Géométrie et complexité
notes informelles I

M. Petitot

20 juillet 2007

Les techniques de réécriture algébriques (bases de Groebner, ensembles caractéristiques, etc.) fournissent des algorithmes puissants pour étudier l'existence et décrire les solutions des équations algébriques ou différentielles. Malheureusement, les formules générées au cours des calculs sont souvent de trés grande taille, ce qui rend le calcul impossible en pratique.

D'un autre point de vue, il semble que ces formules de grande taille soient souvent des invariants différentiels. Ces invariants différentiels forment un corps différentiel finiement engendré sous l'action de dérivations invariantes non commutatives. On montre que les covariants et les invariants de la théorie classique (action d'un sous-groupe du groupe linéaire sur des polynômes en variables commutatives) s'obtiennent par un processus analogue. En fait, c'est la connaissance des dérivations invariantes qui permet de retrouver les fonctions invariantes (et non l'inverse !) et de structurer le calcul d'une base d'invariants en un arbre. Les éléments de cette base de fonctions invariantes (noeuds de l'arbre) sont alors *numérotés* par des multi–indices formés d'entiers.

Il est donc possible d'envisager une compression des formules en recodant celles–ci en terme d'invariants correctement numérotés.

1 Le problème d'équivalence

1.1 Définition générale

On se donne une famille d'équations différentielles et un (pseudo)-groupe de Lie Φ de transformations qui laisse stable la famille d'équations.

Par définition d'un (pseudo)-groupe de Lie, les transformations $\varphi \in \Phi$ sont les solutions analytiques locales d'un sytème fini d'équations et d'inéquations aux dérivées partielles.

On veut pouvoir décider si deux équations de la famille sont équivalentes par une transformation $\varphi \in \Phi$ et si oui calculer φ.

Exemple 1 *Equivalence de* $E_f : y'' = f(x, y, y')$ *avec* $E_{\bar f} : \bar y'' = \bar f(\bar x, \bar y, \bar y')$ *par une transformation* $\varphi \in \Phi$ *de la forme*

$$\varphi(x, y) = (\bar x, \bar y) = (x + C, \eta(x, y)). \qquad (1)$$

On pose $M = \mathrm{J}^1(\mathbb{C}, \mathbb{C})$ munie des coordonnées $(x, y, p := y')$. Une équation E_f est vue comme une diffiété (Vinogradov) qui est, sur l'exemple, la donnée de la distribution (Chevalley) Δ_f définie sur M et orthogonale aux deux formes de contact $dy - p\, dx$ et $dp - f(x, y, p)\, dx$. Cette distribution qui est de dimension 1, vérifie la condition de complète intégrabilité de Frobénius.

1.2 Mise en équation du pb d'équivalence

La transformation φ cherchée est solution du syst. EDP :

$$\Delta_{\bar{f}} = \varphi_* \Delta_f \text{ et } \varphi \in \Phi. \tag{2}$$

Sur l'exemple 1, le calcul donne

$$\begin{gathered} \bar{x}_x = 1,\, \bar{x}_y = 0,\, \bar{x}_p = 0,\, \bar{y}_p = 0,\, \bar{y}_y \neq 0, \\ \bar{p} = \bar{y}_x + p\bar{y}_y, \\ \bar{f}(\bar{x},\, \bar{y},\, \bar{p}) = \bar{y}_{xx} + 2p\bar{y}_{xy} + p^2\bar{y}_{yy} + f(x,y,p)\ \bar{y}_y. \end{gathered} \tag{3}$$

Les deux premières lignes sont les équations et inéquations de définition du pseudo–groupe Φ. La dernière équation représente l'action du pseudo–groupe Φ sur les équations de la famille E_f. On peut s'affranchir de l'inéquation $\bar{y}_y \neq 0$ par une *localisation*, i.e. l'ajout d'une indéterminée supplémentaire w soumise à la contrainte $w\bar{y}_y = 1$.

Le système EDP (3) définit un idéal différentiel dans l'anneau des polynomes différentiels $\mathrm{k}\{\bar{x}, \bar{y}, \bar{p}, f, \bar{f}\}$ avec pour corps différentiel de coefficients $\mathrm{k} := \mathbb{Q}(x,y,p)$ muni des dérivations partielles par rapport à (x,y,p). Comme ce système EDP est quasi–linéaire, il définit un idéal premier.

Exemple 2 (Painlevé I)

$$\bar{y}'' = 6\bar{y}^2 + \bar{x} \ \ \textit{i.e.}\ \ \bar{f}(\bar{x},\, \bar{y},\, \bar{p}) := 6\bar{y}^2 + \bar{x}$$

1.3 Calcul des contraintes d'intégrabilité par la réécriture

On peut calculer un système de réécriture confluent (ensemble caractéristique) qui permet de tester l'égalité à 0 modulo le système (3), *seulement* si on remplace $\bar{f}(\bar{x},\, \bar{y},\, \bar{p})$ par sa valeur. C'est fondamentalement ce qui distingue l'approche par la réécriture de l'approche géométrique basée sur le test d'involution.

Après la substitution $\bar{f} := 6\bar{y}^2 + \bar{x}$, le syst. (3) a pour ensemble caractéristique $C = C_\varphi \cup C_f$, calculé pour le ranking d'élimination : $[\bar{x}, \bar{y}, \bar{p}] \succ [f] \succ (x,y,p)$ vaut

$$C_\varphi \left\{ \begin{array}{lcl} \bar{y} & \rightarrow & 1/12\, f_y - 1/24\, f_{xp} - 1/24\, f_{pp} f + 1/48\, {f_p}^2 - 1/24\, p f_{yp}, \\ \bar{x} & \rightarrow & 1/12 f_{xxy} + 1/12 p^2 f_{yyy} - 1/12 p f_{xyy} - 1/24 f_y^2 + 1/12 f f_{yy} \\ & & + \text{ 37 termes contenant une dérivée partielle de } f \text{ par rapport à } p \end{array} \right. \tag{4}$$

$$C_f \left\{ \begin{array}{lcl} f_{xxxxp} & \rightarrow & -24 + 5/2\, f p f_{pp} f_p f_{yp} - 4\, f_x f_{xyp} + 2\, f_{xxxy} - 2\, p f_{yp} f_p f_{xp} \\ & & + \cdots \\ f_{xxyp} & \rightarrow & -p f_{pp} f_{yy} + 3\, p f_{ypp} f_y + f_{pp} p^2 f_{yyp} - 3/2\, p f_p f_{yyp} \\ & & \cdots \\ f_{xyyp} & \rightarrow & 2\, f_{yyy} + {f_{yp}}^2 - p f_{yyyp} - f_{yypp} f - 2\, f_{ypp} f y + \cdots \\ f_{xpp} & \rightarrow & f_{yp} - p f_{ypp}, \\ f_{ppp} & \rightarrow & 0. \end{array} \right.$$

Les équations C_f donne des conditions génériques portant sur la fonction f et ses dérivées pour que le changement de variables φ existe. Si de plus, certaines inéquations portant sur f et ses dérivées sont vérifiées[1], alors φ existe et est donné par les formules C_φ.

[1] L'inéquation vient de la condition $\bar{y}_y \neq 0$ appliquée à la première equation de C_φ

1.4 Approche géométrique des contraintes d'intégrabilité

Contrairement à l'approche par la réécriture, l'approche géométrique permet de formuler les contraintes d'intégrabilité du système (2) sous forme d'un système infini d'équations de la forme $I[\bar{f}] = I[f]$ où $I[f]$ (respectivement $I[\bar{f}]$) est une fonction qui dépend rationnellement de f et de ses dérivées par rapport aux coordonnées (x, y, p). Les expressions I qui apparaissent dans ces équations forment un corps différentiel d'invariants rationnels finiement engendré.

Définition 1 (invariant différentiel) *L'objet géométrique I est un invariant différentiel du pb d'équivalence $\Delta_{\bar{f}} = \varphi_* \Delta_f$ et $\varphi \in \Phi$ ssi*

$$I[\bar{f}] = \varphi_* I[f], \quad \forall \varphi \textit{ solution du pb d'équivalence}$$

Dans les textes anciens, on utilise le notation allégée $I[\bar{f}] = I[f]$, la difficulté vient du fait que l'égalité est vraie modulo le changement de variables φ ; $I[f]$ est exprimé dans les anciennes coordonnées (x, y, p) et $I[\bar{f}]$ dans les nouvelles $(\bar{x}, \bar{y}, \bar{p})$.

Une dérivée invariante d'un invariant est encore un invariant, la différentielle extérieure d'une forme invariante est encore une forme invariante etc.

1.5 Le corps différentiel K des invariants rationnels du pb (2)

On trouve dans la thèse de S. Neut le calcul des invariants rationnels du pb (2) obtenu par la méthode d'équivalence de Cartan. Le corps des invariants K est un sous–corps du corps $\mathbb{C}(x, y, p, a)\langle f \rangle$ engendré librement par f et ses dérivées partielles par rapport à (x, y, p). La coordonnée a est accessoire et peut être éliminée. Le corps K est engendré par un nombre fini d'invariants dits *fondamentaux*, sous l'action de dérivations invariantes qui ne commutent pas entre elles en général.

1. les invariants fondamentaux engendrant K

$$\left\{ \begin{array}{rcl} I_1 & = & -\dfrac{1}{4}(f_p)^2 - f_y + \dfrac{1}{2} D_x f_p, \\ I_2 & = & \dfrac{f_{ppp}}{2a^2}, \\ I_3 & = & \dfrac{f_{yp} - D_x f_{pp}}{2a}, \end{array} \right. \tag{5}$$

2. les dérivations invariantes agissant sur K

$$\begin{array}{ll} X_1 = \dfrac{1}{a}\dfrac{\partial}{\partial p}, & X_2 = \dfrac{1}{a}\dfrac{\partial}{\partial y} + \dfrac{1}{2}\dfrac{f_p}{a}\dfrac{\partial}{\partial p} - \dfrac{1}{2} f_{pp} \dfrac{\partial}{\partial a}, \\ X_3 = D_x - \dfrac{1}{2} a f_p \dfrac{\partial}{\partial a}, & X_4 = a \dfrac{\partial}{\partial a}. \end{array} \tag{6}$$

où $D_x = \dfrac{\partial}{\partial x} + p\dfrac{\partial}{\partial y} + f(x, y, p)\dfrac{\partial}{\partial p}$ désigne le champ de Cartan de l'équation $y'' = f(x, y, y')$.

1.6 Les invariants différentiels d'une e-structure

Lorsque le problème de self–équivalence ($\bar{f} = f$)

$$\Delta_f = \sigma_*(\Delta_f) \text{ et } \sigma \in \Phi \tag{7}$$

définit un groupe de symétries (les solutions σ du systéme (7)) de dimension finie, on montre par la méthode d'équivalence de Cartan que le corps K des invariants s'obtient à partir d'une e-structure invariante, c'est à dire un repère mobile invariant défini sur une variété $\widetilde{M}$ fibrée au-dessus[2] de M. Ce repère est défini en coordonnées locales par m champs de vecteurs X_j linéairement indépendants ($m = \dim \widetilde{M}$) ou de manière duale par la donnée de 1-formes différentielles indépendantes (corepère invariant) $\theta^i \in \Omega^1 \widetilde{M}$, $1 \leq i \leq m$ avec la relation de dualité suivante

$$(\theta^i; X_j) = \delta^i_j, \qquad (1 \leq i, j \leq m). \tag{8}$$

Sur l'exemple, dans les coordonnées locales (x, y, p, a) du fibré $\widetilde{M} \to M$, les formes invariantes sont

$$\begin{aligned}
\theta^1 &= a\left((dp - f dx) - \frac{1}{2} f_p (dy - p dx)\right), \\
\theta^2 &= a\,(dy - p dx)\,, \\
\theta^3 &= dx, \\
\theta^4 &= \frac{1}{2} f_{pp}(dy - p dx) + \frac{1}{2} f_p dx + \frac{da}{a}.
\end{aligned} \tag{9}$$

Les invariants fondamentaux sont les coefficients de torsion $T^i_{j,k}$ non constants figurant dans les équations de structure dites équations de Maurer–Cartan :

$$d\theta^i = \sum_{j<k} T^i_{j,k} \theta^j \wedge \theta^k \Longleftrightarrow [X_j, X_k] = \sum_{i=1}^{m} - T^i_{j,k} X_i, \qquad (1 \leq i, j, k \leq m). \tag{10}$$

Ils engendrent le corps des invariants différentiels sous l'action des dérivations invariantes $\{X_j\}_{1 \leq j \leq m}$. Sur l'exemple, les équations de structure de Maurer–Cartan sont

$$\begin{aligned}
\mathrm{d}\theta^1 &= -\theta^1 \wedge \theta^4 + I_1\ \theta^2 \wedge \theta^3, \\
\mathrm{d}\theta^2 &= -\theta^1 \wedge \theta^3 - \theta^2 \wedge \theta^4, \\
\mathrm{d}\theta^3 &= 0, \\
\mathrm{d}\theta^4 &= I_2\ \theta^1 \wedge \theta^2 + I_3\ \theta^2 \wedge \theta^3.
\end{aligned} \tag{11}$$

1.7 Les syzygies entre les invariants différentiels

On écrit que le carré de la différentielle extérieure d'une forme est nulle, i.e. $d^2\ \theta^i = 0$, pour $1 \leq i \leq m$. En tenant compte des relations (11) et en appliquant pour toute fonction invariante I, la règle

$$dI = I_{;1}\ \theta^1 + I_{;2}\ \theta^2 + \cdots + I_{;m}\ \theta^m,$$

on obtient les syzygies cherchées (toutes ?)

$$\begin{gathered}
I_{1;1} + I_3 = 0, \quad I_{1;4} = 0, \quad I_{2;4} + 2I_2 = 0, \\
I_{3;1} + I_{2;3} = 0, \quad I_{3;4} + I_3 = 0.
\end{gathered} \tag{12}$$

Le point-clé est que ces syzygies sont obtenues sans utiliser l'expression des invariants en coordonnées locales. Ainsi, dans la thèse de S. Neut, on calcule instantanément les relations entre des invariants différentiels occupant plusieurs mega-octets en mémoire.

[2] En éliminant le coordonnée a, on se ramène au cas $M = \widetilde{M}$

En principe, on peut tester qu'une expression en les invariants est nulle, en la réécrivant dans une base de Poincaré–Birkhoff–Witt (version algèbres de Lie–Rinehart). En effet, le *collect process*

$$X_iX_j \to [X_i, X_j] + X_jX_i, \qquad (i < j).$$

fonctionne correctement à cause des relations (10). A voir plus en détail !!

1.8 La compression des formules

L'ensemble caractéristique (4) se réecrit dans les invariants différentiels (5) :

$$C_\varphi \left\{ \begin{array}{lcl} \bar{x} & = & -\dfrac{I_1^2}{24} - \dfrac{I_{1;33}}{12}, \\ \bar{y} & = & -\dfrac{I_1}{12}, \\ \bar{p} & = & -\dfrac{I_{1;3}}{12}. \end{array} \right. \tag{13}$$

$$C_f \left\{ \begin{array}{lcl} I_2 & = & 0, \\ I_3 & = & 0, \\ I_{1;331} & = & 0, \\ I_1I_{1;2} + I_{1;332} & = & 0, \\ I_1I_{1;3} + I_{1;333} - 1 & = & 0. \end{array} \right.$$

2 Equations algébriques

2.1 Invariants et covariants de $\mathrm{SL}(n, \mathbb{C})$

Les polynômes (résultants) que l'on génère dans la résolution d'un système d'equations algébriques à n inconnues sont des *covariants* du groupe $G := \mathrm{SL}(n+1, \mathbb{C})$.

Exemple 3 *Soit l'équation $E_f : f(x) = 0$ avec $f(x) := a_{20}x^2 + 2a_{11}x + a_{02}$ et $x \in \mathrm{P}^1\mathbb{C}$.*

Soit $x := X_1/X_2$. Considérons la forme binaire

$$\begin{aligned} F(X_1, X_2) &:= a_{20}X_1^2 + 2a_{11}X_1X_2 + a_{02}X_2^2 \\ &:= \begin{pmatrix} X_1 & X_2 \end{pmatrix} \begin{pmatrix} a_{20} & a_{11} \\ a_{11} & a_{02} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} \end{aligned} \tag{14}$$

Soit $\mathbf{a} := (a_{20}, a_{11}, a_{02})$ et $\mathbf{X} := (X_1, X_2)$. En théorie classique des invariants, les covariants sont, par définition, des éléments de $\mathbb{C}[\mathbf{a}, \mathbf{X}]$ qui sont G-invariants ; les invariants sont, par définition, des éléments de $\mathbb{C}[\mathbf{a}]$.

L'action de $G := \mathrm{SL}(2, \mathbb{C})$ sur les inconnues est définie $\forall \gamma \in G$ par

$$\begin{pmatrix} \overline{X}_1 \\ \overline{X}_2 \end{pmatrix} = \gamma \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}. \tag{15}$$

L'action de G sur les éléments de $\mathbf{a}$ est définie par dualité en posant

$$\gamma^T \cdot \begin{pmatrix} \bar{a}_{20} & \bar{a}_{11} \\ \bar{a}_{11} & \bar{a}_{02} \end{pmatrix} \cdot \gamma = \begin{pmatrix} a_{20} & a_{11} \\ a_{11} & a_{02} \end{pmatrix}. \tag{16}$$

Il est alors clair que

1. F est un covariant par construction : $\overline{F}(\overline{X}_1, \overline{X}_2) = F(X_1, X_2)$.
2. $\Delta := \text{Res}(f, f') = a_{11}^2 - a_{20}a_{02} = -\frac{1}{4}\begin{vmatrix} F_{11} & F_{12} \\ F_{12} & F_{22} \end{vmatrix}$ est un invariant (hessien).

2.2 Calcul des invariants et des covariants de $\mathrm{SL}(n, \mathbb{C})$

Il existe plusieurs façons pour calculer ces invariants par les techniques de géométrie différentielle. On peut utiliser la méthode de Darboux qui généralise la méthode du *repère mobile* de Serret-Frenet pour reconnaitre si deux courbes de $\mathbb{R}^3$ sont applicables l'une sur l'autre par un déplacement rigide : les invariants différentiels fondamentaux sont la courbure et la torsion et la dérivation $\frac{d}{ds}$ où s désigne l'abscisse curviligne est une dérivation G-invariante. Darboux a généralisé cette méthode pour reconnaitre si deux variétés plongées dans un espace homogène $X := G/H$ sont applicables l'une sur l'autre par un certain élément $g \in G$. Les groupes G et H sont des groupes de Lie linéaires quelconques et G opère à gauche sur X. Dans le cas traité par Serret–Frenet, on pose $G := \{$ déplacements $\}$, $H := \{$ rotations $\}$. On a alors $X = \{$ translations $\}$ avec évidemment, $X \simeq \mathbb{R}^3$.

La méthode d'équivalence de Darboux est basée sur le calcul d'une forme de connexion définie sur l'espace homogène X et à valeur dans l'algèbre de Lie du groupe G.

Je rédigerai en détail un autre jour ! ! ! ! !

La méthode de Darboux s'apparente [3] à la méthode de la *cross-section*, développée par Lie et son élève Tresse avant 1900 et reprise par P. Olver dans ses travaux récents. La méthode de la cross-section est en dernière analyse un calcul d'élimination, ce qui m'ennuie un peu.

2.3 Méthode des transvectants

Cette méthode repose sur le fait que l'opérateur bi–différentiel

$$\Omega := \frac{\partial}{\partial X} \otimes \frac{\partial}{\partial Y} - \frac{\partial}{\partial Y} \otimes \frac{\partial}{\partial X} \tag{17}$$

est invariant par l'action linéaire de $\mathrm{SL}(2, \mathbb{C})$ sur les deux coordonnées (X, Y). Cet opérateur Ω, attribué à Cayley, agit sur le produit tensoriel de deux fonctions $F(X, Y)$ et $G(X, Y)$

$$\Omega(F \otimes G) := F_X \otimes G_Y - F_Y \otimes G_X.$$

Il est clair que l' opérateur $\Omega^r := \Omega \circ \cdots \circ \Omega$ (r fois) est également $\mathrm{SL}(2)$-invariant pour tout entier $r \geq 0$. Soit μ l'opérateur de multiplication de deux fonctions F et G

$$\mu : \ F \otimes G \longmapsto FG.$$

Le transvectant d'ordre r de deux covariants F et G qui est noté $(F, G)^{(r)}$ vaut par définition

$$(F, G)^{(r)} := \mu \ \Omega^r(F \otimes G), \qquad (r \geq 0). \tag{18}$$

Il est clair que le transvectant d'ordre r de deux covariants est encore un covariant. Le transvectant d'ordre $r = 1$ de deux fonctions correspond au crochet de Poisson

$$(F, G)^{(1)} = F_X G_Y - F_Y G_X$$

[3]Pour moi, le lien précis reste à faire.

Le calcul de Ω^r par la formule du binôme donne la formule explicite ([1] page 99)

$$(F,G)^{(r)} := \sum_{i=0}^{r} (-1)^i \binom{r}{i} \frac{\partial^r F}{\partial X^{r-i} \partial Y^i} - \frac{\partial^r G}{\partial X^i \partial Y^{r-i}} \qquad (r \geq 0). \tag{19}$$

On retrouve le discriminant d'une forme binaire F de degré 2, à savoir le déterminant hessien de F comme le transvectant $\frac{1}{2}(F,F)^{(2)}$ d'ordre $r = 2$.

On a les deux théorèmes de complétude ([1] page 102) suivants

Théorème 1 *Soit $Q_1, \ldots, Q_m$ un système de formes binaires. Alors tout polynôme* SL(2)-*covariant s'exprime comme une combinaison linéaire des transvectants successifs entre les formes $Q_1, \ldots, Q_m$.*

Théorème 2 *Soit Q une forme binaire de degré n. Alors les polynômes Q, $R_r := (Q,Q)^{(2r)}$, $0 \leq 2r \leq n$ et $(Q, R_r)^{(1)}$, $0 \leq 2r \leq n-1$ constituent un système complet de n covariants de Q rationnellement indépendants.*

Références

[1] P. J. Olver. *Equivalence, invariants and symetry.* Graduate Texts in Mathematics. Cambridge University Press, 1995.