Techniques d'évaluation pour la décomposition primaire d'un idéal de polynômes zéro-dimensionel.

Clémence Durvye

UMR 8100 du CNRS
Laboratoire de mathématiques
Université de Versailles
Saint-Quentin-en-Yvelines
France

Problématique

Soit K un corps de caractéristique zéro, de clôture algébrique $\overline{K}$.

Soient $f_1, \ldots, f_s, g \in K[x_1, \ldots, x_n]$ tels que le système

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

admette un ensemble fini de solutions dans $\overline{K}^n$.

On cherche à calculer tous les zéros $p = (p_1, \ldots, p_n) \in \overline{K}^n$ de

$$(f_1, \ldots, f_s) : g^\infty = \{f \mid \exists m \geq 0, \; g^m f \in (f_1, \ldots, f_s)\}$$

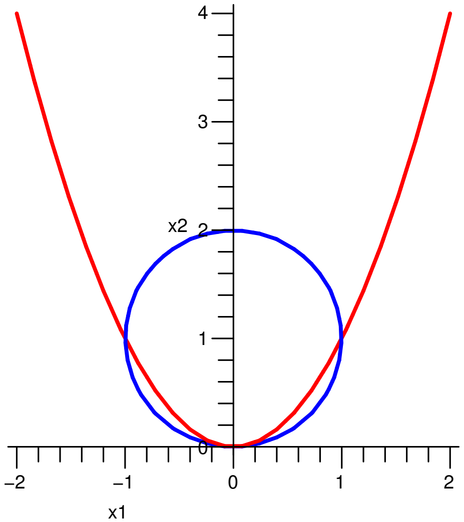
avec leurs algèbres locales

$$\mathbb{D}_p = \overline{K}[[x_1 - p_1, \ldots, x_n - p_n]]/((f_1, \ldots, f_s) : g^\infty).$$

Exemple

$n = 2,\ K = \mathbb{Q},\ g = 1.$

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



$$\begin{cases} \mathbb{D}_{(0,0)} = \bar{\mathbb{Q}}[[x_1, x_2]]/(x_1^2, x_2), \\ \mathbb{D}_{(-1,1)} = \bar{\mathbb{Q}}[[x_1 + 1, x_2 - 1]]/(x_1 + 1, x_2 - 1), \\ \mathbb{D}_{(1,1)} = \bar{\mathbb{Q}}[[x_1 - 1, x_2 - 1]]/(x_1 - 1, x_2 - 1). \end{cases}$$

$\mathbb{D}_{(0,0)}$ est décrite par $M_{x_1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et $M_{x_2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

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

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

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 $f_1, \ldots, f_s$.

Historique de la Décomposition Primaire : Cas Général

Entrée : une famille $f_1, \ldots, f_s$ de plolynômes.
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*] (caractéristique positive),
– [*Gao, Wan, Wang 06*] (corps finis),...

$\rightsquigarrow$ ces algorithmes se réduisent au cas zéro-dimensionel ;
$\rightsquigarrow$ ils procèdent par calcul de bases de Gröbner ;
$\rightsquigarrow$ les polynômes y sont représentés dans la base des monômes.

Historique de la Décomposition Primaire : Cas Zéro-Dimensionel

Entrée : une famille $f_1, \dots, f_s$ 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 $K[x_1, \dots, x_n]/(f_1, \dots, f_s)$

(bases de Gröbner)

– [*Alonso, Becker, Roy, Wörmann 96*] ,...

Algorithmes Locaux (après le calcul d'une racine p du système)

$\rightsquigarrow$ élimination dans $\overline{K}[[x_1 - p_1, \dots, x_n - p_n]]$

(bases standard, ordres locaux)

– [*Mora 91*], [*Greuel, Pfister 96*]

$\rightsquigarrow$ dualité entre polynômes et opérateurs différentiels.

– [*Mourrain 96*], [*Dayton, Zeng 05*]

Avantages du nouvel Algorithme

Notre algorithme mélange des méthodes locales et globales.

$\rightsquigarrow$ il n'utilise ni bases de Gröbner, ni bases standard :

– dans le cas zéro-dimensionel, cela permet d'éviter un coefficient binomial dans l'analyse de coût de l'algorithme.
– cet algorithme peut sans doute être généralisé au calcul des composantes primaires dans le cas général.

$\rightsquigarrow$ il repose entièrement sur des techniques d'évaluation :

– le coût de l'algorithme de Mourrain fait intervenir "le nombre de monômes obtenus par dérivation des monômes de $f_1, \ldots, f_s$".

Plan de l'exposé

1. Position de Noether, élement primitif et représentation de Kronecker.
2. Calcul du radical : l'algorithme Kronecker.
3. Module localisé de la courbe et intersection.

1. Position de Noether, élement primitif et représentation de Kronecker.
2. Calcul du radical : l'algorithme Kronecker.
3. Module localisé de la courbe et intersection.

Position de Noether Générale

Soit $\mathcal{I}$ un idéal de $K[x_1, \ldots, x_n]$.

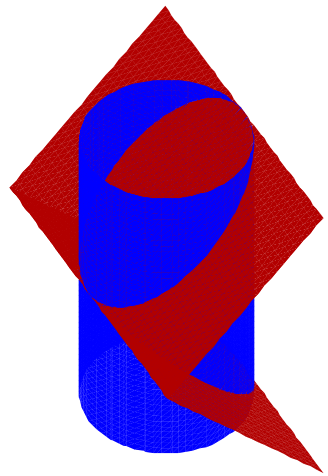
Définition

$\mathcal{I}$ est dit en position de Noether générale (p.N.g.) s'il existe r t.q.

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

Exemple

$((x_2 - 1)^2 + x_1^2 - 1, x_3^2 - x_2^2)$ est en p.N.g.



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

Soit $\mathcal{I}$ un idéal de $K[x_1, \ldots, x_n]$ en p.N.g., et soit

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

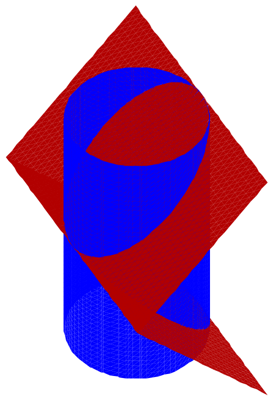
Proposition

Le $K[x_1, \ldots, x_r]$-module $\mathbb{B}$ est sans torsion ssi $\mathcal{I}$ est r-équidimensionel (i.e. ses premiers associés sont tous de dimension r).

CAS D'UNE COURBE

Si $\mathcal{I}$ est un idéal 1-équidimensionel, alors $\mathbb{B}$ est un $K[x_1]$-module libre de type fini.

Exemple $K[x_1, x_2, x_3]/(x_1^2 + (x_2 - 1)^2 - 1, x_3^2 - x_2^2)$ est un $K[x_1]$-module libre de type fini.



Élément Primitif

Définition

Soit $\mathcal{I}$ en p.N.g. radical, et $\mathcal{I}' = \mathcal{I}K(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$.
On dit que x_{r+1} est primitif pour $\mathcal{I}$ si ses puissances engendrent le $K(x_1, \ldots, x_r)$-espace vectoriel

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

Propriété utile

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

Représentation de Kronecker d'une Courbe Réduite

Soit $\mathcal{I}$ un idéal radical 1-équidimensionel en p.N.g..
On suppose que x_2 est primitif pour $\mathcal{I}$,
et on note q son polynôme minimal dans

$$\mathbb{B}' = K(x_1)[x_2, \dots, x_n]/\mathcal{I}K(x_1)[x_2, \dots, x_n].$$

Proposition

$\exists\,!\; q, v_3, \dots, v_n \in K(x_1)[x_2],\ \deg(v_i) \leq \deg(q) - 1$ tels que
$\mathcal{I}K(x_1)[x_2, \dots, x_n] = \big(q, x_3 - v_3, \dots, x_n - v_n\big)$.

$\exists\,!\; q, w_3, \dots, w_n \in K[x_1, x_2],\ \deg_{x_2}(w_i) \leq \deg_{x_2}(q) - 1$ tels que $\mathcal{I}K(x_1)[x_2, \dots, x_n] = \big(q, \frac{\partial q}{\partial x_2} x_3 - w_3, \dots, \frac{\partial q}{\partial x_2} x_n - w_n\big)$.

$\leadsto$ La suite $q, w_3, \dots, w_n$ est la représentation de Kronecker de $\mathcal{I}$.

Propriétés utiles

$\mathcal{I} \cap K[x_1, x_2] = (q)$ et $\forall j \in \{3, \dots, n\},\ \frac{\partial q}{\partial x_2} x_j - w_j \in \mathcal{I}$.

1. Position de Noether, élement primitif et représentation de Kronecker.
2. Calcul du radical : l'algorithme Kronecker.
3. Module localisé de la courbe et intersection.

On veut résoudre $\boldsymbol{f_1 = \cdots = f_s = 0,\ g \neq 0}$.
$\rightsquigarrow$ On suppose que $\boldsymbol{s = n}$.

Réduction à une Suite Régulière

On pose $\left\{\begin{array}{rcl} h_1 & = & \alpha_{1,1}f_1 + \cdots + \alpha_{1,n}f_n, \\ & \vdots & \\ h_n & = & \alpha_{n,1}f_1 + \cdots + \alpha_{n,n}f_n. \end{array}\right.$

Proposition

Pour $(\alpha_{k,l})$ dans un ouvert de Zariski dense, on a

$\forall i \in \{1, \ldots, n-1\}$,

- $(h_1, \ldots, h_i) : g^\infty$ est radical,
- h_{i+1} ne divise pas zéro dans $K[x_1, \ldots, x_n]/(h_1, \ldots, h_i) : g^\infty$
- $(h_1, \ldots, h_n) : g^\infty = (f_1, \ldots, f_n) : g^\infty$.

$\rightsquigarrow$ On note $f_1, \ldots, f_n$ les nouvelles équations.

$\rightsquigarrow$ En particulier, $\mathcal{I} = (f_1, \ldots, f_{n-1}) : g^\infty$ est un idéal radical 1-équidimensionel.

Coordonnées Suffisamment Génériques

Proposition

Pour ϕ dans un ouvert de Zariski dense des changements de variables affines,

– $\mathcal{I} = (f_1 \circ \phi, \ldots, f_{n-1} \circ \phi) : g \circ \phi^\infty$ est en p.N.g. ;

– x_2 est primitif pour $\mathcal{I}$;

– x_1 est primitif pour $\sqrt{\mathcal{I} \circ \phi + (f_n) \circ \phi}$.

  (x_1 sépare les racines de $\mathcal{I} \circ \phi + (f_n \circ \phi)$ dans $\overline{K}^n$.)

$\rightsquigarrow$ on note $f_1, \ldots, f_n$ les nouvelles équations.

Résolution de la Suite Régulière

Étant donnés $f_1, \dots, f_n, g$ de degré au plus d tels que

- $\forall i \in \{1, \dots, n-1\}$, $(f_1, \dots, f_i) : g^\infty$ est radical, et f_{i+1} ne divise pas zéro dans $K[x_1, \dots, x_n]/(h_1, \dots, h_i) : g^\infty$;
- $\mathcal{I} = (f_1, \dots, f_{n-1}) : g^\infty$ est en p.N.g., avec x_2 comme élément primitif,

l'algorithme dit Kronecker calcule

- la représentation de Kronecker $q, w_3, \dots, w_n$ de $\mathcal{I}$ pour x_2 ;
- les racines de $(\mathcal{I} + (f_n)) : g^\infty$ avec leur multiplicités, qui sont les dimensions de leurs algèbres locales,

en

$$\tilde{\mathcal{O}}(n(nL + n^4)d^{2(n+1)})$$

opérations dans K, où L est le coût d'évaluation de $f_1, \dots, f_n, g$.

Historique rapide de l'agorithme Kronecker

1990–1999 Algorithmes probabilistes théoriques avec un coût polynomial en le degré géométrique pour calculer les racines isolées : Fitchas, 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*]

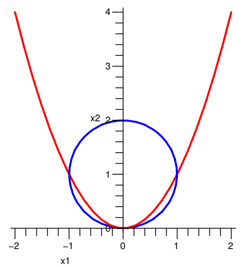
2007 Description algébrique des racines isolées.

Données après le Calcul du Radical

$\rightsquigarrow$ $q, w_3, \ldots, w_n \in K[x_1, x_2]$, représentation de Kronecker d'un idéal $\mathcal{I}$ 1-équidimensionel radical en p.N.g.,
$\rightsquigarrow$ un polynôme $f(= f_n)$ tels que
– $\mathcal{I} + (f)$ est zéro-dimensionel,
– x_1 est un élément primitif pour $\sqrt{\mathcal{I} + (f)}$,
– l'origine 0 est un zéro multiple de $(\mathcal{I} + (f)) : g^\infty$.
On veut calculer

$$\mathbb{D}_0 = \overline{K}[[x_1, \ldots, x_n]]/(\mathcal{I} + (f))_0.$$

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



1. Position de Noether, élement primitif et représentation de Kronecker.
2. Calcul du radical : l'algorithme Kronecker.
3. Module localisé de la courbe et intersection.

Module de la Courbe et Algèbres Locales

Proposition

Comme $\mathcal{I}$ est un idéal radical 1-équidimensionel en p.N.g., $\mathbb{B} = K[x_1, \ldots, x_n]/\mathcal{I}$ est un $K[x_1]$-module libre de type fini, de dimension $\delta = \deg_{x_2}(q)$.

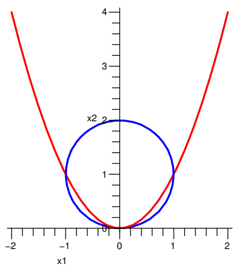
Proposition

Soient $p_1, p_2, \ldots, p_\ell$ les racines de $\mathcal{I} + (f)$ dans $\overline{K}^n$.
On a

$$\overline{K} \otimes \mathbb{B}/(f) \simeq \mathbb{D}_{p_1} \times \mathbb{D}_{p_2} \times \cdots \times \mathbb{D}_{p_\ell}.$$

Exemple

$n = 2, \mathcal{I} = (x_1^2 + (x_2 - 1)^2 - 1), f = x_2 - x_1^2$.
$\overline{K} \otimes \mathbb{B}/(f) \simeq \mathbb{D}_{(0,0)} \times \mathbb{D}_{(1,1)} \times \mathbb{D}_{(-1,1)}$.



Localisation et Complétion en $x_1 = 0$

Soient

– $K[[x_1]]$ l'anneau des séries formelles en x_1,

– et $\mathcal{I}_0 = \mathcal{I}K[[x_1]][x_2, \ldots, x_n]$.

On pose

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

Proposition

$\mathbb{B}_0$ est un $K[[x_1]]$-module libre de type fini, de dimension $\delta = \deg_{x_2}(q)$. De plus, on a

$$\overline{K} \otimes \mathbb{B}_0/(f) \simeq \mathbb{D}_0.$$

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

$(\mathcal{I} + (f))K[[x_1]][x_2] = (x_1^2, x_2)$, et $\overline{K} \otimes \mathbb{B}_0/(f) \simeq \mathbb{D}_{(0,0)}$.

Algorithme pour le Calcul de $\mathbb{D}_0$

Entrée :

- $q, w_3, \ldots, w_n$, représentation de Kronecker de $\mathcal{I} = (f_1, \ldots, f_{n-1}) : g^\infty$;
- $f = f_n$.

Sortie :

- les matrices de multiplication par les variables dans une base de l'algèbre locale $\mathbb{D}_0$ de la racine $\mathbf{0}$.

Étape 1 Calculer une base du module localisé de la courbe

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

Étape 2 Calculer la forme de Smith de la multiplication par f dans $\mathbb{B}_0$, puis les matrices $M_{x_1}, \ldots, M_{x_n}$ dans une base de

$$\mathbb{D}_0 \simeq \overline{K} \otimes \mathbb{B}_0/(f).$$

Étape 2 : forme de Smith et base de $\mathbb{D}_0$

Entrée : une base of $\mathbb{B}_0 = K[[x_1]][x_2, \ldots, x_n]/\mathcal{I}_0$.
Sortie : une base de $\mathbb{D}_0 = \overline{K} \otimes \mathbb{B}_0/(f)$.

Forme de Smith de la matrice de multiplication par f dans $\mathbb{B}_0$:
$\exists \varepsilon_1, \ldots, \varepsilon_\delta$ et $\varepsilon'_1, \ldots, \varepsilon'_\delta$ bases de $\mathbb{B}_0$,
$\exists 0 \leq \nu_1 \leq \cdots \leq \nu_\delta$, tels que $\forall i \in \{1, \ldots, \delta\},\ f\varepsilon_i = x_1^{\nu_i} \varepsilon'_i$.

$\rightsquigarrow x_1^{\nu_1} \varepsilon'_1, \ldots, x_1^{\nu_n} \varepsilon'_n$ sont nuls dans $\mathbb{B}_0/(f)$.

Proposition

$$\left\{ \begin{array}{cccc} \varepsilon'_1, & x_1\varepsilon'_1, & \ldots, & x_1^{\nu_1 - 1}\varepsilon'_1 \\ \vdots & \vdots & & \vdots \\ \varepsilon'_\delta, & x_1\varepsilon'_\delta, & \ldots, & x_1^{\nu_\delta - 1}\varepsilon'_\delta \end{array} \right. \quad \text{est une base de } \mathbb{D}_0 \simeq \overline{K} \otimes \mathbb{B}_0/(f).$$

$\rightsquigarrow$ forme de Smith avec multiplicateurs (*Villard 93*)

Étape 1 : calcul d'une base de $\mathbb{B}_0$

Entrée : la représentation de Kronecker $(q, w_2, \ldots, w_n)$ de $\mathcal{I}$.

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

Propriétés de $\mathbb{B}_0$ (1)

$\mathbb{B}_0$ est une sous algèbre de la clôture entière de $K[[x_1]]$ dans $K((x_1))[x_2]/(q)$, où $K((x_1))$ désigne l'anneau des séries de Laurent.

Proposition

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

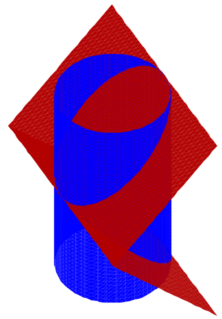
$$\begin{aligned} \mathbb{L}_0 &= K[[x_1]]\frac{1}{\mathrm{Disc}_{x_2}(q)} \oplus \cdots \oplus K[[x_1]]\frac{x_2^{\delta-1}}{\mathrm{Disc}_{x_2}(q)} \\ &= K[[x_1]]\frac{1}{x_1^m} \oplus \cdots \oplus K[[x_1]]\frac{x_2^{\delta-1}}{x_1^m}, \end{aligned}$$

où $\delta = \deg_{x_2}(q)$, et $m \leq \delta(\delta-1)$ est la valuation en x_1 du discriminant $\mathrm{Disc}_{x_2}(q) \in K[[x_1]]$ de q par rapport à x_2.

Exemple

Exemple

$$\begin{cases} f_1 = & (x_2-1)^2+(x_1+2x_2+4x_3)^2+1 \\ f_2 = & x_3^2-x_2^2 \end{cases}$$



La représentation de Kronecker de $\mathcal{I}=(f_1,f_2)$ est

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

$w_3=-\frac{208x_1-64}{185}x_2^3+\frac{64x_1^2}{185}x_2^2+\frac{16x_1^3}{185}x_2.$

$\mathrm{Disc}_{x_2}(q)$ a pour valuation 6.

$$\mathbb{L}_0=K[[x_1]]\frac{1}{x_1^6}\oplus K[[x_1]]\frac{x_2}{x_1^6}\oplus K[[x_1]]\frac{x_2^2}{x_1^6}\oplus K[[x_1]]\frac{x_2^3}{x_1^6}$$

et $\qquad x_3=\frac{370x_1^5}{32}\Big(\sum_{l\in\mathbb{N}}(\frac{17}{4})^l x_1^l\Big)\frac{x_2^3}{x_1^6}+\cdots \qquad$ (car $\frac{\partial q}{\partial x_2}x_3-w_3\in\mathcal{I}$.)

Propriétés de $\mathbb{B}_0$ (2)

On pose

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

Proposition

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

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

Cardinal d'une chaine de sous-modules

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

Soit $\mathbb{M}_0 \subsetneq \mathbb{M}_1 \subsetneq \cdots \subsetneq \mathbb{M}_\gamma \subset \mathbb{L}_0$ une chaine de sous-modules de $\mathbb{L}_0$. Alors $\gamma \leq m\delta$.

Calcul de $\mathbb{B}_0$

$\rightsquigarrow$ $\mathbb{B}_0$ est la plus petite algèbre qui contient $\mathbb{M}_0$ et $x_3, \ldots, x_n$.

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

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

Algorithme

– soit $\mathbb{M} = \mathbb{M}_0 (= K[[x_1]] \oplus \cdots \oplus K[[x_1]]x_2^{\delta-1})$;
– calculer $\mathbb{M}' = \mathbb{M} + K[[x_1]]x_3 + \cdots + K[[x_1]]x_n$;
– tant que $\mathbb{M} \neq \mathbb{M}'$,
  – $\mathbb{M} = \mathbb{M}'$, donné par une base $e_1, \ldots, e_\delta$,
  – $\mathbb{M}' = \mathbb{M} + \sum_{1 \le i,j \le \delta} K[[x_1]]e_i e_j$.

Coût

Le calcul de $\mathbb{B}_0$ coute $\tilde{\mathcal{O}}((n+m)m\delta^5)$ opérations dans K.

Conclusion

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

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

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 $f_1, \ldots, f_s$.