(4-6x_1^2)}{185} x_2^2 + \frac{(x_1^3+x_1^2)}{185} x_2 + \frac{x_1^4}{185},$$

$$x_3 = \frac{370}{136x_1^2+32x_1} x_2^3 - \frac{361x_1-168}{136x_1^2+32x_1} x_2^2 - \frac{10x_1^2-10x_1-8}{136x_1^2+32x_1} x_2 - \frac{13x_1^3-4x_1^2}{136x_1^2+32x_1}.$$

Représentation de Kronecker (RK) pour x_2

$$q = x_2^4 + \frac{(84-88x_1)}{185} x_2^3 + \frac{(4-6x_1^2)}{185} x_2^2 + \frac{(x_1^3+x_1^2)}{185} x_2 + \frac{x_1^4}{185},$$

$$\frac{\partial q}{\partial x_2} x_3 = -\frac{208x_1-64}{185} x_2^3 + \frac{64x_1^2}{185} x_2^2 + \frac{16x_1^3}{185} x_2.$$

Représentation de Kronecker

Soit

$$\mathcal{I}' = (q(x_{r+1}), q'(x_{r+1})x_{r+2} - w_{r+2}(x_{r+1}), \ldots, q'(x_{r+1})x_n - w_n(x_{r+1}))$$

la représentation de Kronecker d'un idéal radical en position de Noether générale $\mathcal{I}$ pour l'élément primitif x_{r+1}.

Proposition

$$\begin{cases} q, w_{r+1}, \ldots, w_n \in \mathbb{K}[x_1, \ldots, x_r][x_{r+1}]; \\ \deg(q) = \deg_{x_{r+1}}(q) = \delta \text{ et } \deg(w_j) \leq \delta. \end{cases}$$

De plus, on a

$$\begin{cases} (q) = \mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_r, x_{r+1}]; \\ \forall j \in \{r+2, \ldots, n\},\ q'(x_{r+1})x_j - w_j(x_{r+1}) \in \mathcal{I}. \end{cases}$$

Descriptions de l'ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

Conclusion

Vue d'ensemble de l'algorithme de résolution géométrique

Soient $f_1, \ldots, f_n, g \in \mathbb{K}[x_1, \ldots, x_n]$. On pose

$$\begin{cases} \mathcal{I}_i & := & (f_1, \ldots, f_i) : g^\infty, \\ \mathcal{J}_i & := & \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i-1}, x_{n-i})}, \\ \mathcal{K}_i & := & \sqrt{\mathcal{I}_i + (x_1, \ldots, x_{n-i-1})}. \end{cases}$$

Boucle principale (sous les bonnes hypothèses) :

calcul d'une représentation de $\mathcal{J}_{i+1}$ à partir de celle de $\mathcal{J}_i$:

– (1) relèvement : calcul d'une représentation de $\mathcal{K}_i$;

– (2) intersection : calcul d'une représentation de $\sqrt{\mathcal{K}_i + (f_{i+1})}$;

– (3) nettoyage : calcul d'une représentation de $\sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty$.

“Mélanges”

Les données $f_1, \ldots, f_n, g \in \mathbb{K}[x_1, \ldots, x_n]$ vérifient
$(H) : \forall i \in \{0, \ldots, n-1\}$, $\mathcal{I}_i = (f_1, \ldots, f_i) : g^\infty$ est radical et f_{i+1} n'est pas diviseur de 0 modulo $\mathcal{I}_i$.

Proposition

Après un changement de variables affine $x = Ay + b$, pour A et b dans un ouvert de Zariski dense, on a :

- $\mathcal{I}_i$ est en position de Noether générale avec $r = n - i$ variables libres ;
- x_{r+1} est primitif pour $\mathcal{J}_i$ et pour $\mathcal{K}_i$;
- x_r est primitif pour $\sqrt{\mathcal{K}_i + (f_{i+1})}$;
- $\mathcal{J}_{i+1} = \sqrt{\mathcal{K}_i + (f_{i+1})} : g^\infty$.

$\rightsquigarrow$ un “mélange des équations” permet d'obtenir (H) sans perte de généralité.

Descriptions de l'ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

Conclusion

Polynôme caractéristique et multiplicités

Soient

– $\mathcal{I}$ un idéal 1-équidimensionel radical en p.N.g., de représentation univariée $q, v_3, \ldots, v_n$ pour l'élément primitif x_2,

– f un polynôme non diviseur de 0 dans $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$,

tels que $\mathcal{I} + (f)$ admet x_1 comme élément primitif.

Soit $\chi \in \mathbb{K}[x_1]$ le pol. caract. de m_{x_1} dans $\mathbb{B}/(f)$.

Alors $\chi(x_1) = \mathrm{Res}_{x_2}(q(x_2), f(x_1, x_2, v_3(x_2), \ldots, v_n(x_2)))$.

Or

soient $\rho^{(1)}, \ldots, \rho^{(s)} \in \bar{\mathbb{K}}^n$ les racines distinctes de $\mathcal{I} + (f)$, de multiplicités respectives $m_1, \ldots, m_s$.

Alors $\chi(x_1) = \prod_{\ell=1}^{s} \left(x_1 - \rho_1^{(\ell)}\right)^{m_\ell}$.

Descriptions de l’ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

1. Localisation et intersection
2. Calcul du module localisé de courbe
3. Formes de Hermite et sommes de modules

Conclusion

Réductions préliminaires

On se ramène à

– un idéal $(f_1, \ldots, f_{n-1}) : g^\infty$ radical 1-équidimensionel, en position de Noether générale, donné par sa représentation de Kronecker pour l'élément primitif x_2,

– une nouvelle équation f_n telle que $(f_1, \ldots, f_{n-1}) : g^\infty + (f_n)$ est de dimension nulle et admet pour élément primitif x_1.

On suppose que 0 est racine multiple de $(f_1, \ldots, f_n) : g^\infty + (f_n)$, de multiplicité μ_0 connue.

On veut calculer

$$\begin{aligned}\mathbb{D}_0 &= \mathbb{K}[[x_1, \ldots, x_n]]/(f_1, \ldots, f_n) : g^\infty \\ &= \mathbb{K}[[x_1, \ldots, x_n]]/(f_1, \ldots, f_{n-1}) : g^\infty + (f_n)\end{aligned}$$

Descriptions de l’ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

1. Localisation et intersection
2. Calcul du module localisé de courbe
3. Formes de Hermite et sommes de modules

Conclusion

Localisation en $x_1 = 0$

Soient $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-1}) : g^\infty$, et $p^{(1)}, \ldots, p^{(s)} \in \mathbb{K}^n$ les racines de $(f_1, \ldots, f_{n-1}) : g^\infty + (f_n)$. Alors

$$\mathbb{B}/(f_n) \simeq \mathbb{D}_{p^{(1)}} \times \mathbb{D}_{p^{(2)}} \times \cdots \times \mathbb{D}_{p^{(s)}}.$$

Soient $\mathbb{K}[[x_1]]$ l'anneau des séries formelles en x_1, et

$$\mathbb{B}_0 = \mathbb{K}[[x_1]][x_2, \ldots, x_n]/(f_1, \ldots, f_{n-1}) : g^\infty.$$

Proposition

$\mathbb{B}_0$ est un $\mathbb{K}[[x_1]]$-module libre de type fini, et

$$\mathbb{B}_0/(f_n) \simeq \mathbb{D}_0 = \mathbb{K}[[x_1, \ldots, x_n]]/(f_1, \ldots, f_{n-1}) : g^\infty + (f_n).$$

Exemple $(f_1, f_2) = (x_1^2(x_1 - 1)(x_1 + 1), x_2 - x_1^2)$.
$(f_1, f_2)\mathbb{K}[[x_1]][x_2] = (x_1^2, x_2)$, et $\mathbb{B}_0/(f_2) \simeq \mathbb{D}_0$.

Calcul d'une base de $\mathbb{D}_0$

Entrée : une base de
$\mathbb{B}_0 = \mathbb{K}[[x_1]][x_2, \ldots, x_n]/(f_1, \ldots, f_{n-1}) : g^\infty$.
Sortie : une base de $\mathbb{D}_0 \simeq \mathbb{B}_0/(f_n)$.

Forme de Smith
(Diagonalisation d'une matrice dans un anneau principal)
Soit δ_0 la dimension du $\mathbb{K}[[x_1]]$-module $\mathbb{B}_0$.
$\exists e_1, \ldots, e_{\delta_0}$ et $e'_1, \ldots, e'_{\delta_0}$ bases de $\mathbb{B}_0$,
$\exists \nu_1 \leq \cdots \leq \nu_\delta$ suite d'entiers, tels que $f_n e_i = x_1^{\nu_i} e'_i$.

Proposition

$$\left\{ \begin{array}{cccc} e'_1, & x_1 e'_1, & \ldots, & x_1^{\nu_1 - 1} e'_1 \\ \vdots & \vdots & & \vdots \\ e'_{\delta_0}, & x_1 e'_{\delta_0}, & \ldots, & x_1^{\nu_{\delta_0} - 1} e'_{\delta_0} \end{array} \right. \quad \text{est une base de } \mathbb{B}_0/(f_n).$$

Descriptions de l'ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

1. Localisation et intersection
2. Calcul du module localisé de courbe
3. Formes de Hermite et sommes de modules

Conclusion

Propriétés de $\mathbb{B}_0$ (1)

$\rightsquigarrow$ $\mathbb{B}_0$ est une sous-algèbre de la clôture entière de $\mathbb{K}[[x_1]]$ dans $\mathbb{K}((x_1))[x_2]/(q)$.

Soit $\delta = \deg(q)$, et $m \leq \delta(\delta-1)/2$ la demi-valuation en x_1 de $\operatorname{disc}_{x_2}(q)$.

On pose

$$\mathbb{L}_0 = \mathbb{K}[[x_1]]\frac{1}{x_1^m} \oplus \cdots \oplus \mathbb{K}[[x_1]]\frac{x_2^{\delta-1}}{x_1^m}.$$

Proposition

$\mathbb{B}_0$ est un sous-module de $\mathbb{L}_0$.

$\rightsquigarrow$ les relations $q'(x_2)x_j - w_j(x_2) \in \mathcal{I}$ permettent de calculer les coordonnées des x_j dans la base canonique de $\mathbb{L}_0$.

Propriétés de $\mathbb{B}_0$ (2)

On pose

$$\mathbb{M}_0 = \mathbb{K}[[x_1]] \oplus \cdots \oplus \mathbb{K}[[x_1]]x_2^{\delta-1}.$$

Proposition

Comme $\mathcal{I} \cap \mathbb{K}[x_1, x_2] = (q)$,

$\mathbb{M}_0$ est un sous-module de $\mathbb{B}_0$.

$\leadsto$ $\mathbb{B}_0$ est la plus petite sous-algèbre de $\mathbb{L}_0$ qui contient $\mathbb{M}_0$ et $x_3, \ldots, x_n$.

Calcul de $\mathbb{B}_0$

Entrée : la représentation de Kronecker de $\mathcal{I}$.

Sortie : une base de $\mathbb{B}_0 = \mathbb{K}[[x_1]][x_2, \ldots, x_n]/\mathcal{I}_0$.

Algorithme

- on pose $\mathbb{M} = \mathbb{M}_0$;
- on calcule $\mathbb{M}' = \mathbb{M} + \mathbb{K}[[x_1]]x_3 + \cdots + \mathbb{K}[[x_1]]x_n$;
- tant que $\mathbb{M} \neq \mathbb{M}'$,

  $\mathbb{M} = \mathbb{M}'$, donné par une base $e_1, \ldots, e_\delta$,

  $\mathbb{M}' = \mathbb{M} + \sum_{1 \leq i,j \leq \delta} \mathbb{K}[[x_1]]e_i e_j$.

Coût Cet algorithme nécessite au pire $(n-2) + m\delta^3$ sommes du type $\mathbb{M} + \mathbb{K}[[x_1]]v$, où $\mathbb{M}$ est un sous module de $\mathbb{L}_0$ et $v \in \mathbb{L}_0$.

Descriptions de l’ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

1. Localisation et intersection
2. Calcul du module localisé de courbe
3. Formes de Hermite et sommes de modules

Conclusion

Forme de Hermite Normale

Soit $M \in (\mathbb{K}[[x_1]])_{\delta\times(\delta+1)}$ de rang δ.

$\exists\,!\, H \in (\mathbb{K}[[x_1]])_{\delta\times(\delta+1)}$, $\exists\,!\, P \in (\mathbb{K}[[x_1]])_{(\delta+1)\times(\delta+1)}$ inversible, telles que

- $H = MP$,
- H est de la forme

$$H = \begin{pmatrix} x_1^{\nu_1} & 0 & \cdots & 0 & 0 \\ h_{2,1} & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ h_{\delta,1} & \cdots & h_{\delta,\delta-1} & x_1^{\nu_\delta} & 0 \end{pmatrix},$$

- pour $k > l$, $\deg(h_{k,l}) < \nu_k$.

Bases Polynomiales de Sous Modules de $\mathbb{L}_0$

Soit $\mathbb{M}$ un sous module de rang δ de

$$\mathbb{L}_0 = \mathbb{K}[[x_1]]\frac{1}{x_1^m} \oplus \cdots \oplus \mathbb{K}[[x_1]]\frac{x_2^{\delta-1}}{x_1^m}.$$

Définition

Une base $\varepsilon_1, \ldots, \varepsilon_\delta$ de $\mathbb{M}$ est dite base triangulaire normale de $\mathbb{M}$ si la matrice $\begin{pmatrix} \varepsilon_1 & \cdots & \varepsilon_\delta \end{pmatrix}$ est sous forme de Hermite normale.

Proposition

- Il existe une unique base triangulaire normale de $\mathbb{M}$;
- Pour $j \in \{1, \ldots, \delta\}$, les coordonnés des ε_j appartiennent à $\mathbb{K}[x_1]$.
- Si $\mathbb{M}$ contient $\mathbb{M}_0 = \mathbb{K}[[x_1]] \oplus \cdots \oplus \mathbb{K}[[x_1]]x_2^{\delta-1}$, les coordonnées de $\varepsilon_1, \ldots, \varepsilon_n$ sont de degré au plus m.

Somme de modules

Entrée :

– un sous module $\mathbb{M}$ de $\mathbb{L}_0$ de rang δ contenant $\mathbb{M}_0$, donné par sa base triangulaire normale $\varepsilon_1, \ldots, \varepsilon_\delta$;
– $v \in \mathbb{L}_0$.

Sortie :

la base triangulaire normale $\eta_1, \ldots, \eta_\delta$ de $\mathbb{M} + \mathbb{K}[[x_1]]v$.

On pose $M = \begin{pmatrix} \varepsilon_1 & \cdots & \varepsilon_\delta & v \end{pmatrix}$,

et $M_{m\delta+1} = M \mod x_1^{m\delta+1}$.

Proposition

Les formes de Hermite normales de M et $M_{m\delta+1}$ sont égales. En particulier, les coordonnées de η_j sont les coefficients de la j-ème colonne de la forme de Hermite de $M_{m\delta+1}$.

Descriptions de l’ensemble des solutions

1. Description ensembliste
2. Description algébrique

Calcul de la description ensembliste

1. Position de Noether et module de courbe
2. Éléments primitifs et représentations univariées
3. Algorithme de résolution
4. Calcul des multiplicités

Calcul de la description algébrique

1. Localisation et intersection
2. Calcul du module localisé de courbe
3. Formes de Hermite et sommes de modules

Conclusion

Résultat principal

Théorème [*Durvye 07*]
Sous les hypothèses précédentes,
il existe un algorithme probabiliste qui calcule

- les racines p du système,
- les matrices de multiplication par $x_1, \ldots, x_n$ dans une base de leur algèbre locale $\mathbb{D}_p$,

avec

$$\tilde{\mathcal{O}}(D^{11} + (L + ns)D^6) \text{ operations arithmétiques dans } \mathbb{K},$$

où

- n est le nombre de variables,
- L est le coût d'évaluation de $f_1, \ldots, f_s, g$ donnés par un circuit arithmétique,
- et $D = d^n$, où $d \geq 2$ est le maximum des degrés de $f_1, \ldots, f_s$.

Contributions

– présentation concise de l'algorithme Kronecker et preuves constructives (les seuls prérequis pour la lecture de la thèse sont quelques résultats sur les modules sur un anneau principal) ;
– lever des hypothèses de régularité, ce qui permet de calculer les multiplicités sans coût supplémentaire ;
– algorithmes pour le calcul des formes réduites de matrices à coefficients dans un anneau de séries formelles (formes de Hermite et de Smith, avec multiplicateurs) ;
– nouvel algorithme de calcul de la décomposition primaire pour les idéaux de dimension nulle, avec son étude de coût.