Factorisation et Résolution des polynômes paramétriques

Ali AYAD

1 Resumé de l'exposé dans les Journées Nationales du Calcul Formel 2005

J'exposerai deux algorithmes, le premier porte sur la factorisation absolue des polynômes paramétriques et le deuxième sur la résolution des systèmes algébriques paramétriques zéro-dimensionnels. Notons que le deuxième sera utilisé comme sous-algorithme du premier.

1.1 Factorisation absolue des polynômes paramétriques

Etant donné un corps commutatif F de caractéristique quelconque $p \geq 0$ et un polynôme paramétrique $f \in F[u_1, \ldots, u_r, Z_0, \ldots, Z_n]$ où les variables $u = (u_1, \ldots, u_r)$ sont des paramètres qui peuvent prendre des valeurs dans l'espace $\mathcal{P} = \overline{F}^r$ qui sera appelé l'espace des paramètres. La question posée est d'obtenir une factorisation absolue de f qui est valable pour une valeur générique des paramètres. Celle-ci est obtenue par un algorithme qui décompose l'espace des paramètres $\mathcal{P}$ à

$$d^{O(nr^2d^2)}$$

ensembles constructibles $\mathcal{U}$ deux à deux disjoints qui vérifient:

1) Chaque $\mathcal{U}$ est donné par ses équations et ses inéquations de degrés bornés par

$$d^{O(d^2)}$$

2) Pour chaque $\mathcal{U}$ l'algorithme calcule s polynômes $G_j \in F(C, u)[Z_0, \ldots, Z_n]$ $(1 \leq j \leq s \leq d)$ et un polynôme $\chi \in F(u)[C]$ où C est une nouvelle variable. Pour toute spécialisation des paramètres $a = (a_1, \ldots, a_r) \in \mathcal{U}$, il existe $c \in \overline{F}$, racine de $\chi^{(a)} \in \overline{F}[C]$ (aucun des dénominateurs des coefficients de χ ne s'annule en a) qui vérifie:

- Aucun des dénominateurs des coefficients de G_j ne s'annule en (c, a).

- $\deg_C(G_j), \deg_C(\chi) \leq d^{O(d)}$, $\deg_u(G_j), \deg_u(\chi) \leq d^{O(d^2)}$ (le degré d'une fonction rationnelle est le maximum de degrés de son numérateur et de son dénominateur).

- La factorisation absolue du polynôme $f^{(a)} := f(a_1, \ldots, a_r, Z_0, \ldots, Z_n) \in \overline{F}[Z_0, \ldots, Z_n]$ est donnée par:

$f^{(a)} = \prod_{1 \leq j \leq s} \left(G_j^{(c,a)}\right)^{k_j}$, $G_j^{(c,a)} := G_j(c, a_1, \ldots, a_r, Z_0, \ldots, Z_n)$ est absolument irréductible.

En particulier, le nombre des facteurs absolument irréductibles distincts de $f^{(a)}$ est constant sur $\mathcal{U}$ et il est égale à s. Le vecteur de multiplicités $(k_1, \ldots, k_s)$ est le même pour tout $a \in \mathcal{U}$.

Cet algorithme est basé sur le lemme de Hensel, l'élimination des quantificateurs dans la théorie des corps algébriquement clos et sur l'algorithme suivant:

1.2 Résolution des systèmes algébriques paramétriques zéro-dimensionnels

Soient $f_1, \ldots, f_k \in F[u_1, \ldots, u_r, X_0, X_1, \ldots, X_n]$ des polynômes paramétriques homogènes en $X_0, X_1, \ldots, X_n$ de degré $\leq d$ chacun, soit δ une borne supérieure des degrés de $f_1, \ldots, f_k$ par rapport aux paramètres $u = (u_1, \ldots, u_r)$. La question posée ici est de décrire les solutions du système $f_1 = \cdots = f_k = 0$ qui sont valables pour une valeur générique des paramètres. On s'intéresse ici seulement au sous-ensemble $\mathcal{V}$ de $\mathcal{P}$ qui est formé par les paramètres $a \in \mathcal{P}$ tel que le système $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ est de dimension zéro et n'admet pas de solutions à l'infini, i.e la variété $V^{(a)} := \{f_1^{(a)} = \cdots = f_k^{(a)} = 0\}$ est un sous-ensemble fini de $P^n(\overline{F})$ et $V^{(a)} \cap \{X_0 = 0\} = \emptyset$. On décrit un algorithme qui décompose $\mathcal{V}$ à

$$\delta^{r^2} O\Big((nd)^{2n^2r^2}\Big)$$

ensembles constructibles $\mathcal{W}$ deux à deux disjoints qui vérifient:

1) Les degrés des équations et des inéquations qui définissent $\mathcal{W}$ sont bornés par

$$\delta O\Big((nd)^{2n^2}\Big).$$

2) Le nombre D des solutions est constant sur $\mathcal{W}$.
3) Pour chaque $\mathcal{W}$, l'algorithme calcule de polynômes $\chi, \psi_1, \ldots, \psi_n \in F(u_1, \ldots, u_r)[Z]$ de degrés inférieurs ou égale à D. Toute spécialisation des paramètres $a \in \mathcal{W}$ vérifie:
- Aucun des dénominateurs des coefficients de $\chi, \psi_1, \ldots, \psi_n$ ne s'annule en a.
- Les degrés des coefficients de $\chi, \psi_1, \ldots, \psi_n$ par rapport à $u_1, \ldots, u_r$ sont bornés par $\delta O\Big((nd)^{2n^2}\Big)$.
- Pour toute solution $(\xi_0, \ldots, \xi_n) \in P^n(\overline{F})$ du système homogène $f_1^{(a)} = \cdots = f_k^{(a)} = 0$, il existe une racine η de $\chi^{(a)} \in \overline{F}[Z]$ vérifiant:

$$\Big(\frac{\xi_j}{\xi_0}\Big)^{p^{\nu_j}} = \psi_j^{(a)}(\eta), \quad 1 \leq j \leq n.$$

Cet algorithme calcule les U-Résultants des variétés $V^{(a)}$ d'une manière générique, il utilise l'élimination de Gauss et le Shape lemma sous forme paramétrique.
N.B: On peut produire un algorithme qui cherche toutes les solutions (même les solutions à l'infini).

Une telle décomposition de $\mathcal{V}$ se trouve dans les travaux de Grigoriev et Vorobjov (2000), leur algorithme calcule une base de Gröbner *paramétrique* du système $(f_1, \ldots, f_k)$ avec une complexité simplement exponentielle en n.
Schost (2002) a décrit une telle représentation des solutions qui est valable seulement pour un hypersurface de l'espace des paramètres $\mathcal{P}$ avec la même borne de complexité. Citons encore les travaux de Weispfenning (1990); Gao et Chou (1992); Lazard et Rouillier (2004).