

Chapitre 1

Triangularisation de systèmes de polynômes différentiels

François Boulier¹

1.1 Introduction

L'algèbre différentielle est une généralisation de l'algèbre commutative destinée à l'étude des systèmes d'équations différentielles ordinaires ou aux dérivées partielles. Les premiers pas de la théorie sont dus à des chercheurs Français (Riquier et Janet [Riq10, Jan20, Jan29]) et Américains (Ritt [Rit32]). La discipline a ensuite principalement été développée par les équipes de Ritt et Kolchin dont les résultats sont synthétisés dans [Rit50, Kol73]. Elle a connu un regain d'intérêt en France depuis les années 80 avec les travaux de Pommaret [Pom78] d'une part et de Fliess [Fli89] d'autre part. Dans ce chapitre, nous présentons un algorithme de « résolution » de systèmes d'équations différentielles polynomiales, nommé Rosenfeld–Gröbner [Bou94, BLOP95, BLOP97]. Il est implanté dans le paquetage `diffalg` qui fait partie de la bibliothèque standard de MAPLE V version 5.

Résoudre un système de polynômes différentiels

Le système suivant comporte trois équations aux dérivées partielles polynomiales. On cherche deux fonctions $u(x, y)$ et $v(x, y)$ dépendant de deux variables x et y . Les équations sont des polynômes en les dérivées des fonctions u et v .

$$\Sigma : \left(\frac{\partial u}{\partial x} \right)^2 - 4u = 0, \quad \left(\frac{\partial^2 u}{\partial x \partial y} \right) \left(\frac{\partial v}{\partial y} \right) - u + 1 = 0, \quad \frac{\partial^2 v}{\partial x^2} - \frac{\partial u}{\partial x} = 0.$$

L'algorithme Rosenfeld–Gröbner permet de transformer ce système en un système plus simple à partir duquel il est possible de déterminer le nombre de

1. Université Lille I, LIFL, 59655 Villeneuve d'Ascq CEDEX.

constantes arbitraires dont dépendent les solutions et d'en calculer des développements de Taylor. Sur l'exemple, les solutions sont des polynômes dépendant de trois constantes arbitraires c_0 , c_1 et c_2 . Un développement de Taylor au voisinage de l'origine fournit :

$$\begin{aligned} u(x, y) &= c_0 + c_3 x + c_4 y + x^2 + \frac{2c_4}{c_3} xy + \frac{1}{2} y^2, \\ v(x, y) &= c_1 + c_2 x - \frac{c_4 c_3 - c_4 c_3 c_0}{4c_0} y + \frac{c_3}{2} x^2 + c_4 xy \\ &\quad + \frac{c_0}{c_3} y^2 + \frac{1}{3} x^3 + \frac{c_4}{c_3} x^2 y + \frac{1}{2} xy^2 + \frac{c_4}{6c_3} y^3. \end{aligned}$$

Les constantes c_3 et c_4 sont algébriques sur c_0, c_1, c_2 et satisfont²

$$c_3^2 = 4c_0, \quad c_4^2 = 2c_0, \quad c_0 \neq 0.$$

Posons qu'une équation différentielle est conséquence des équations de Σ si elle s'annule sur toutes les solutions du système, c'est-à-dire si on peut la rajouter au système sans en changer les solutions. C'est ici le cas de l'équation

$$\left(\frac{\partial u}{\partial y}\right)^2 - 2u = 0.$$

Les solutions de Σ satisfont cette équation pour toutes les valeurs de x et de y et en particulier à l'origine :

$$\left(\frac{\partial u}{\partial y}(0, 0)\right)^2 - 2u(0, 0) = 0,$$

ce qui impose une contrainte algébrique entre deux coefficients du développement de Taylor des solutions de Σ . Pour calculer ce dernier, Rosenfeld-Gröbner est donc amené à déterminer toutes les équations différentielles conséquences du système, même celles qui sont « cachées ». Cet ensemble forme ce qu'on appelle un idéal de polynômes différentiels. C'est le radical de l'idéal différentiel engendré par Σ . Nous le notons

$$\sqrt{[\Sigma]}.$$

L'algorithme Rosenfeld-Gröbner résout le problème d'algèbre différentielle suivant : étant donnée une famille finie de polynômes différentiels Σ , construire un simplificateur qui réécrit à zéro tout polynôme différentiel appartenant au radical de l'idéal différentiel engendré par Σ :

$$p \in \sqrt{[\Sigma]} \quad \text{ssi} \quad p \xrightarrow{*} 0.$$

2. La contrainte $c_0 \neq 0$ est en fait superflue.

Rosenfeld–Gröbner décide du vide c’est-à-dire si $1 \in \sqrt{[\Sigma]}$. La possibilité de calculer des développements de Taylor de solutions de Σ n’est qu’un sous-produit de la propriété énoncée ci-dessus. Les habitués des bases de Gröbner remarqueront que cette situation est similaire à celle de l’algorithme de Buchberger, qui résout un problème théorique d’algèbre commutative (décider de l’appartenance à un idéal de polynômes) et fournit en sous-produit des algorithmes de résolution de systèmes polynomiaux.

Les théorèmes importants

Le théorème clef est un lemme, dû à Rosenfeld [Ros59], qui améliore un théorème démontré et utilisé par Seidenberg [Sei56] pour prouver son algorithme d’élimination pour des systèmes d’équations aux dérivées partielles polynomiales. Le lemme de Rosenfeld donne une condition suffisante pour qu’un système d’équations aux dérivées partielles ait une solution différentielle si et seulement s’il a une solution, vu en tant que système purement algébrique dans l’espace des jets. On peut penser que si Seidenberg ou Rosenfeld n’ont pas formulé dans les années 50 l’algorithme présenté dans ce chapitre, c’est qu’il leur manquait les algorithmes de résolution de systèmes polynomiaux. La thèse de Buchberger [Buc65] date de 1965.

Parmi les théorèmes importants, citons aussi le lemme de Lazard [BLOP95] qui date de 1994 et qui montre que si un système de polynômes différentiels satisfait le lemme de Rosenfeld alors l’idéal qu’il définit a d’excellentes propriétés (entr’autres, il est radiciel).

Applications

L’algorithme Rosenfeld–Gröbner permet de faire de l’élimination dans les idéaux différentiels.

- Éliminer une fonction et ses dérivées présente un grand intérêt en automatique non linéaire comme l’ont montré Fliess [Fli89] et les chercheurs [Dio89] qui ont travaillé avec lui. L’élimination de variables d’état dans un système dynamique permet, par exemple, d’en définir le comportement entrée-sortie.
- Éliminer les variables les plus dérivées permet d’obtenir les contraintes algébriques cachées des systèmes d’équations différentielles algébriques (DAE et PDAE).
- Éliminer des dérivations permet de rechercher la présence d’équations différentielles ordinaires dans un système aux dérivées partielles, pour en simplifier la résolution.

Disposer d'un solveur non linéaire permet enfin de traiter des systèmes linéaires dépendant de paramètres. L'algorithme discute alors le résultat en fonction des paramètres. Nous donnons un exemple en fin de chapitre.

Le paquetage `difalg`

Le paquetage `difalg`, qui contient une implantation assez travaillée de Rosenfeld–Gröbner, fait partie de la bibliothèque standard de MAPLE V version 5. Il a été initialement écrit par l'auteur puis amélioré par Évelyne Hubert qui a inclus une implantation du Low Power Theorem [Hub97] et a retravaillé la partie purement algébrique de Rosenfeld–Gröbner qui s'applique aux systèmes satisfaisant la condition de Rosenfeld. Elle a aussi beaucoup contribué à diffuser le paquetage et à le faire interagir avec d'autres fonctions de MAPLE V.

Autres algorithmes existant

De nombreux autres algorithmes que Rosenfeld–Gröbner ont été proposés.

Les algorithmes d'élimination de Seidenberg [Sei56] résolvent le même problème que nous : ils permettent de décider si un polynôme différentiel appartient au radical d'un idéal différentiel de type fini mais sont inutilisables en pratique, parce qu'ils retournent un booléen et pas une version simplifiée du système donné en entrée. Il y a toutefois une filiation directe entre les méthodes de Seidenberg et l'algorithme que nous exposons.

Ritt [Rit50] a proposé un algorithme reposant sur des factorisations au-dessus de tours d'extensions algébriques. Wu Wen Tsün [Wu 87] a décrit une variante de l'algorithme de Ritt, sans factorisations, mais fournissant un résultat plus faible. L'algorithme de Wu Wen Tsün ne décide pas du vide par exemple. Dongming Wang [Wan94] a plus tard développé les idées de Wu et de Seidenberg pour systèmes différentiels ordinaires et proposé récemment [LW99] une variante de Rosenfeld–Gröbner pour les systèmes aux dérivées partielles.

Ollivier [Oll90] et Carra–Ferro [CF87] ont généralisé l'algorithme de Buchberger aux systèmes d'équations différentielles. Les bases de Gröbner définies par ces auteurs peuvent toutefois être infinies.

Mansfield [Man91] a proposé une autre définition de bases de Gröbner différentielles. Son algorithme, qui s'applique aussi aux systèmes aux dérivées partielles, termine dans tous les cas mais ne garantit pas que le résultat calculé soit bien une base de Gröbner différentielle. À ce propos, on peut remarquer que l'appartenance à un idéal différentiel de type fini est toujours ouvert [GMO91].

Bouziane, Kandri Rody et Maârouf [BKM96, Maâ96] ont mis au point des algorithmes proches de Rosenfeld–Gröbner, à partir de l'algorithme de triangularisation de Kalkbrener [Kal93].

Hubert [Hub00] a clarifié la partie purement algébrique de l'algorithme Rosenfeld–Gröbner et a proposé une variante d'un algorithme de Kolchin (dont

certaines parties n'étaient pas effectives) en s'appuyant sur le lemme de Lazard et son lifting pour l'algèbre différentielle.

Sadik [Sad00] a récemment rédigé une description très synthétique des algorithmes [BLOP95, BKM96, BLOP97, Hub00] entièrement fondée sur [Kol73].

Reid, Wittkopf, Lin et Boulton [RWB94, RLW96] ont développé des algorithmes de simplification de systèmes d'équations aux dérivées partielles et ont montré comment calculer des développements de Taylor de leurs solutions. Leurs algorithmes ne permettent toutefois pas de traiter des systèmes quelconques.

Organisation du chapitre

La section 1.2 présente les premières définitions. La section 1 est dédiée à la notion de solution d'un système d'équations différentielles polynomiales. On y présente une version différentielle du théorème des zéros de Hilbert. Les systèmes différentiels qui satisfont les hypothèses du lemme de Rosenfeld sont présentés en section 1.3.3 avec les principaux théorèmes qui les concernent. En section 1.4 nous donnons les spécifications de l'algorithme Rosenfeld–Gröbner ainsi que plusieurs implantations : de la plus naïve, peu efficace mais simple à comprendre, jusqu'aux implantations les plus récentes. Quelques exemples sont traités en section 1.7.

1.2 Éléments d'algèbre différentielle

1.2.1 Rappels d'algèbre commutative

Un idéal \mathfrak{a} d'un anneau R est un sous-ensemble non vide de R vérifiant

$$\begin{aligned} a, b \in \mathfrak{a} &\Rightarrow a + b \in \mathfrak{a} \\ a \in \mathfrak{a} \text{ et } b \in R &\Rightarrow ab \in \mathfrak{a} \end{aligned}$$

Un idéal \mathfrak{a} est dit *radiciel* si $a \in \mathfrak{a}$ dès qu'il existe un entier $n > 0$ tel que $a^n \in \mathfrak{a}$. Il est dit *premier* si $ab \in \mathfrak{a}$ implique $a \in \mathfrak{a}$ ou $b \in \mathfrak{a}$. On note $\sqrt{\mathfrak{a}}$ le radical de l'idéal \mathfrak{a} , c'est-à-dire le plus petit idéal radiciel contenant \mathfrak{a} . Soit $S = \{s_1, \dots, s_t\}$ une famille finie de R , on note $\mathfrak{a} : S^\infty$ la *saturation* (à ne pas confondre avec le *résiduel* d'un idéal par un autre) de \mathfrak{a} par S c'est-à-dire l'idéal

$$\mathfrak{a} : S^\infty = \{a \in R \mid \exists e_1, \dots, e_t \in \mathbb{N} \text{ tels que } s_1^{e_1} \cdots s_t^{e_t} a \in \mathfrak{a}\}.$$

On a l'inclusion $\mathfrak{a} \subset \mathfrak{a} : S^\infty$. Si $A \subset R$ on note (A) le plus petit idéal de R contenant A .

Cas des anneaux de polynômes

Soient A un sous-ensemble fini d'un anneau de polynômes (mettons) $R = \mathbb{Q}[x_1, \dots, x_n]$ et V l'ensemble des solutions, prises dans \mathbb{C}^n , du système $A = 0$. Alors $\sqrt{(A)}$ est l'idéal des polynômes qui s'annulent en tout point de V . Soit de plus S un sous-ensemble fini de R et Z l'ensemble des solutions, prises dans \mathbb{C}^n , du système $A = 0, S \neq 0$. Alors l'idéal $\sqrt{(A) : S^\infty}$ est l'idéal des polynômes qui s'annulent en tout point de Z . C'est le théorème des zéros qui est utilisé implicitement ici.

1.2.1.1 Polynômes

Soit $R = K[X]$ un anneau de polynômes où K est un corps et X est un alphabet (éventuellement infini) ordonné. Soit $p \in R \setminus K$ un polynôme. L'indéterminée principale (le *leader* en Anglais) de p est la plus grande indéterminée $x \in X$ qui figure dans p . Nous la notons $\text{ld } p$. Le polynôme p peut s'écrire

$$p = a_d x^d + \dots + a_1 x + a_0$$

où les polynômes a_i ne comportent pas l'indéterminée x et $a_d \neq 0$. L'entier $d = \deg(p, x)$ est le degré de p en l'indéterminée x . Le rang de p est le monôme $\text{rang } p = x^d$. Le polynôme $i_p = a_d$ est l'*initial* de p . Le *séparant* de p est le polynôme

$$s_p = \frac{\partial p}{\partial x} = d a_d x^{d-1} + \dots + a_1.$$

Si $A \subset R \setminus K$ alors le rang de A est l'ensemble des rangs de ses éléments. On note I_A (resp. S_A) l'ensemble des initiaux (resp. des séparants) des éléments de A . On note $H_A = I_A \cup S_A$. Un sous-ensemble A de $R \setminus K$ est dit *triangulaire* si ses éléments ont des dérivées dominantes distinctes.

1.2.1.2 Pseudo-division

Soient $f = f_m x^m + \dots + f_1 x + f_0$ et $g = g_n x^n + \dots + g_1 x + g_0$ deux polynômes en une indéterminée x et à coefficients dans un anneau R . Il existe un unique couple (q, r) de polynômes de $R[x]$ vérifiant

$$\begin{aligned} g_n^{n-m+1} f &= g q + r, \\ \deg(r, x) &< \deg(g, x). \end{aligned}$$

Le polynôme q est le pseudo-quotient, le polynôme r est le pseudo-reste de la pseudo-division de f par g . L'algorithme de pseudo-réduction est présenté dans [Knu66, vol. 2, page 407]. On note $r = \text{prem}(f, g, x)$.

1.2.2 Algèbre différentielle

Les ouvrages de référence sont [Rit50] et [Kol73]. Une dérivation sur un anneau R est une application δ de R dans R qui vérifie pour tous $a, b \in R$

$$\begin{aligned}\delta(a + b) &= \delta a + \delta b \\ \delta(ab) &= (\delta a)b + a\delta b \quad (\text{règle de Leibniz})\end{aligned}$$

Un *anneau différentiel* est un anneau muni d'un nombre fini de dérivations $\delta_1, \dots, \delta_m$ qui commutent entr'elles. Un anneau différentiel *ordinaire* est un anneau muni d'une seule dérivation.

Exemple \triangleright Tout anneau peut être muni d'une structure différentielle: il suffit de le munir de la dérivation triviale, qui envoie tous ses éléments sur 0. Le corps $\mathbb{Q}(x)$ muni de la dérivation $\partial/\partial x$ est un exemple de corps différentiel (ordinaire). \triangleleft

On note Θ le monoïde commutatif engendré par les dérivations. Ses éléments sont les *opérateurs de dérivations* $\theta = \delta_1^{a_1} \dots \delta_m^{a_m}$ où les a_i sont des entiers positifs ou nuls. La somme des exposants a_i , appelée l'*ordre* de l'opérateur θ , est notée $\text{ord } \theta$. L'opérateur identité est l'unique opérateur d'ordre 0. Les autres opérateurs sont dits *propres*. Si $\theta = \delta_1^{a_1} \dots \delta_m^{a_m}$ et $\phi = \delta_1^{b_1} \dots \delta_m^{b_m}$ alors $\theta\phi = \delta_1^{a_1+b_1} \dots \delta_m^{a_m+b_m}$. Un *idéal différentiel* \mathfrak{a} de R est un idéal de R stable par dérivation, c'est-à-dire tel que

$$a \in \mathfrak{a} \Rightarrow \delta_i a \in \mathfrak{a} \quad (1 \leq i \leq m)$$

Soit Σ un sous-ensemble non vide de R . On note $[\Sigma]$ et $\sqrt{[\Sigma]}$ respectivement l'idéal différentiel et le radical de l'idéal différentiel engendré par Σ . Il s'agit respectivement du plus petit idéal différentiel et du plus petit idéal différentiel radical contenant Σ .

1.2.2.1 Polynômes différentiels

Soit $U = \{u_1, \dots, u_n\}$ un ensemble de n *indéterminées différentielles*. Les opérateurs de dérivation agissent sur les indéterminées différentielles, donnant des *dérivées* θu . Si θu et ϕu sont deux dérivées d'une même indéterminée différentielle on note $\text{ppcd}(\theta u, \phi u) = \text{ppcm}(\theta, \phi) u$ leur plus petite dérivée commune.

On note ΘU l'ensemble des dérivées. Soit K un corps différentiel. L'anneau différentiel des polynômes différentiels construits sur l'alphabet ΘU et à coefficients dans K est noté $K\{u_1, \dots, u_n\}$. Dans la suite, nous le noterons R .

Exemple ▷ Reprenons l'exemple donné en introduction avec une autre notation. Il comporte trois polynômes différentiels

$$\Sigma \begin{cases} p_1 = u_x^2 - 4u, \\ p_2 = u_{xy}v_y - u + 1, \\ p_3 = v_{xx} - u_x. \end{cases}$$

Il y a deux dérivations ∂/∂_x et ∂/∂_y et deux indéterminées différentielles u et v représentant moralement deux fonctions $u(x, y)$ et $v(x, y)$ de deux variables. On peut prendre pour corps des coefficients K le corps \mathbb{Q} des rationnels ou le corps des fractions rationnelles $\mathbb{Q}(x, y)$. L'anneau de polynômes différentiels est $K\{u, v\}$, les dérivées figurant dans le système sont u_x, u, u_{xy}, v_y et v_{xx} . Les opérateurs de dérivation sont notés en indice. Par exemple, $u_x = \partial u/\partial x$ et $u_{xy} = \partial^2 u/\partial x \partial y$. ◀

Classements (rankings)

Un *classement* (en Anglais un *ranking*) est un ordre total sur l'ensemble des dérivées, compatible avec l'action des dérivations sur ΘU . Il s'agit donc de n'importe quel ordre total sur ΘU vérifiant :

1. $\delta v > v$ (pour toute dérivation δ et toute dérivée v)
2. $v > w \Rightarrow \delta v > \delta w$ (pour toute dérivation δ et toutes dérivées v et w)

On distingue les classements compatibles avec l'ordre total (en Anglais *orderly*), c'est-à-dire vérifiant

$$\text{ord } \theta > \text{ord } \phi \Rightarrow \theta u > \phi v \quad \text{pour tous } u, v \in U$$

des classements d'élimination qui satisfont

$$u > v \Rightarrow \theta u > \phi v \quad \text{pour tous } \theta, \phi \in \Theta \text{ et } u, v \in U.$$

Une fois fixé un classement, on peut définir la *dérivée dominante* d'un polynôme différentiel p : c'est l'indéterminée principale (le leader) de p , vu comme un polynôme sur l'alphabet infini des dérivées. L'initial et le séparant d'un polynôme différentiel sont alors bien définis. Les axiomes des classements font que le séparant d'un polynôme différentiel f est égal à l'initial de toutes les dérivées propres de f .

Exemple ▷ Fixons le classement \mathcal{R} suivant, compatible avec l'ordre total :

$$\dots > v_{xx} > v_{xy} > v_{yy} > u_{xx} > u_{xy} > u_{yy} > v_x > v_y > u_x > u_y > v > u.$$

Les dérivées dominantes des éléments de Σ sont respectivement u_x, u_{xy}, v_{xx} ; les rangs u_x^2, u_{xy}, v_{xx} ; les séparants $2u_x, v_y$ et 1. Dérivons le polynôme p_1 par rapport à y :

$$\delta_y p_1 = 2u_x u_{xy} - 4u_y.$$

On vérifie que l'initial de ce polynôme est bien le séparant de p_1 . ◀

Polynômes (partiellement) réduits

Soit $p \in R \setminus K$ et $q \in R$ deux polynômes différentiels. Notons $\text{rang } p = v^d$. Le polynôme différentiel q est dit *partiellement réduit* par rapport à p si aucune dérivée propre de la dérivée dominante de p ne figure dans q ; il est dit *réduit* par rapport à p s'il est partiellement réduit par rapport à p et si $\text{deg}(q, v) < d$.

Ensembles différentiellement triangulaires et autoréduits

Soit $R = K\{U\}$ un anneau de polynômes différentiels. Un ensemble $A \subset R \setminus K$ est dit *différentiellement triangulaire* s'il est triangulaire et si ses éléments sont deux-à-deux partiellement réduits. Un ensemble $A \subset R \setminus K$ est dit *autoréduit* si ses éléments sont réduits deux-à-deux. Tout ensemble autoréduit est différentiellement triangulaire.

Ensembles caractéristiques

Soit $A \subset K\{U\}$ un ensemble de polynômes. Supposons que A ne contienne aucun élément non nul de K . Alors un sous-ensemble C de A est un *ensemble caractéristique* de A s'il est autoréduit et si A ne contient aucun élément non nul réduit par rapport à C .

Exemple \triangleright Continuons l'exemple précédent. Le polynôme différentiel p_2 n'est pas partiellement réduit par rapport à p_1 puisqu'une dérivée propre u_{xy} de la dérivée dominante u_x de p_1 y figure. Le système Σ n'est donc pas différentiellement triangulaire. Les polynômes p_1 et p_3 sont réduits deux-à-deux. On peut vérifier que $\{p_1, p_3\}$ forme un ensemble caractéristique de Σ . \triangleleft

Si $A \subset R \setminus K$ et si $v \in \Theta U$ alors

$$A_v = \{\theta p \mid p \in A, \theta \in \Theta \text{ et } \text{ld } \theta p \leq v\}.$$

Par conséquent, R_v désigne le sous anneau de R constitué par les polynômes différentiels de dérivée dominante inférieure ou égale à v et

$$A \cap R_v = \{p \in A \mid \text{ld } p \leq v\}.$$

1.2.2.2 Les algorithmes de réduction de Ritt

Les algorithmes de réduction de Ritt sont des extensions de l'algorithme de pseudo-réduction aux polynômes différentiels : on s'autorise à dériver les polynômes par lesquels on divise. On distingue l'algorithme de *réduction partielle* de l'algorithme de *réduction complète*. Soient $f \in R$ un polynôme différentiel et A un sous-ensemble fini de $R \setminus K$. Notons v la dérivée dominante de f et $\bar{A} = \{g \in A \mid \text{rang } g \leq v\}$. L'algorithme de réduction partielle de f par A

calcule un polynôme différentiel $r = \text{reste_partiel}(g, A)$ et un produit h de puissances de séparants d'éléments de A vérifiant

1. r est partiellement réduit par rapport à \overline{A} ,
2. $hf = r \pmod{(\overline{A}_v)}$.

fonction $\text{reste_partiel}(f, A)$

début

$h := 1$

$r := f$

tant que r n'est pas partiellement réduit par rapport à

tous les éléments de A faire

soit w la plus grande dérivée figurant dans r qui soit aussi

la dérivée propre de la dérivée dominante d'un élément $p \in A$

soit $\theta \in \Theta$ tel que $\theta \text{ld } p = w$

$h := h s_p^{\text{deg}(r,w)}$

$r := \text{prem}(r, \theta p, w)$

fait

retourner $[h, r]$

fin

L'algorithme de réduction complète de f par A calcule un polynôme différentiel $r = \text{reste_complet}(g, A)$ et un produit h de puissances d'initiaux et de séparants d'éléments de A vérifiant

1. r est réduit par rapport à \overline{A} ,
2. $hf = r \pmod{(\overline{A}_v)}$.

fonction $\text{reste_complet}(f, A)$

début

$h := 1$

$r := f$

tant que r n'est pas réduit par rapport à tous les éléments de A faire

soit w la plus grande dérivée figurant dans r qui vérifie

aussi l'une des conditions suivantes

(a) w est la dérivée propre de la dérivée dominante d'un élément $p \in A$

(b) w est égale à la dérivée dominante d'un $p \in A$ et $\text{deg}(r, w) \geq \text{deg}(p, w)$

si la condition (a) est remplie alors

soit $\theta \in \Theta$ tel que $\theta \text{ld } p = w$

$h := h s_p^{\text{deg}(r,w)}$

$r := \text{prem}(r, \theta p, w)$

sinon

```

    h := h v_p^{deg(r,w)-deg(p,w)+1}
    r := prem(r, p, w)
  fin si
  fait
  retourner [h, r]
fin

```

Exemple ▷ Considérons le polynôme différentiel $f = 2u_{xy} + u_x$ et calculons le polynôme `reste_partiel(f, Σ)`. La dérivée dominante u_{xy} de f est une dérivée propre de la dérivée dominante u_x de p_1 . On dérive donc p_1 par rapport à y obtenant un polynôme différentiel

$$\delta_y p_1 = 2u_x u_{xy} - 4u_y.$$

Le calcul de $r = \text{prem}(f, \delta_y p_1, u_{xy})$ consiste à interpréter $\delta_y p_1$ comme la règle de réécriture

$$u_{xy} \rightarrow \frac{4u_y}{2u_x}$$

et à multiplier le résultat par une puissance appropriée du séparant de p_1 (le polynôme h) pour chasser les dénominateurs. Le reste

$$r = u_x^2 + 4u_y$$

est partiellement réduit par rapport à Σ . Notons $w = u_{xy}$ la dérivée dominante de f . Alors $\bar{\Sigma} = \{p_1, p_2\}$ et $\bar{\Sigma}_w = \{p_1, \delta_y p_1, p_2\}$. On peut vérifier que $hf = r \pmod{(\bar{\Sigma}_w)}$. Le calcul de `reste_complet(f, A)` commence comme ci-dessus. Le reste r n'est pas réduit par rapport à p_1 . Il suffit de lui appliquer la substitution

$$u_x^2 \rightarrow 4u$$

pour obtenir le nouveau reste $4u_y + 4u$ avec $h = 2u_x$. ◁

1.2.2.3 Paires critiques et Δ -polynômes

Définition 1 (paires critiques)

Un ensemble $\{p_1, p_2\}$ de polynômes différentiels forme une paire critique si les dérivées dominantes de p_1 et de p_2 ont des dérivées communes. Si A est un ensemble de polynômes différentiels alors `paires_critiques(A)` désigne l'ensemble de toutes les paires critiques qu'il est possible de former avec ses éléments.

Dans une paire critique, l'ordre des éléments est sans importance. On ne considérera jamais de paires critiques $\{p_1, p_2\}$ telle que $\text{rang } p_1 = \text{rang } p_2$ (par

contre, il se peut que les dérivées dominantes soient égales). Si la dérivée dominante de (mettons) p_2 est une dérivée de celle de p_1 alors la paire est appelée une *paire de réduction*.

Définition 2 (Δ -polynômes)

Soit $\{p_1, p_2\}$ une paire critique. Supposons $\text{rang } p_1 < \text{rang } p_2$. Notons respectivement $\theta_1 u$, $\theta_2 u$ les dérivées dominantes de p_1 et de p_2 et $\theta_{12} u$ leur plus petite dérivée commune. Le Δ -polynôme $\Delta(p_1, p_2)$ entre p_1 et p_2 est défini comme suit. Si $\{p_1, p_2\}$ est une paire de réduction alors

$$\Delta(p_1, p_2) = \text{prem}(p_2, \frac{\theta_2}{\theta_1} p_1, \theta_2 u) ;$$

sinon

$$\Delta(p_1, p_2) = s_1 \frac{\theta_{12}}{\theta_2} p_2 - s_2 \frac{\theta_{12}}{\theta_1} p_1.$$

Si A est un ensemble de polynômes différentiels, $\Delta(A)$ désigne l'ensemble de tous les Δ -polynômes qu'il est possible de former à partir de ses éléments.

Exemple \triangleright On a $\text{paires_critiques}(\Sigma) = \{\{p_1, p_2\}\}$. La paire $\{p_1, p_2\}$ est une paire de réduction et

$$\Delta(p_1, p_2) = \text{reste_complet}(p_2, \delta_y p_1) = 4u_y v_y - 2u u_x + 2u_x.$$

Ce polynôme (appelons-le p_4) admet v_y pour dérivée dominante. Son séparant est $s_4 = 4u_y$. Il forme une paire qui n'est pas une paire de réduction avec p_3 et on a

$$\begin{aligned} \Delta(p_3, p_4) &= \delta_{xx} p_4 - s_4 \delta_y p_3 \\ &= 2u_{xxx} - 2u_{xxx} u - 6u_{xx} u_x + 4u_{xy} v_y + 8u_{xy} v_{xy} + 4u_y u_{xy}. \end{aligned}$$

\triangleleft

Moralement, une paire $\{p_1, p_2\}$ est dite *résolue* par un système différentiel A si on a $\text{reste_complet}(\Delta(p_1, p_2), A) = 0$. Cette définition intuitive n'est malheureusement pas suffisante pour rendre compte de ce que l'algorithme Rosenfeld-Gröbner calcule. Plus rigoureusement,

Définition 3 (paires critiques résolues)

Une paire critique $\{p_1, p_2\}$ est dite résolue par un système d'équations et d'inéquations polynomiales différentielles $A = 0$, $S \neq 0$ s'il existe une dérivée v strictement inférieure à la plus petite dérivée commune des dérivées dominantes de p_1 et de p_2 telle que

$$\Delta(p_1, p_2) \in (A_v) : (S \cap R_v)^\infty.$$

Le lecteur peut vérifier que toute paire critique résolue selon le sens intuitif est résolue au sens de la définition 3, sous réserve que les initiaux des éléments de A fassent partie de S .

1.3 Solutions d'un système

Nous commençons par le « point de vue de la théorie », c'est-à-dire les définitions et les constructions rigoureuses. Nous tenterons de rendre ce point de vue plus intuitif ensuite.

Définition 4 On appelle solution d'un système $A = 0, S \neq 0$ d'équations et d'inéquations polynomiales différentielles de $R = K\{u_1, \dots, u_n\}$ la donnée

1. d'une extension de corps différentielle G de K ,
2. d'un n -uplet $z = (\bar{u}_1, \dots, \bar{u}_n) \in G^n$ qui annule tous les éléments de A et aucun élément de S .

1.3.1 Lien avec les idéaux différentiels premiers

Trouver une solution de $A = 0, S \neq 0$, c'est trouver un idéal différentiel premier \mathfrak{p} qui contient tous les éléments de A et aucun élément de S . En effet, le corps des fractions G de R/\mathfrak{p} constitue une extension de corps différentielle de K ; le n -uplet z s'obtient en prenant les images des indéterminées différentielles par le morphisme canonique $R \rightarrow G$. Cet argument est parfaitement correct mais n'explique pas grand-chose (il est qualifié d'*algebraic nonsense* par certains!). Un point de vue plus proche de l'intuition consiste à définir une solution comme un n -uplet de séries formelles³

$$\sum c_{k_1 \dots k_m} x_1^{k_1} \dots x_m^{k_m}$$

à coefficients dans une extension universelle de K ou dans \mathbb{C} si on préfère. Il faut alors assimiler les dérivations δ_i aux dérivations $\partial/\partial x_i$. Cette définition est équivalente à celle donnée plus haut parce que tout zéro générique de l'idéal différentiel premier \mathfrak{p} peut être développé en série formelle. Nous expliquerons ultérieurement comment calculer des séries formelles solutions de \mathfrak{p} à partir d'un ensemble caractéristique de cet idéal.

1.3.2 Lien avec les idéaux différentiels radiciels

Toute solution d'un système Σ annule le radical $\sqrt{[\Sigma]}$ de l'idéal différentiel engendré par Σ . En effet,

- si $p(z) = q(z) = 0$ alors $(p + q)(z) = 0$,
- si $p(z) = 0$ alors quel que soit $q \in R$ on a $(pq)(z) = 0$,
- si $(p^d)(z) = 0$ alors $p(z) = 0$ (on utilise ici le fait que $p(z)$ appartient à un corps et ne peut donc pas diviser zéro),

³. une série formelle n'étant jamais qu'un développement de Taylor dont on ne se préoccupe pas de la convergence.

- si $p(z) = 0$ c'est-à-dire égal à la fonction identiquement nulle, alors $\delta p(z) = 0$ (les dérivées de la fonction nulle étant nulles).

Ces remarques suffisent à justifier l'implication de gauche à droite dans le théorème et le corollaire ci-dessous. L'autre implication vient de ce que le radical d'un idéal différentiel est un idéal différentiel radiciel et que tout idéal différentiel radiciel est l'intersection des idéaux différentiels premiers qui le contiennent [Sei52].

Théorème 1 (théorème des zéros)

Soit Σ un système de polynômes différentiels de $K\{U\}$. Un polynôme différentiel $p \in \sqrt{[\Sigma]}$ si et seulement si toute solution de Σ est solution de p . En particulier, Σ est sans solutions si et seulement si $1 \in \sqrt{[\Sigma]}$.

Corollaire 1 Soit $A = 0$, $S \neq 0$ un système d'équations et d'inéquations différentielles de $K\{U\}$. Un polynôme différentiel $p \in \sqrt{[A] : S^\infty}$ si et seulement si toute solution de $A = 0$, $S \neq 0$ est solution de p .

Exemple \triangleright On peut se servir du théorème des zéros pour montrer que l'idéal différentiel $[u_x^2 - 4u]$ n'est pas premier. L'équation $u_x^2 - 4u = 0$ admet deux solutions : la solution $u(x) = 0$ et la solution $u(x) = (x + c)^2$ où c est une constante. En dérivant, on trouve $\delta_x(u_x^2 - 4u) = 2u_x(u_{xx} - 2)$. Ce polynôme appartient à l'idéal différentiel. Son premier facteur ne s'annule pas sur la solution $u(x) = (x + c)^2$. D'après le théorème des zéros, il n'appartient pas au radical de l'idéal et donc pas non plus à l'idéal $[u_x^2 - 4u]$. Son deuxième facteur ne s'annule pas sur la solution $u(x) = 0$. Il n'appartient donc pas non plus à l'idéal. Donc l'idéal n'est pas premier et on a l'intersection :

$$\sqrt{[u_x^2 - 4u]} = [u_x^2 - 4u, u_{xx} - 2] \cap [u] = [u_x^2 - 4u] : u_x^\infty \cap [u].$$

\triangleleft

L'intersection ci-dessus est la décomposition en idéaux différentiels premiers *minimale* (au sens où aucune des composantes de l'intersection n'en contient une autre) de l'idéal différentiel radiciel $\sqrt{[u_x^2 - 4u]}$.

Théorème 2 Tout idéal différentiel radiciel \mathfrak{r} inclus strictement dans R est une intersection finie d'idéaux différentiels premiers $\mathfrak{p}_1, \dots, \mathfrak{p}_t$. Cette décomposition est unique lorsqu'elle est minimale. Les idéaux \mathfrak{p}_i sont appelés les composantes premières minimales de \mathfrak{r} .

On ne connaît aucun algorithme pour calculer la décomposition *minimale* d'un idéal différentiel radiciel, à l'exception du cas des idéaux différentiels engendrés par un seul polynôme différentiel pour lequel on dispose du *Low Power Theorem*.

1.3.3 Lien avec les idéaux différentiels réguliers

Dans cette partie, on s'intéresse au problème de la description *en pratique* des idéaux différentiels radiciels. Le calcul d'une décomposition (non minimale) en idéaux différentiels premiers est algorithmique mais coûteux, puisqu'il nécessite des factorisations de polynômes sur des tours d'extensions algébriques. Le calcul d'une décomposition en idéaux différentiels *réguliers* [BLOP97] offre une alternative plus intéressante du point de vue algorithmique. Les idéaux sont décrits par des ensembles ou des présentations⁴ caractéristiques.

Définition 5 (systèmes différentiels réguliers)

Un système différentiel $A = 0$, $S \neq 0$ est appelé un système différentiel régulier s'il vérifie les trois conditions suivantes :

- C1** A est différentiellement triangulaire⁵,
- C2** S contient les séparants des éléments de A et ne comporte que des polynômes différentiels partiellement réduits par rapport à A ,
- C3** toutes les paires critiques $\{p, p'\} \in \text{paires_critiques}(A)$ sont résolues⁶ par le système $A = 0$, $S \neq 0$ (propriété de cohérence).

Si $A = 0$, $S \neq 0$ est un système différentiel régulier, on appelle *idéal algébrique régulier* défini par le système l'idéal $(A) : S^\infty$ et *idéal différentiel régulier* l'idéal différentiel $[A] : S^\infty$.

Ensembles autoréduits et cohérents

Les ensembles autoréduits et cohérents définis dans [Ros59, Kol73] sont des cas particuliers de systèmes différentiels réguliers. Plus précisément, si C est un ensemble autoréduit et cohérent alors le système suivant est un système différentiel régulier

$$C = 0, H_C \neq 0.$$

Le théorème qui suit synthétise les principales propriétés des systèmes différentiels réguliers.

Théorème 3 Soient $A = 0$, $S \neq 0$ un système différentiel régulier d'un anneau de polynômes différentiels R et R_0 l'anneau des polynômes différentiels partiellement réduits par rapport à A . Alors

- l'idéal algébrique régulier $(A) : S^\infty$ est radiciel (lemme de Lazard) ;

4. définition plus bas

5. i.e. A est triangulaire et ses éléments sont deux-à-deux partiellement réduits.

6. C'est le cas par exemple si $I_A \subset S$ et si, pour toute paire critique $\{p, p'\} \in \text{paires_critiques}(A)$, on a $\text{reste_complet}(\Delta(p, p'), A) = 0$.

- l'ensemble des dérivées qui ne sont dérivées dominantes d'aucun élément de A fournit un ensemble paramétrique pour tout idéal premier minimal sur $(A) : S^\infty$; en particulier, l'idéal algébrique $(A) : S^\infty$ est équidimensionnel (lemme de Lazard) ;
- on a $[A] : S^\infty \cap R_0 = (A) : S^\infty$ (lemme de Rosenfeld) ;
- l'idéal différentiel $[A] : S^\infty$ est radiciel (lifting du lemme de Lazard) ;
- si $(A) : S^\infty$ admet t idéaux premiers minimaux \mathfrak{b}_i alors $[A] : S^\infty$ admet t idéaux différentiels premiers minimaux \mathfrak{p}_i qui sont complètement caractérisés par $\mathfrak{p}_i \cap R_0 = \mathfrak{b}_i$ (lifting du lemme de Lazard) ;
- le système $A = 0, S \neq 0$ admet une solution purement algébrique, vu comme un système de R_0 , si et seulement s'il admet une solution différentielle ;
- toute solution algébrique du système $A = 0, S \neq 0$, vu comme un système de R_0 , se prolonge de façon unique en une solution différentielle.

Le lemme de Lazard est énoncé pour la première fois dans [BLOP95], son lifting pour les idéaux différentiels dans [BLOP97]. La première preuve rigoureuse est due à [Mor95, Mor99]. D'autres preuves ont été fournies par [SL95, Hub00, Sad00].

1.3.4 Présentations caractéristiques

À l'instar des idéaux différentiels premiers qui en sont des cas particuliers, les idéaux différentiels réguliers peuvent être représentés par leurs ensembles caractéristiques. Comme ces derniers ne sont pas uniques, un choix de pose. Une *présentation caractéristique* d'un idéal différentiel régulier i est un représentant canonique parmi les ensembles caractéristiques de i . Cette notion a été introduite dans [BLOP97] puis clarifiée dans [Hub00] et [BL00].

Un polynôme différentiel p est dit *fortement normalisé* vis-à-vis d'un système triangulaire C si aucune dérivée dominante de C ne figure dans l'initial de p . Un système triangulaire C est dit *fortement normalisé* si tout $p \in C$ est fortement normalisé vis-à-vis de $C \setminus \{p\}$.

Soient L et N deux alphabets et considérons un polynôme $p \in K[L, N]$. Ce polynôme peut s'écrire $p = a_0 t_0 + \dots + a_k t_k$ où les t_i sont des produits de puissances d'éléments de L et les $a_i \in K[N]$. Il est dit *primitif au-dessus* de $K[N]$ si le pgcd des a_i vaut 1.

Définition 6 *Un ensemble autoréduit $C \subset R$ est une présentation caractéristique de l'idéal différentiel $[C] : H_C^\infty$ si*

D1 *le système différentiel $C = 0, H_C \neq 0$ est régulier ;*

D2 $p \in [C] : H_C^\infty \Leftrightarrow \text{reste_complet}(p, C) = 0 ;$

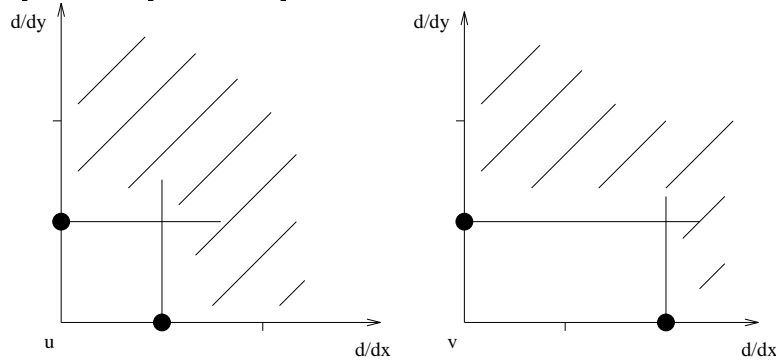
D3 C est un système fortement normalisé de $K[L, N]$ composé de polynômes primitifs au-dessus de $K[N]$ (où L désigne l'ensemble des dérivées dominantes des éléments de C et N les autres dérivées figurant dans C).

Un ensemble C est une présentation caractéristique de $[C] : H_C^\infty$ si et seulement si C est un ensemble caractéristique de $[C] : H_C^\infty$ qui satisfait **D3**. Une présentation caractéristique est un représentant canonique de l'idéal qu'elle définit : elle ne dépend que de l'idéal et du classement choisi.

Exemple $\triangleright C$ est une présentation caractéristique de l'idéal $[C] : H_C^\infty = \sqrt{[\Sigma]}$.

$$C \begin{cases} v_{xx} - u_x, \\ 4v_y u + u_x u_y - u_x u_y u, \\ u_x^2 - 4u, \\ u_y^2 - 2u. \end{cases}$$

L'ensemble $H_C = \{4u, 2u_x, 2u_y\}$ est l'ensemble des initiaux et séparants non constants des éléments de C . L'ensemble C est d'ailleurs aussi un ensemble caractéristique de $[C] : H_C^\infty$ puisqu'il est autoréduit. Les dérivées dominantes des éléments de C sont v_{xx}, v_y, u_x, u_y . Le diagramme suivant montre l'ensemble des dérivées des indéterminées différentielles u et v . Les dérivées dominantes sont représentées par des disques noirs. Leurs dérivées sont hachurées.

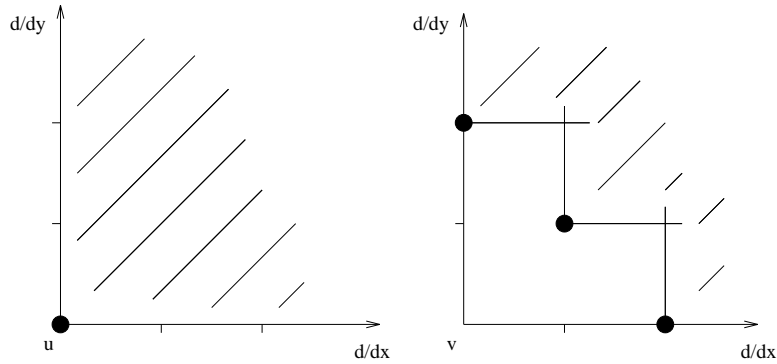


On appelle *dérivées sous les escaliers de C* les dérivées qui ne sont les dérivées d'aucune dérivée dominante de C . Ce sont celles qui figurent dans les zones non hachurées. Sur l'exemple, elles sont en nombre fini et ce sont u, v, v_x . On en déduit que le radical de l'idéal engendré par Σ est une intersection d'idéaux différentiels premiers \mathfrak{p}_i qui admettent tous $\{u, v, v_x\}$ pour ensemble paramétrique. Par conséquent les corps de fractions des anneaux R/\mathfrak{p}_i ont un degré de transcendance sur K égal à 3. Ce degré est un invariant de l'idéal $\sqrt{[\Sigma]}$: il ne dépend pas de la présentation caractéristique calculée. Par exemple, le système \tilde{C} est une présentation caractéristique du même idéal, pour

le classement d'élimination

$$\cdots > u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v.$$

$$\tilde{C} \begin{cases} u - v_{yy}^2, \\ v_{xx} - 2v_{yy}, \\ v_y v_{xy} - v_{yy}^3 + v_{yy}, \\ v_{yy}^4 - 2v_{yy}^2 - 2v_y^2 + 1. \end{cases}$$



Les dérivées sous les escaliers (i.e. v , v_x et v_y) ont changé mais leur nombre est resté le même. Ce nombre correspond au nombre de constantes arbitraires dont dépendent les développements de Taylor des solutions du système. \triangleleft

1.3.5 Développement de Taylor des solutions

La donnée d'un système régulier $A = 0$, $S \neq 0$ permet de calculer facilement un développement de Taylor des solutions du système pour des conditions initiales « non singulières », c'est-à-dire qui n'annulent pas les séparants des éléments de A . Une méthode simple, déjà décrite dans [Sei56] est exposée dans [BLOP97]. Nous l'illustrons sur l'exemple précédent.

$$A \begin{cases} v_{xx} - u_x, \\ 4v_y u + u_x u_y - u_x u_y u, \\ u_x^2 - 4u, \\ u_y^2 - 2u ; \end{cases}$$

avec $S = \{4u, 2u_x, 2u_y\}$. On est d'abord obligé de se restreindre à un point d'expansion (x_0, y_0) qui n'annule aucun des séparants de A . Dans notre cas, tous les points d'expansion conviennent. Prenons $x_0 = y_0 = 0$. On interprète le système différentiel comme un système algébrique portant sur les conditions

initiales, c'est-à-dire

$$A \begin{cases} v_{xx}(0,0) - u_x(0,0) = 0, \\ 4v_y(0,0)u(0,0) + u_x(0,0)u_y(0,0) - u_x(0,0)u_y(0,0)u(0,0) = 0, \\ u_x(0,0)^2 - 4u(0,0) = 0, \\ u_y(0,0)^2 - 2u(0,0) = 0, \\ 4u(0,0) \neq 0, \\ 2u_x(0,0) \neq 0, \\ 2u_y(0,0) \neq 0. \end{cases}$$

Ce système se résout simplement grâce au lemme de Lazard. On sait en effet qu'on peut prendre les conditions initiales associées aux dérivées sous l'escalier comme constantes arbitraires :

$$u(0,0) = c_0, \quad v(0,0) = c_1 \quad v_x(0,0) = c_2.$$

En notant $u_x(0,0) = c_3$ et $u_y(0,0) = c_4$ on retrouve les conditions algébriques données en introduction

$$c_3^2 = 4c_0, \quad c_4^2 = 2c_0$$

qui imposent $c_0 \neq 0$. Soit maintenant θu une dérivée propre de la dérivée dominante d'un élément de A . Pour déterminer $\theta u(0,0)$, il suffit de réduire cette dérivée grâce à l'algorithme de réduction partielle en une fraction

$$\theta u \rightarrow \frac{r}{h}$$

puis d'évaluer la fraction en les conditions initiales

$$\theta u(0,0) = \frac{r(0,0)}{h(0,0)}.$$

Le dénominateur est non nul puisqu'il est un produit de puissances de séparants d'éléments de A . Remarquer que la fraction r/h n'est pas définie de façon unique mais que sa valeur en les conditions initiales l'est : si θu se réécrit en une autre fraction r'/h' alors $r(0,0)/h(0,0) = r'(0,0)/h'(0,0)$. Il ne reste plus qu'à substituer les valeurs calculées dans le développement de Taylor générique de deux fonctions de deux variables

$$\begin{aligned} u(x,y) &= u(0,0) + x u_x(0,0) + y u_y(0,0) + x^2 \frac{u_{xx}(0,0)}{2} + \dots \\ v(x,y) &= v(0,0) + x v_x(0,0) + y v_y(0,0) + x^2 \frac{v_{xx}(0,0)}{2} + \dots \end{aligned}$$

pour obtenir les solutions du système données en introduction. On peut remarquer à ce propos que la condition initiale « singulière » $c_0 = 0$ est ici une fausse singularité.

1.4 L'algorithme Rosenfeld–Gröbner

L'algorithme Rosenfeld–Gröbner prend en entrée un système quelconque d'équations et d'inéquations polynomiales différentielles $P_0 = 0$, $S_0 \neq 0$ et un classement \mathcal{R} .

- Il retourne un ensemble, éventuellement vide, de systèmes différentiels réguliers pour le classement \mathcal{R} :

$$\{A_1 = 0, S_1 \neq 0, \dots, A_t = 0, S_t \neq 0\}$$

tels que

$$\sqrt{[P_0] : S_0^\infty} = [A_1] : S_1^\infty \cap \dots \cap [A_t] : S_t^\infty. \quad (1.1)$$

- L'ensemble est vide si et seulement si $\sqrt{[P_0] : S_0^\infty} = R$.
- Dans le paquetage `diffalg`, chaque système A_i est une présentation caractéristique de l'idéal différentiel $[A_i] : S_i^\infty$ et $S_i = H_{A_i}$.
- La représentation calculée permet de décider de l'appartenance à l'idéal $\sqrt{[P_0] : S_0^\infty}$. Soit p un polynôme différentiel. Dans le cas où chaque A_i est une présentation caractéristique,

$$p \in \sqrt{[P_0] : S_0^\infty} \text{ ssi } \text{reste_complet}(p, A_1) = \dots = \text{reste_complet}(p, A_t) = 0.$$

Dans le cas général,

$$p \in \sqrt{[P_0] : S_0^\infty} \text{ ssi } \begin{array}{l} \text{reste_partiel}(p, A_1) \xrightarrow[*]{B_1} 0, \\ \vdots \\ \text{reste_partiel}(p, A_t) \xrightarrow[*]{B_t} 0, \end{array}$$

où chaque B_i désigne une base de Gröbner de l'idéal $(A_i) : S_i^\infty$.

- La représentation calculée permet de calculer des développements de Taylor de solutions du système $P_0 = 0$, $S_0 \neq 0$.

Plusieurs versions de Rosenfeld–Gröbner sont décrites ci-dessous. Toutes ont été programmées en MAPLE V. La plus évoluée a également été réalisée en C++.

1.4.1 Une version naïve

La version ci-dessous est celle de [Bou94, BLOP95]. Elle est fortement inspirée des algorithmes d'élimination de Seidenberg [Sei56]. À chaque étape, l'algorithme extrait un ensemble caractéristique A de l'ensemble des équations et s'en sert pour réduire les équations restantes et tous les Δ -polynômes engendrés par les éléments de A . La boucle pour finale effectue les scindages en considérant la possible annulation des initiaux et séparants des éléments de A . Dans [Bou94, BLOP95], c'est la version la plus simple des traitements algébriques qui est effectuée.

fonction Rosenfeld-Gröbner ($A = 0, S \neq 0$)

début

si A contient un élément non nul de K ou $0 \in S$ alors

$\mathcal{F} :=$ l'ensemble vide

sinon

$\overline{A} :=$ un ensemble caractéristique de l'ensemble fini A

$\{h_1, \dots, h_t\} :=$ les initiaux et séparants non constants de \overline{A}

$B :=$ reste_complet($A \cup \Delta(\overline{A}), \overline{A}$)

si $B \setminus \{0\}$ est vide alors

$\overline{S} :=$ reste_partiel(S, \overline{A}) $\cup \{h_1, \dots, h_t\}$

$\mathcal{F} :=$ traitement_algébrique ($\overline{A} = 0, \overline{S} \neq 0$)

sinon

$A' := \overline{A} \cup B$

$S' := S \cup \{h_1, \dots, h_t\}$

$\mathcal{F} :=$ Rosenfeld-Gröbner ($A' = 0, S' \neq 0$)

fin si

pour i variant de t à 1 faire

$A' := A \cup \{h_i\}$

$S' := S \cup \{h_1, \dots, h_{i-1}\}$

$\mathcal{F} := \mathcal{F} \cup$ Rosenfeld-Gröbner ($A' = 0, S' \neq 0$)

fait

fin si

retourner \mathcal{F}

fin

Le théorème des zéros justifie les scindages effectués par la fonction ci-dessus. Considérons par exemple le système

$$\begin{cases} p = 0, \\ q = 0; \end{cases}$$

et mettons que $\overline{A} = \{p\}$ et que $A \cup \Delta(\overline{A}) = \{q\}$. Notons $r =$ reste_complet(q, p). On a la relation

$$i_p^\alpha s_p^\beta q = r \pmod{[p]}$$

où i_p et s_p désignent respectivement l'initial et le séparant de p et α, β sont des entiers naturels. Toute solution commune à p et à q est solution de r . Réciproquement, toute solution commune à p et à r qui n'annule ni l'initial ni le séparant de p est solution de q . Afin de préserver ses solutions, l'algorithme scinde le système en trois systèmes (dans les deux systèmes de droite, le polynôme q peut être réécrit en un polynôme de degré strictement plus petit) :

$$\left\{ \begin{array}{l} p = 0, \\ r = 0, \\ i_p s_p \neq 0 ; \end{array} \right. \quad \left\{ \begin{array}{l} p = 0, \\ q = 0, \\ i_p = 0, \\ s_p \neq 0 ; \end{array} \right. \quad \left\{ \begin{array}{l} p = 0, \\ q = 0, \\ s_p = 0. \end{array} \right.$$

En appliquant le théorème des zéros, on trouve :

$$\sqrt{[p, q]} = \sqrt{[p, r] : (i_p s_p)^\infty} \cap \sqrt{[p, q, i_p] : (s_p)^\infty} \cap \sqrt{[p, q, s_p]}.$$

1.4.2 Une version plus évoluée

Dans une branche de l'arbre des scindages engendré par la version naïve, un même Δ -polynôme peut être calculé et réduit de nombreuses fois. Ce n'est plus le cas dans la version qui suit : les paires critiques en attente sont rangées dans une liste. On obtient ainsi une implantation qui se rapproche des implantations traditionnelles de l'algorithme de Buchberger des années 80.

Quadruplets

Un système différentiel en cours de traitement est codé par un *quadruplet*

$$\langle A, D, P, S \rangle.$$

Informellement, A est l'ensemble des équations déjà traitées, D est un ensemble de paires critiques en attente d'être traitées, P est un ensemble de polynômes en attente d'être traités et S un ensemble d'inéquations. Soit à traiter le système $P_0 = 0$, $S_0 \neq 0$. On pose initialement $A = D = \emptyset$, $P = P_0$ et $S = S_0$. Le mécanisme de complétion s'arrête lorsque $D = P = \emptyset$. Reste alors à réduire partiellement les éléments de A entr'eux (fonction *autoréduction*) puis à appliquer le traitement algébrique final (fonction *traitement_algébrique*). Les scindages sont gérés au moyen d'une pile de quadruplets.

Les propriétés suivantes sont des invariants du « tant que » intérieur (certains invariants [BLOP97] ont été omis pour simplifier l'exposé). Soit $G = \langle A, D, P, S \rangle$ un quadruplet.

I1 Le rang de l'ensemble A est autoréduit.

I4 Si $p \in A$ ou si p appartient à une paire critique de D alors l'initial et le séparant de p appartiennent à S .

I6 Si $\{p, p'\} \in D$ est une paire critique alors $\text{rang } p \neq \text{rang } p'$.

fonction Rosenfeld-Gröbner ($P_0 = 0, S_0 \neq 0$)

début

résultat := \emptyset

empiler $\langle \emptyset, \emptyset, P_0, S_0 \rangle$

tant que la pile n'est pas vide faire

dépiler un quadruplet $\langle A, D, P, S \rangle$

inconsistant := faux

tant que non inconsistant et ($D \neq \emptyset$ ou $P \neq \emptyset$) faire

prendre au choix une nouvelle équation q_0 :

soit

q_0 := un élément de P

$P^* := P \setminus \{q_0\}$

$D^* := D$

soit

$\{p, p'\} :=$ un élément de D

$q_0 := \Delta(p, p')$

$P^* := P$

$D^* := D \setminus \{\{p, p'\}\}$

$q := \text{reste_complet}(q_0, A)$

si $q \in K$ alors

si $q = 0$ alors

$\langle A, D, P, S \rangle := \langle A, D^*, P^*, S \rangle$

sinon

inconsistant := vrai

fin si

sinon

posons $q = a_n v^n + a_{n-1} v^{n-1} + \dots + a_0$ où $v = \text{ld } q$

$q_i := a_{n-1} v^{n-1} + \dots + a_0$

$q_s := nq - v s_q$

empiler $\langle A, D^*, P^* \cup \{i_q, q_i\}, S \rangle$

empiler $\langle A, D^*, P^* \cup \{s_q, q_s\}, S \cup \{i_q\} \rangle$

$\langle A, D, P, S \rangle := \text{compléter}(\langle A, D^*, P^*, S \rangle, q)$

fin si

fait

si non inconsistant alors

résultat := résultat \cup autoréduction ($A = 0, S \neq 0$)

fin si

fait

retourner résultat

fin

La fonction qui suit considère le cas $q = 0, i_q s_q \neq 0$. Elle reçoit en pa-

ramètre un quadruplet $\langle A, D, P, S \rangle$ et un polynôme $q \notin K$ réduit par rapport à A . Elle retourne un quadruplet $\langle A', D', P', S' \rangle$ obtenu en insérant q dans A . Certains polynômes de A ne figurent pas dans A' . On les retrouve dans des paires de réduction de D' .

fonction compléter ($\langle A, D, P, S \rangle, q$)

début

$A' := \{q\} \cup \{p \in A \mid \text{ld } p \text{ n'est pas une dérivée de } \text{ld } q\}$
 $D' := D \cup \{\{q, p\} \mid p \in A \text{ et } \{q, p\} \text{ forme une paire critique}\}$
 $P' := P$
 $S' := S \cup \{i_q, s_q\}$
 retourner $\langle A', D', P', S' \rangle$

fin

La fonction suivante rend les polynômes de A partiellement réduits deux-à-deux et réduit partiellement les éléments de S par rapport à A . Le rang de A est déjà autoréduit (invariant **I1**). S'il dégénère, c'est que le système est inconsistant (invariant **I4**) sinon, le système différentiel $\overline{A} = 0, \overline{S} \neq 0$ obtenu est régulier. Il ne reste plus qu'à lui appliquer le traitement purement algébrique final.

fonction autoréduction ($A = 0, S \neq 0$)

début

inconsistant := faux
 $\overline{A} := A$
 tant que non inconsistant et des dérivées propres de dérivées dominantes
 d'éléments de \overline{A} figurent dans \overline{A} faire
 $\theta u :=$ la plus grande dérivée qui figure dans un $p \in \overline{A}$ et qui soit aussi
 une dérivée propre de la dérivée dominante $\theta' u$ d'un $p' \in \overline{A}$
 $\phi := \theta / \theta'$
 $\overline{p} := \text{reste_complet}(p, \phi p')$
 si $\text{rang } p \neq \text{rang } \overline{p}$ alors
 inconsistant := vrai
 sinon
 $\overline{A} := \overline{A} \setminus \{p\} \cup \{\overline{p}\}$
 fin si
 fait
 si inconsistant alors
 retourner \emptyset
 sinon
 $\overline{S} := \text{reste_partiel}(S, \overline{A}) \cup S_{\overline{A}}$
 retourner traitement_algébrique ($\overline{A} = 0, \overline{S} \neq 0$)

fin si

fin

1.4.3 La version du paquetage *diffalg*

Seule la réalisation de la fonction `compléter` change par rapport à la version précédente. Les spécifications de cette fonction ne changent pas. Elle met en œuvre des analogues des critères de Buchberger [Buc79], destinés à éviter des réductions inutiles de Δ -polynômes. L'application de ces critères (présentés après) permet non seulement d'éviter d'engendrer des paires critiques inutiles mais aussi de supprimer certaines paires critiques de D . Aucune paire de réduction ne peut être ainsi supprimée. Une justification théorique est donnée dans [BLOP97].

L'implantation obtenue se rapproche de l'implantation de l'algorithme de Buchberger par [GM88] Gebauer et Möller. Par exemple, si on lui fournit un système d'équations aux dérivées partielles linéaires, homogènes, à coefficients constants et dans lesquelles ne figurent que les dérivées d'une seule même indéterminée différentielle — système qui peut être vu comme un codage d'un système de polynômes usuels — l'implantation se comporte exactement comme celle de Gebauer et Möller (à un « overhead » près), telle qu'elle est décrite dans [BW91, page 230].

fonction `compléter` ($\langle A, D, P, S \rangle, q$)

début

$A' := \{q\} \cup \{p \in A \mid \text{ld } p \text{ n'est pas une dérivée de } \text{ld } q\}$

$D_a := \emptyset$

$D_b := \emptyset$

pour tout $p \in A$ tel que $\{p, q\}$ forme une paire critique faire

si la paire critique $\{p, q\}$ satisfait Buchberger-1 alors

$D_b := D_b \cup \{\{p, q\}\}$

sinon

$D_a := D_a \cup \{\{p, q\}\}$

fin si

fait

$D_1 := \emptyset$

tant que D_a n'est pas vide faire

$\{p, q\} :=$ un élément de D_a

$D_a := D_a \setminus \{\{p, q\}\}$

si il n'existe aucune paire critique $\{p', q\} \in D_a \cup D_b \cup D_1$ telle que
le triplet $\langle q, p', p \rangle$ satisfasse Buchberger-2 alors

$D_1 := D_1 \cup \{\{p, q\}\}$

fin si

fait

$D_2 := \emptyset$

pour toute paire critique $\{p, p'\} \in D$ faire

si $\text{ppcd}(\text{ld } p, \text{ld } p') = \text{ppcd}(\text{ld } p, \text{ld } q)$ ou $\text{ppcd}(\text{ld } p, \text{ld } p') = \text{ppcd}(\text{ld } p', \text{ld } q)$
ou si le triplet $\langle p, q, p' \rangle$ ne satisfait pas Buchberger-2 alors

```

       $D_2 := D_2 \cup \{p, p'\}$ 
    fin si
  fait
     $D' := D_1 \cup D_2$ 
     $P' := P$ 
     $S' := S \cup \{i_q, s_q\}$ 
  retourner  $\langle A', D', P', S' \rangle$ 
fin

```

Les deux critères suivants sont des analogues de deux critères établis par Bruno Buchberger pour éviter les réductions inutiles de S -polynômes lors des calculs de bases de Gröbner [Buc79].

- Une paire critique $\{p, p'\}$ satisfait Buchberger-1 si les deux conditions suivantes sont satisfaites :
 1. p et p' sont deux polynômes différentiels linéaires, homogènes, à coefficients constants et ne dépendent que d'une même indéterminée différentielle u ;
 2. $\text{ppcd}(\theta u, \theta' u) = \theta \theta' u$ où θu et $\theta' u$ désignent les dérivées dominantes respectives de p et de p' .
- Un triplet $\langle p_1, p_2, p_3 \rangle$ satisfait Buchberger-2 s'il satisfait les trois conditions suivantes :
 1. les dérivées dominantes des trois polynômes sont deux-à-deux distinctes et admettent des dérivées communes ;
 2. $\text{ppcd}(\text{ld } p_1, \text{ld } p_3)$ est une dérivée de $\text{ld } p_2$;
 3. l'une des quatre conditions suivantes est vérifiée :
 - (a) la situation est triangulaire : $\text{ld } p_i$ n'est pas une dérivée de $\text{ld } p_j$ pour $1 \leq i \neq j \leq 3$,
 - (b) $\text{ld } p_1 < \text{ld } p_2 < \text{ld } p_3$ ou $\text{ld } p_3 < \text{ld } p_2 < \text{ld } p_1$,
 - (c) $\text{ld } p_2 < \text{ld } p_1 < \text{ld } p_3$ et $\text{deg}(p_1, \text{ld } p_1) = 1$,
 - (d) $\text{ld } p_1 < \text{ld } p_3 < \text{ld } p_2$ et $\text{deg}(p_3, \text{ld } p_3) = 1$.

1.4.4 Traitement algébrique des systèmes réguliers

Soit $A = 0$, $S \neq 0$ un système différentiel régulier pour un classement \mathcal{R} .

1.4.4.1 Une version simple

Le plus élémentaire des traitements algébriques consiste à calculer une base de Gröbner B de l'idéal $(A):S^\infty$. C'est ce qui est fait dans [Bou94, BLOP95]. Ce calcul ne fournit pas une présentation caractéristique de l'idéal. En pratique,

on calcule une base de Gröbner \overline{B} de l'idéal $S^{-1}(A)$ de l'anneau $S^{-1}R$ en appliquant l'algorithme de Buchberger à la famille

$$A \cup \{s\bar{s} - 1 \mid s \in S\}.$$

Chaque \bar{s} désigne une nouvelle indéterminée codant l'inverse de s dans $S^{-1}R$. Si le classement choisi est un ordre qui élimine les \bar{s} alors la base B de $(A) : S^\infty$ s'obtient en retirant de \overline{B} tous les polynômes dans l'écriture desquels au moins un \bar{s} apparaît.

fonction traitement_algébrique ($A = 0, S \neq 0$)

début

 Calculer une base de Gröbner \overline{B} de l'idéal $S^{-1}(A)$

 si $1 \notin \overline{B}$ alors

 retourner $\{A = 0, S \neq 0\}$

 sinon

 retourner l'ensemble vide

 fin si

fin

À noter : le calcul de la base peut se faire en dimension zéro, c'est-à-dire en faisant passer dans le corps des coefficients toutes les dérivées figurant dans $A \cup S$ qui ne sont les dérivées dominantes d'aucun élément de A . Cette possibilité, qui accélère considérablement les calculs et rend la base plus petite, est due au lemme de Lazard.

1.4.4.2 Une version plus évoluée

Elle transforme le système $A = 0, S \neq 0$ en une famille de présentations caractéristiques C_1, \dots, C_t telles que

$$[A] : S^\infty = [C_1] : H_{C_1}^\infty \cap \dots \cap [C_t] : H_{C_t}^\infty.$$

Elle retourne alors l'ensemble $\{C_1 = 0, H_{C_1} \neq 0, \dots, C_t = 0, H_{C_t} \neq 0\}$. Cet ensemble est vide si le système est inconsistant.

Ces présentations caractéristiques peuvent être calculées à coup de bases de Gröbner. C'est ce qui est fait dans le paquetage `diffalg`. Une solution plus efficace consiste à appliquer une variante très proche de `Lextriangular` [Laz92, Mor97, Aub99], nommée `regCharacteristic` [BL00]. L'algorithme s'appuie sur des calculs d'inverses de nombres algébriques dont nous rappelons le principe en section 1.6. L'étude théorique menée dans [Hub00] permet de justifier facilement l'application aux systèmes différentiels réguliers.

Notons $L = v_1 < \dots < v_t$ l'ensemble des dérivées dominantes des éléments de A . On fait passer dans le corps des coefficients K toutes les dérivées figurant dans $A \cup S$ qui n'appartiennent pas à L . Appelons G le corps de fractions

rationnelles ainsi obtenu. Vus comme des systèmes de $G[L]$, le système A est un système triangulaire de dimension zéro (il comporte autant d'équations qu'il y a d'inconnues) et les présentations caractéristiques C_i que l'on cherche sont des systèmes triangulaires de dimension zéro normalisés (c'est-à-dire constitués de polynômes dont l'initial vaut 1). On construit les C_i incrémentalement du bas vers le haut. Il suffit de prendre les numérateurs des polynômes qui les composent pour obtenir à la fin des présentations caractéristiques au sens de la définition 6.

Les équations

Soit $C = p_1 < \dots < p_i$ un système normalisé de $G[v_1, \dots, v_i]$ et $p \in G[v_1, \dots, v_{i+1}]$ un nouveau polynôme, extrait de A avec lequel on souhaite étendre C . Trois situations peuvent se présenter.

1. L'initial $i_p \in G$. Il suffit d'ajouter p/i_p à C .
2. L'initial $i_p \in (C)$. On abandonne le calcul de présentations caractéristiques à partir de C qui ne conduit qu'à des branches sans solutions.
3. L'initial $i_p \notin (C)$ et admet une certaine dérivée v_k pour dérivée dominante ($1 \leq k < i$). On tente alors de calculer une identité de Bézout entre i_p et p_k modulo l'idéal (p_1, \dots, p_{k-1}) c'est-à-dire trois polynômes g_1, g_2, g_3 de $G[v_1, \dots, v_k]$ tels que

$$g_1 i_p + g_2 p_k = g_3 \pmod{(p_1, \dots, p_{k-1})}.$$

Ici aussi, trois situations peuvent se présenter.

- (a) Le calcul réussit et $g_3 \in G$. Alors l'inverse de i_p est g_1 modulo (C) et on étend C avec le polynôme $g_1 p \pmod{(C)}$.
- (b) Le calcul réussit et $g_3 \notin G$. Alors l'inverse n'existe pas mais on a exhibé une factorisation $p_k = g_3 \bar{g}_3 \pmod{(p_1, \dots, p_{k-1})}$ du polynôme $p_k \in C$. Cette factorisation permet de scinder l'idéal (C) en une intersection de deux idéaux, que l'on obtient en remplaçant p_k par l'un ou l'autre de ses facteurs. Il ne reste plus alors qu'à reprendre le calcul de la présentation caractéristique en parallèle à partir de chacun des deux systèmes.
- (c) Le calcul ne réussit pas. Cette situation est en fait identique à la précédente: un calcul d'inverse modulaire a échoué en révélant une factorisation de l'idéal (C) . Elle se traite pareillement.

Les inéquations

Soit C un système normalisé de $G[v_1, \dots, v_i]$ et $s \in G[v_1, \dots, v_i]$ une inéquation prise dans S . Il s'agit de tester que s ne divise pas zéro modulo (C) et, en cas de scindage, d'abandonner la branche dans laquelle $s = 0$. Trois situations peuvent se présenter.

1. L'inéquation $s \in G$. On a fini de vérifier que s est un non diviseur de zéro modulo (C) .
2. L'inéquation $s \in (C)$. On abandonne le calcul de présentations caractéristiques à partir de C .
3. L'inéquation $s \notin (C)$ et admet une certaine dérivée v_k pour dérivée dominante ($1 \leq k < i$). On tente alors de calculer une identité de Bézout entre s et p_k modulo l'idéal (p_1, \dots, p_{k-1}) c'est-à-dire trois polynômes g_1, g_2, g_3 de $G[v_1, \dots, v_k]$ tels que

$$g_1 s + g_2 p_k = g_3 \pmod{(p_1, \dots, p_{k-1})}.$$

Ici aussi, trois situations peuvent se présenter.

- (a) Le calcul réussit et $g_3 \in G$. On a alors fini de vérifier que s est non diviseur de zéro modulo (C) .
- (b) Le calcul réussit et $g_3 \notin G$. On a ainsi exhibé une factorisation $p_k = g_3 \bar{g}_3 \pmod{(p_1, \dots, p_{k-1})}$ du polynôme $p_k \in C$. On remplace p_k par \bar{g}_3 dans (C) et, soit on sait que l'idéal (C) est radiciel (en vertu du lemme de Lazard, si les séparants de toutes les équations de C ont déjà été inversés) et on a fini la vérification, soit on recommence le test d'inversibilité de s modulo l'idéal engendré par le système C simplifié.
- (c) Le calcul ne réussit pas. On a exhibé une factorisation $p_j = g_3 \bar{g}_3 \pmod{(p_1, \dots, p_{j-1})}$ d'un polynôme $p_j \in C$ pour un certain $j < k$. Cette factorisation permet de scinder l'idéal (C) en une intersection de deux idéaux, que l'on obtient en remplaçant p_j par l'un ou l'autre de ses facteurs. On reprend le test d'inversibilité de s sur chacune des deux branches.

1.5 Calculer dans un produit de corps différentiels

Si \mathfrak{p} est un idéal différentiel premier d'un anneau de polynômes différentiels $R = K\{U\}$ alors le corps des fractions de R/\mathfrak{p} est un corps différentiel. Si \mathfrak{i} est un idéal différentiel régulier de R alors l'anneau total des fractions⁷ de R/\mathfrak{i} est

7. L'anneau total des fractions d'un anneau A s'obtient en rendant inversible tous les non diviseurs de zéros de A .

un produit de corps différentiels (il s'agit du produit des corps de fractions des R/\mathfrak{p}_i où les \mathfrak{p}_i sont les composantes premières minimales de \mathfrak{i}).

Principe

L'idéal différentiel régulier \mathfrak{i} est supposé décrit par sa présentation caractéristique C et on a $\mathfrak{i} = [C] : H_C^\infty$. On dispose (cf. paragraphe suivant) d'un algorithme qui calcule l'inverse d'un élément de R/\mathfrak{i} . Ce calcul échoue parfois. Dans ce cas, une factorisation non triviale d'un élément $p \in C$ est exhibée (mettons $p = p_1 p_2 \pmod{\mathfrak{i} \cap R'}$ où $R' \subset R$ désigne l'anneau des polynômes différentiels de dérivée dominante strictement inférieure à celle de p). Les deux facteurs ont même dérivée dominante que p . Cette factorisation fournit une décomposition (un scindage) de \mathfrak{i} en une intersection de deux idéaux différentiels réguliers. Les présentations caractéristiques de ces deux idéaux s'obtiennent à partir de C en remplaçant p par l'un ou l'autre de ses facteurs. Dans les deux cas, certains éléments de C de dérivée dominante supérieure à celle de p peuvent n'être plus algébriquement réduits par rapport au nouvel élément. Reste alors à les réduire et à les rendre à nouveau primitifs.

Calcul de l'inverse

Rappelons qu'un polynôme différentiel $a \in R$ est non diviseur de zéro dans R/\mathfrak{i} si et seulement si a est inversible dans l'anneau total des fractions de R/\mathfrak{i} .

Un polynôme différentiel $a \in R$ est diviseur de zéro dans $R/[C] : H_C^\infty$ si et seulement si $r = \text{reste_partiel}(a, C)$ est diviseur de zéro dans $R/(C) : H_C^\infty$. C'est une conséquence du lemme de Rosenfeld. Cette dernière propriété peut être testée en calculant un inverse algébrique de r dans l'anneau total des fractions de $R/(C) : H_C^\infty$ (obtenu en faisant passer dans le corps K toutes les dérivées sous les escaliers de C) par l'algorithme donné en section 1.6.

1.5.1 Formes normales modulo un idéal différentiel régulier

Notons $N \subset \Theta U$ l'ensemble des dérivées sous les escaliers de C . Ce qui suit est extrait de [BL00].

Théorème 4 (et définition)

Quel que soit $a \in R$ il existe une unique fraction rationnelle p/q , appelée forme normale de a et notée $\text{NF}(a, C)$ satisfaisant

1. $a = p/q \pmod{\mathfrak{i}}$ (dans le sens où $qa = p \pmod{\mathfrak{i}}$ et q est non diviseur de zéro dans R/\mathfrak{i});
2. p est réduit par rapport à C ;
3. $q \in K[N]$.

C'est le fait que $q \in K[N]$ qui assure que q est non diviseur de zéro dans R/i . L'ensemble des formes normales de R modulo i forme un espace vectoriel sur K (i.e. toute combinaison linéaire de formes normales est une forme normale). Cette propriété, qui permet de détecter facilement les dépendances linéaires sur K entre éléments de R/i , a fourni un analogue de [FGLM93] mis en œuvre dans [Bou99].

Calcul de la forme normale

Soient $a \in R$ un polynôme différentiel et $r = \text{reste_complet}(a, C)$. On a la relation

$$i_1^{\alpha_1} \dots i_t^{\alpha_t} s_1^{\beta_1} \dots s_t^{\beta_t} a = r \pmod{i} \quad (1.2)$$

où les i_ℓ et les s_ℓ désignent respectivement les initiaux et les séparants des éléments de C et où les α_ℓ, β_ℓ sont des entiers naturels. L'algorithme de calcul d'inverse permet, pour chaque s_ℓ , de calculer un couple $(\bar{s}_\ell, \bar{r}_\ell)$ tel que $\bar{r}_\ell \in K[N]$ et

$$\bar{s}_\ell s_\ell = \bar{r}_\ell \pmod{i}.$$

En pratique, les inverses des séparants auront déjà été calculés lors du traitement algébrique des systèmes réguliers (cf. section 1.4.4). En multipliant l'égalité (1.2) par les puissances appropriées des \bar{s}_ℓ on obtient

$$i_1^{\alpha_1} \dots i_t^{\alpha_t} \bar{r}_1^{\beta_1} \dots \bar{r}_t^{\beta_t} a = \bar{s}_1^{\beta_1} \dots \bar{s}_t^{\beta_t} r \pmod{i}. \quad (1.3)$$

Le membre gauche de l'égalité (1.3) appartient à $K[N]$ mais le membre droit n'est pas nécessairement réduit par rapport à C . En effectuant une réduction purement algébrique, on obtient

$$i_1^{\gamma_1} \dots i_t^{\gamma_t} \bar{s}_1^{\beta_1} \dots \bar{s}_t^{\beta_t} r = r' \pmod{i}.$$

La forme normale $\text{NF}(a, C)$ s'obtient en rendant irréductible la fraction rationnelle

$$\frac{r'}{i_1^{\alpha_1 + \gamma_1} \dots i_t^{\alpha_t + \gamma_t} \bar{r}_1^{\beta_1} \dots \bar{r}_t^{\beta_t}}.$$

Exemple \triangleright Considérons le polynôme différentiel $u_x^2 - 4u$, qui forme une présentation caractéristique C de l'idéal différentiel premier $i = [u_x^2 - 4u] : (u_x)^\infty$. Calculons la forme normale de u_{xy} . En réduisant partiellement u_{xy} par $u_x^2 - 4u$, on trouve la relation $2u_x u_{xy} = 4u_y \pmod{i}$. Un calcul d'inverse algébrique fournit $1/u_x = u_x/4u \pmod{i}$, ce qui nous donne

$$\text{NF}(u_{xy}, C) = \frac{u_x u_y}{2u}.$$

\triangleleft

1.6 Inverse d'un nombre algébrique

L'algorithme que nous présentons dans cette section n'est autre qu'une généralisation très naturelle de l'algorithme d'Euclide étendu. Il s'agit d'un algorithme purement algébrique dont l'idée remonte à [Laz91], qui est mis en œuvre dans [MR95] et dont nous ne rappelons que le principe. On évite dans les implantations de manipuler des fractions rationnelles et de calculer les identités de Bézout (le pgcd suffit). Ce sont des variantes de l'algorithme de Lionel Ducos [Duc00] qui sont utilisées. Des versions basées sur [LRS00] devraient donner d'excellents résultats également.

Dans l'anneau de polynômes $R = K[x_1, \dots, x_n]$ (les indéterminées sont ordonnées $x_1 < \dots < x_n$), on considère un système triangulaire $T = \{p_1, \dots, p_n\}$ de dimension zéro (il y a autant d'équations que d'inconnues) et normalisé (l'initial de chaque p_i vaut 1).

Le système T constitue une base de Gröbner de l'idéal $i = (T)$ pour l'ordre lexicographique induit par l'ordre sur l'alphabet et peut donc servir à calculer la forme normale $NF(p, T)$ d'un polynôme quelconque $p \in R$. Cette forme normale est un polynôme équivalent à p dans R/i .

Si a et b sont deux polynômes de $R[y]$ et si l'initial de b vaut 1, on peut calculer le quotient q et le reste r de la division euclidienne de a par b , vus comme des polynômes en la nouvelle indéterminée y . Appliquons l'algorithme de forme normale sur chacun des coefficients de q et de r , on obtient une forme normale du quotient et du reste de la division euclidienne de a par b dans $(R/i)[y]$.

La fonction inverse retourne l'inverse de a dans R/i ou échoue. Dans le deuxième cas, elle lève une exception et exhibe une factorisation d'un élément de T . On suppose a non nul dans R/i .

fonction inverse ($a, \{p_1, \dots, p_n\}$)

début

 si $a \in K$ alors

 retourner a^{-1}

 sinon

 soit i tel que $\text{ld } a = \text{ld } p_i$

$(u_1, u_2, u_3) := \text{Bézout}(p_i, a, \{p_1, \dots, p_{i-1}\})$

 si $g = 1$ alors

 retourner u_2

 sinon

 le calcul d'inverse échoue;

 le polynôme u_3 est un facteur non trivial de p_i modulo (p_1, \dots, p_{i-1})

 fin si

 fin si

fin

La fonction Bézout retourne une identité de Bézout

$$u_1 a + u_2 b = u_3 \pmod{(p_1, \dots, p_n)}.$$

Les polynômes a et b appartiennent à $R[y]$ et sont vus comme des polynômes en y . On suppose que l'initial de a vaut 1. L'initial du polynôme u_3 résultat (éventuellement u_3 lui-même) vaut 1. Le calcul échoue si un appel à `inverse` échoue. Invariants de boucle :

1. $u_1 a + u_2 b = u_3 \pmod{(p_1, \dots, p_n)}$, $v_1 a + v_2 b = v_3 \pmod{(p_1, \dots, p_n)}$;
2. l'ensemble des diviseurs communs modulo (p_1, \dots, p_n) de a et de b est égal à l'ensemble des diviseurs communs modulo (p_1, \dots, p_n) de u_3 et de v_3 .

fonction Bézout ($a, b, \{p_1, \dots, p_n\}$)

début

$$(u_1, u_2, u_3) := (1, 0, a)$$

$$(v_1, v_2, v_3) := (0, 1, b)$$

tant que $v_3 \neq 0$ faire

$$\bar{c} := \text{inverse}(\text{coefficient_principal}(v_3, y), \{p_1, \dots, p_n\})$$

$$(v_1, v_2, v_3) := \bar{c} \cdot (v_1, v_2, v_3) \text{ (prendre les formes normales des coefficients)}$$

$$q := \text{le quotient de la division euclidienne de } u_3 \text{ par } v_3 \text{ dans } (R/i)[y]$$

$$(t_1, t_2, t_3) := (v_1, v_2, v_3)$$

$$(v_1, v_2, v_3) := (u_1, u_2, u_3) - q \cdot (v_1, v_2, v_3)$$

$$(u_1, u_2, u_3) := (t_1, t_2, t_3)$$

fait

$$\text{retourner}(u_1, u_2, u_3)$$

fin

1.7 Exemples

1.7.1 Exemple d'élimination

Reprenons l'exemple introductif.

$$\Sigma \begin{cases} p_1 = u_x^2 - 4u, \\ p_2 = u_{xy}v_y - u + 1, \\ p_3 = v_{xx} - u_x. \end{cases}$$

Appliquons Rosenfeld–Gröbner pour un classement éliminant u et ses dérivées.

$$\dots > u_x > u_y > u > \dots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v.$$

On obtient une présentation caractéristique C où

$$C \begin{cases} q_1 = u - v_{yy}^2, \\ q_2 = v_{xx} - 2v_{yy}, \\ q_3 = v_y v_{xy} - v_{yy}^3 + v_{yy}, \\ q_4 = v_{yy}^4 - 2v_{yy}^2 - 2v_y^2 + 1. \end{cases}$$

Notons $\overline{C} = \{q_2, q_3, q_4\}$. On a

$$\sqrt{[\Sigma]} \cap K\{v\} = [\overline{C}] : H_{\overline{C}}^{\infty}.$$

Le raisonnement est le suivant. Soit $p \in \sqrt{[\Sigma]} \cap K\{v\}$ un polynôme différentiel.

1. Ce polynôme est réduit à zéro par C .
2. Comme $p \in K\{v\}$, seuls les éléments de C dont la dérivée dominante est une dérivée de v (i.e. ceux de \overline{C}) permettent de le réduire.
3. Comme le classement élimine u , les éléments de \overline{C} appartiennent à $K\{v\}$.
4. La réduction de p par les éléments de \overline{C} ne fait donc apparaître aucune dérivée de u dans les restes successifs. Par conséquent p est réduit à zéro par les seuls éléments de \overline{C} et $p \in [\overline{C}] : H_{\overline{C}}^{\infty}$.

Éliminer peut aussi aider à résoudre un système. Les fonctions `pdsolve` et `pdesolve` de MAPLE V version 5 ne permettent pas de résoudre Σ directement. On s'aperçoit après le calcul de \overline{A} que l'idéal $\sqrt{[\Sigma]}$ comporte une équation différentielle ordinaire où ne figurent que les dérivées d'une seule indéterminée différentielle

$$v_{yy}^4 - 2v_{yy}^2 - 2v_y^2 + 1 = 0.$$

Cette équation, qui se résout aisément avec `dsolve`, aide à résoudre le système complet.

1.7.2 Symétries de Lie avec discussion automatique

Cet exemple consiste à résoudre un système d'équations aux dérivées partielles linéaires, dépendant d'une fonction arbitraire. En scindant l'idéal, l'algorithme Rosenfeld–Gröbner discute les solutions en fonction du paramètre. L'exemple, ainsi qu'une partie de son analyse sont extraits de [Rei91]. Voir aussi [Pet99]. Il s'agit de symétries de Lie d'équations différentielles. L'équation différentielle ci-dessous est une variante de l'équation des ondes. Le symbole H désigne une fonction arbitraire de $u(x, y)$.

$$E_H : \quad \frac{\partial^2}{\partial x^2} u(x, y) = \frac{\partial^2}{\partial y^2} u(x, y) + H(u(x, y)) \frac{\partial}{\partial y} u(x, y)$$

On s'intéresse aux symétries de Lie de l'équation (E_H) . En fait, le graphe d'une solution de l'équation (E_H) est un ensemble de points $(x, y, u) \in \mathbb{R}^3$; une symétrie de Lie de cette équation est une transformation (un difféomorphisme local) qui envoie le graphe de n'importe quelle solution sur le graphe d'une autre solution:

$$\begin{cases} X &= \varphi_1(x, y, u), \\ Y &= \varphi_2(x, y, u), \\ U &= \varphi_3(x, y, u). \end{cases}$$

On cherche les champs de vecteurs

$$V = V^1(x, y, u) \frac{\partial}{\partial x} + V^2(x, y, u) \frac{\partial}{\partial y} + V^3(x, y, u) \frac{\partial}{\partial u}$$

dont les flots sont les symétries désirées. L'ensemble de ces champs de vecteurs forme une algèbre de Lie, c'est-à-dire un espace vectoriel muni d'un crochet de Lie. En posant que la dérivée de Lie de E_H est nulle modulo E_H on obtient un système Σ_H d'équations aux dérivées partielles linéaires (appelées équations de Lie) en les trois indéterminées différentielles V^1 , V^2 et V^3 . Les dérivations sont $\partial/\partial x$, $\partial/\partial y$ et $\partial/\partial u$.

$$\begin{aligned} \Sigma_H = [& V_{xx}^1 - H V_y^1 - 2 V_{xu}^3 - V_{yy}^1, V_{xx}^2 - V_{yy}^2 + H V_y^2 + V^3 H_u + 2 V_{yu}^3, \\ & V_{xx}^3 - H V_y^3 - V_{yy}^3, V_{uu}^1, V_{uu}^2, -2 V_{xu}^1 + V_{uu}^3, V_u^2, V_u^1, V_x^1 - V_y^2, \\ & V_{yu}^2 - V_{xu}^1, V_x^2 - V_y^1, V_{xu}^2 - V_{yu}^1] \end{aligned}$$

Des dérivées du paramètre H figurent dans les coefficients des équations différentielles linéaires. On enrichit le système avec les deux équations suivantes afin d'exprimer l'hypothèse que H ne dépend que de u .

$$H_x = 0, H_y = 0.$$

Nous souhaitons discuter en fonction de H la structure de l'algèbre de Lie et en particulier sa dimension, en tant qu'espace vectoriel. Pour cette raison, nous choisissons de considérer Σ_H comme un système d'équations aux dérivées partielles polynomiales en les quatre indéterminées différentielles V^1 , V^2 , V^3 et H . Nous lui appliquons l'algorithme Rosenfeld-Gröbner pour un classement qui élimine les V . En scindant les cas, l'algorithme discute en fonction de H la structure de l'algèbre de Lie. Remarquer que d'après le lemme de Lazard, l'algorithme est *obligé* de scinder les cas correspondant à des dimensions différentes. Quatre systèmes différentiels réguliers sont produits.

Les calculs détaillés ci-dessous sont effectués grâce au paquetage `difalg`. Les sorties sont mises en page. Les développements de Taylor sont calculés au voisinage de $x = 0$, $y = 0$, $u = 0$. les symboles commençant par la lettre C désignent les constantes apparaissant dans ces développements (par exemple, $CH = H(0, 0, 0)$, $CH_u = H_u(0, 0, 0)$, ...).

1.7.2.1 Premier système

Voici une présentation caractéristique du premier système.

$$V_x^1 = 0, V_y^1 = 0, V_u^1 = 0, V_x^2 = 0, V_y^2 = 0, V_u^2 = 0, V^3 = 0, H_x = 0, H_y = 0.$$

On n'y voit aucune équation différentielle en H et ses dérivées à l'exception de celles que nous avons introduites ci-dessus. Il s'agit donc du cas général. Les

solutions des V sont

$$\begin{aligned}V^1(x, y, u) &= CV^1, \\V^2(x, y, u) &= CV^2, \\V^3(x, y, u) &= 0.\end{aligned}$$

Les transformations autorisées sont des translations dans le plan (x, y) (λ, μ désignent des constantes) :

$$X = x + \lambda, \quad Y = y + \mu, \quad U = u.$$

1.7.2.2 Deuxième système

En voici une présentation caractéristique.

$$\begin{aligned}V_x^1 &= -\frac{V^3 H_u}{H}, V_y^1 = 0, V_u^1 = 0, V_x^2 = 0, V_y^2 = -\frac{V^3 H_u}{H}, V_u^2 = 0, V_x^3 = 0, \\V_y^3 &= 0, V_u^3 = -\frac{-V^3 H_u^2 + H_{uu} H V^3}{H_u H}, H_{uuu} = -\frac{-2 H H_{uu}^2 + H_u^2 H_{uu}}{H_u H}, \\H_x &= 0, H_y = 0.\end{aligned}$$

Ce cas correspond à n'importe quelle fonction H satisfaisant l'équation différentielle d'ordre 3 ci-dessus. Le calcul des développements de Taylor des solutions donne

$$\begin{aligned}V^1(x, y, u) &= CV^1 - \frac{x CV^3 CH_u}{CH}, \\V^2(x, y, u) &= CV^2 - \frac{y CV^3 CH_u}{CH}, \\V^3(x, y, u) &= CV^3 - \frac{u (-CV^3 CH_u^2 + CH_{uu} CH CV^3)}{CH_u CH}\end{aligned}$$

L'algèbre de Lie est de dimension 3 c'est-à-dire que les solutions du système dépendent de trois constantes arbitraires CV^1 , CV^2 et CV^3 (les constantes qui apparaissent dans le développement de Taylor de H sont supposées connues).

$$V = CV^1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + CV^2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + CV^3 \begin{pmatrix} -\frac{x CH_u}{CH} \\ -\frac{y CH_u}{CH} \\ CH_u CH + u (CH_u^2 - CH_{uu} CH) \end{pmatrix}$$

On peut remarquer qu'on retrouve (en posant $CV^3 = 0$) les symétries de Lie de la section 1.7.2.1 mais d'autres symétries existent dans ce cas-ci. Une classe

de fonctions H qui satisfont l'équation différentielle d'ordre 3 est donnée par

$$H(u) = \alpha u + \beta$$

où α, β sont des constantes (en fait $\alpha = CH_u$ et $\beta = CH$ puisque les solutions ont été développées au voisinage de l'origine). En posant $CH_u = CH = 1$ nous trouvons le groupe de symétries

$$V = CV^1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + CV^2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + CV^3 \begin{pmatrix} -x \\ -y \\ u+1 \end{pmatrix}$$

Les flots engendrés par les deux premiers champs de vecteurs sont des translations dans le plan (x, y) . Le troisième champ de vecteurs engendre le groupe de dilatations (où λ désigne une constante)

$$X = \frac{x}{\lambda}, \quad Y = \frac{y}{\lambda}, \quad U + 1 = \lambda(u + 1).$$

1.7.2.3 Troisième système

Il correspond au cas $H(u) = \text{constant}$.

$$V_{xx}^2 = 0, \quad V_{xx}^3 = H V_y^3 + V_{yy}^3, \quad V_{xu}^3 = -\frac{1}{2} V_x^2 H, \quad V_{yu}^3 = 0, \quad V_{uu}^3 = 0, \quad V_x^1 = 0,$$

$$V_y^1 = V_x^2, \quad V_u^1 = 0, \quad V_y^2 = 0, \quad V_u^2 = 0, \quad H_x = 0, \quad H_y = 0, \quad H_u = 0.$$

Les solutions des V sont

$$V^1(x, y, u) = CV^1 + y CV_x^2,$$

$$V^2(x, y, u) = CV^2 + x CV_x^2,$$

$$V^3(x, y, u) = CV^3 + x CV_x^3 + y CV_y^3 + u CV_u^3 + \frac{1}{2} x^2 (CH CV_y^3 + CV_{yy}^3) \\ + xy CV_{xy}^3 - \frac{1}{2} xu CV_x^2 CH + \frac{1}{2} y^2 CV_{yy}^3 + \dots$$

Les champs de vecteurs associés à CV^1 et à CV^2 engendrent les translations que nous avons déjà rencontrées dans le cas général. Le champ de vecteur associé à CV_x^2 engendre une rotation hyperbolique

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad U = u e^{-\frac{1}{2}(Y-y)}$$

où $a^2 - b^2 = 1$. Le champ de vecteurs associé à CV_u^3 engendre le groupe de dilatations $U = \lambda u$. Les autres symétries dépendent d'une solution arbitraire $\alpha(x, y)$ de l'équation E_H puisqu'elle est linéaire dans ce cas-ci.

$$V = \alpha(x, y) \frac{\partial}{\partial u}.$$

1.7.2.4 *Quatrième système*

Il correspond à l'équation des ondes ($H(u) = 0$). Il y a encore davantage de symétries que dans le troisième cas. Voir [Olv93, page 124] pour leur description.

$$\begin{aligned}V_{xx}^2 = V_{yy}^2, V_{xx}^3 = V_{yy}^3, V_{xu}^3 = 0, V_{yu}^3 = 0, V_{uu}^3 = 0, V_x^1 = V_y^2, V_y^1 = V_x^2, \\V_u^1 = 0, V_u^2 = 0, H = 0.\end{aligned}$$

Bibliographie

- [Aub99] Philippe Aubry, *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.*, Ph.D. thesis, Université Paris VI, 1999.
- [BKM96] D. Bouziane, Abdelillah Kandri Rody, and Hamid Maârouf, *Unmixed-Dimensional Decomposition of a Finitely Generated Perfect Differential Ideal*, Journal of Symbolic Computation (1996), (submitted).
- [BL00] François Boulier and François Lemaire, *Computing canonical representatives of regular differential ideals*, proceedings of ISSAC 2000 (St Andrews, Scotland), 2000, pp. 37–46.
- [BLOP95] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot, *Representation for the radical of a finitely generated differential ideal*, proceedings of ISSAC'95 (Montréal, Canada), 1995, pp. 158–166.
- [BLOP97] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot, *Computing representations for radicals of finitely generated differential ideals*, Tech. report, Université Lille I, LIFL, 59655, Villeneuve d'Ascq, France, 1997, (ref. IT306, december 1998 version published in the habilitation thesis of Michel Petitot).
- [Bou94] François Boulier, *Étude et implantation de quelques algorithmes en algèbre différentielle*, Ph.D. thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, 1994.
- [Bou99] François Boulier, *Efficient computation of regular differential systems by change of rankings using Kähler differentials*, Tech. report, Université Lille I, 59655, Villeneuve d'Ascq, France, November 1999, (ref. LIFL 1999–14, presented at the MEGA2000 conference).
- [Buc65] Bruno Buchberger, *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German)*, Ph.D. thesis, Math. Inst. Univ. of Innsbruck, Austria, 1965.

- [Buc79] Bruno Buchberger, *A criterion for detecting unnecessary reductions in the construction of Gröbner bases*, Lecture Notes in Computer Science, vol. 72, pp. 3–21, Springer Verlag, 1979.
- [BW91] Thomas Becker and Volker Weispfenning, *Gröbner Bases: a computational approach to commutative algebra*, Graduate Texts in Mathematics, vol. 141, Springer Verlag, 1991.
- [CF87] Giuseppa Carra-Ferro, *Gröbner bases and differential ideals*, Notes of AAEECC 5 (Menorca, Spain), Springer Verlag, 1987, pp. 129–140.
- [Dio89] Sette Diop, *Théorie de l'élimination et principe du modèle interne en automatique*, Ph.D. thesis, Université Paris–Sud, (Orsay), 1989.
- [Duc00] Lionel Ducos, *Optimizations of the subresultant algorithm*, Journal of Pure and Applied Algebra **145** (2000), 149–163.
- [FGLM93] Jean-Charles Faugère, Patricia Gianni, Daniel Lazard, and Teo Mora, *Efficient computation of Gröbner bases by change of orderings*, Journal of Symbolic Computation **16** (1993), 329–344.
- [Fli89] Michel Fliess, *Automatique et corps différentiels*, Forum Math. **1** (1989), 227–238.
- [GM88] R. Gebauer and H. M. Möller, *On an Installation of Buchberger's Algorithm*, Journal of Symbolic Computation **6** (1988), no. 2&3, 275–286.
- [GMO91] Giovanni Gallo, Bubaneshwar Mishra, and François Ollivier, *Some constructions in rings of differential polynomials*, Lecture Notes in Computer Science, vol. 539, pp. 171–182, , Montréal, Canada, 1991.
- [Hub97] Évelyne Hubert, *Étude Algébrique et Algorithmique des Singularités des Équations Différentielles Implicites*, Ph.D. thesis, Institut National Polytechnique de Grenoble, France, 1997.
- [Hub00] Évelyne Hubert, *Factorization free decomposition algorithms in differential algebra*, Journal of Symbolic Computation **29** (2000), no. 4,5, 641–662.
- [Jan20] Maurice Janet, *Systèmes d'équations aux dérivées partielles*, Journal de Mathématiques, 8^e série, vol. 3, Gauthier–Villars, Paris, 1920.
- [Jan29] Maurice Janet, *Leçons sur les systèmes d'équations aux dérivées partielles*, Cahiers Scientifiques, vol. IV, Gauthier–Villars, Paris, 1929.

- [Kal93] Mickael Kalkbrener, *A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties*, Journal of Symbolic Computation **15** (1993), 143–167.
- [Knu66] Donald Erwin Knuth, *The art of computer programming*, Addison-Wesley, 1966, Second edition.
- [Kol73] Ellis R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.
- [Laz91] Daniel Lazard, *A new method for solving algebraic systems of positive dimension*, Discrete Applied Mathematics **33** (1991), 147–160.
- [Laz92] Daniel Lazard, *Solving Zero-dimensional Algebraic Systems*, Journal of Symbolic Computation **13** (1992), 117–131.
- [LRS00] Henri Lombardi, Marie-Françoise Roy, and Mohab Safey El Din, *New structure theorem for subresultants*, Journal of Symbolic Computation **29** (2000), no. 4,5, 663–690.
- [LW99] Ziming Li and Dongming Wang, *Coherent, regular and simple systems in zero decompositions of partial differential systems*, Systems Science and Mathematical Sciences **12** (1999), 43–60.
- [Maã96] Hamid Maârouf, *Étude de Quelques Problèmes Effectifs en Algèbre Différentielle*, Ph.D. thesis, Université Cadi Ayyad, Morocco, 1996.
- [Man91] Elizabeth L. Mansfield, *Differential Gröbner Bases*, Ph.D. thesis, University of Sydney, Australia, 1991.
- [Mor95] Sally Morrison, *Yet another proof of Lazard’s lemma*, private communication, december 1995.
- [Mor97] Marc Moreno Maza, *Calculs de Pgcd au-dessus des Tours d’Extensions Simples et Résolution des Systèmes d’Équations Algébriques*, Ph.D. thesis, Université Paris VI, France, 1997.
- [Mor99] Sally Morrison, *The Differential Ideal $[P] : M^\infty$* , Journal of Symbolic Computation **28** (1999), 631–656.
- [MR95] Marc Moreno Maza and Renaud Rioboo, *Polynomial gcd computations over towers of algebraic extensions*, Proceedings of AAEECC11, Springer Verlag, 1995, pp. 365–382.
- [Oll90] François Ollivier, *Le problème de l’identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité*, Ph.D. thesis, Ecole Polytechnique, Palaiseau, France, 1990.

- [Olv93] Peter J. Olver, *Applications of Lie groups to differential equations*, second ed., Graduate Texts in Mathematics, vol. 107, Springer Verlag, 1993.
- [Pet99] Michel Petitot, *Quelques méthodes de Calcul Formel appliquées à l'étude des équations différentielles*, February 1999, Mémoire d'habilitation à diriger des recherches, Université Lille I, LIFL, 59655 Villeneuve d'Ascq, France.
- [Pom78] Jean-François Pommaret, *Systems of Partial Differential Equations and Lie pseudogroups*, Gordon and Breach science publishers Inc., 1978.
- [Rei91] Gregory J. Reid, *Algorithms for reducing a system of PDEs to standard form determining the dimension of its solution space and calculating its Taylor series solution*, Eur. J. of Applied Math. **2** (1991), 293–318.
- [Riq10] C. Riquier, *Les systèmes d'équations aux dérivées partielles*, Gauthier–Villars, Paris, 1910.
- [Rit32] Joseph Fels Ritt, *Differential equations from the algebraic standpoint*, American Mathematical Society Colloquium Publications, vol. 14, AMS, New York, 1932.
- [Rit50] Joseph Fels Ritt, *Differential Algebra*, Dover Publications Inc., New York, 1950.
- [RLW96] Gregory J. Reid, Ping Lin, and Allan D. Wittkopf, *Differential Elimination–Completion Algorithms for DAE and PDAE*, Tech. report, Dept. of Maths of the University of British Columbia, Vancouver, Canada, 1996.
- [Ros59] Azriel Rosenfeld, *Specializations in differential algebra*, Trans. Amer. Math. Soc. **90** (1959), 394–407.
- [RWB94] Gregory J. Reid, Allan D. Wittkopf, and Alan Boulton, *Reduction of systems of nonlinear partial differential equations to simplified involutive forms*, Eur. J. of Applied Math. (1994), (to appear).
- [Sad00] Brahim Sadik, *Une note sur les algorithmes de décomposition en algèbre différentielle*, Comptes Rendus de l'Académie des Sciences **330** (2000), 641–646.
- [Sei52] Abraham Seidenberg, *Some basic theorems in differential algebra (characteristic p arbitrary)*, Trans. Amer. Math. Soc. **73** (1952), 174–190.

- [Sei56] Abraham Seidenberg, *An elimination theory for differential algebra*, Univ. California Publ. Math. (New Series) **3** (1956), 31–65.
- [SL95] Josef Schicho and Ziming Li, *A construction of radical ideals in polynomial algebra*, Tech. report, RISC, Johannes Kepler University, Linz, Austria, august 1995.
- [Wan94] Dongming Wang, *An elimination method for differential polynomial systems I*, Tech. report, LIFIA–IMAG, Grenoble, France, 1994.
- [Wu 87] Wu Wen Tsün, *On the foundation of algebraic differential geometry*, Mechanization of Mathematics, research preprints **3** (1987).

Index

- $(A) : S^\infty$, 7
- A_v , 11
- H_A , 8
- R , 9
- R_v , 11
- $[A]$, 9
- Δ , 14
- Δ -polynôme, 14
- NF, 32
- ΘU , 9
- $\langle A, D, P, S \rangle$, 24
- ppcd, 9
- ord, 9
- paire_critiques, 14
- prem, 8
- reste_complet, 12
- reste_partiel, 12
- élimination, 5, 10

- anneau total des fractions, 31
- autoréduction, 26
- autoréduit, 11

- classement, 10
- cohérent, 17
- complétion, 26, 27
- critères de Buchberger, 28

- dérivée, 9
- dérivée dominante d'un polynôme, 10
- dérivées sous les escaliers, 19
- dérivation, 9
- développement de Taylor, 20
- dimension zéro, 29, 30, 34

- diviseur de zéro, 32

- ensemble caractéristique, 11

- forme normale, 32

- idéal différentiel, 9
- identité de Bézout, 34
- indéterminée différentielle, 9
- initial d'un polynôme, 8
- invariants, 24
- inverse algébrique, 34
- invertible, 32

- leader d'un polynôme, 8, 10
- lemme de Lazard, 17
- lemme de Rosenfeld, 17
- lextriangular, 29
- lifting du lemme de Lazard, 17

- normalisé, 30, 34
- normalisé, fortement, 18

- orderly, 10
- ordre d'un opérateur, 9

- paire critique, 13
- paire critique résolue, 14
- paire de réduction, 14
- partiellement réduit, 11
- présentation caractéristique, 18
- primitif, 18
- propre, 9

- quadruplet, 24

- réduction complète, 12

réduction partielle, 12
réduit, 11
régulier, 17
radical d'un idéal, 7
rang d'un polynôme, 8
ranking, 10
regCharacteristic, 29
Rosenfeld–Gröbner, 22

séparant, 10
séparant d'un polynôme, 8
saturation d'un idéal, 7

triangulaire, 8
triangulaire, différentiellement, 11