Calcul algébrique efficace de résolvantes relatives

Philippe Aubry, Annick Valibouze

LIP6 - Université Pierre et Marie Curie

Journées Nationales du Calcul Formel
Luminy 2010

Historique

$f \in k[x]$ de degré n avec n racines distinctes $(\alpha_1, \ldots, \alpha_n) = \underline{\alpha}$

Résolvante : polynôme univarié résultant de la transformation de f relative à un groupe L par l'invariant d'un sous-groupe H de L.

- Lagrange (1770) : résolvante absolue de f dans le cadre de la résolution d'équation par radicaux.
  - $L = \mathfrak{S}_n$, le groupe symétrique de degré n.
  - Les facteurs des résolvantes absolues déterminent le groupe de Galois de f (Arnaudiès-Val, 1993).
- Jordan (1870) : résolvante relative à L, avec $G < L < \mathfrak{S}_n$ où G groupe de Galois de $\underline{\alpha}$.
  - La descente de Jordan dans le graphe des sous-groupes détermine G.

Calcul des résolvantes

- Absolues : ses coefficients sont des fonctions symétriques des racines de $f \longrightarrow$ théorème fondamental des fonctions symétriques. Plusieurs algorithmes sont implantés dans Maxima (module "Symmetries")
- Relatives : ses coefficients sont invariants par le groupe G. Problème de la version effective du théorème de Galois.
  - Stauduhar (1973) : méthode numérique
  - Arnaudiès-Valibouze (1993) : méthode algébrique utilisant les éléments primitifs des corps (coût important)
  - Aub-Val (1998) : méthode algébrique d'élimination la calculant à la puissance Card(H).

But : éviter la puissance superflue.

Idéaux galoisiens

$k(\underline{\alpha})$ isomorphe à $k[x_1, \ldots, x_n]/\mathfrak{M}$ où

$$\mathfrak{M} = \{r \in k[x_1, \ldots, x_n] \mid r(\underline{\alpha}) = 0\}$$

idéal maximal des $\underline{\alpha}$-relations. Le *groupe de Galois* de $\underline{\alpha}$ est :

$$G = Stab_{\mathfrak{S}_n}(\mathfrak{M})$$

Déf. idéal galoisien

Idéal des $\underline{\alpha}$-relations invariantes par L où $L \subset \mathfrak{S}_n$

$$I \quad = \quad \{r \in k[x_1, \ldots, x_n] \mid \forall \sigma \in L \quad \sigma.r(\underline{\alpha}) = 0\}$$

Note : $I = Id(L.\underline{\alpha})$

L n'est pas forcément un groupe :
$\mathfrak{M} = Id(I_n.\underline{\alpha}) = Id(G.\underline{\alpha}) = Id(\{g\}.\underline{\alpha}), \forall g \in G$

Idéaux galoisiens triangulaires

Un idéal galoisien I est *pur* s'il existe un groupe L tel que :

$$G < L \text{ et } I = Id(L.\underline{\alpha})$$

Propriété (Aub-Val, 1998)

Un idéal galoisien pur est triangulaire

Exemples

- $\mathfrak{M}$ idéal des $\underline{\alpha}$-relations
- $\mathcal{S} = Id(\mathfrak{S}_n.\underline{\alpha})$ idéal des relations symétriques

$\mathcal{S}$ est triangulaire. Engendré par les *modules de Cauchy*

$$C_n = f(x_n), C_{n-1} = C_n(x_{n-1}) - C_n(x_n)/(x_{n-1} - x_n), \ldots$$

formant un ensemble triangulaire séparable.

Nous avons besoin que I soit triangulaire. Pour simplifier nous supposons I galoisien pur dans la suite.

Polynôme caractéristique et résolvante

$\Theta \in k[x_1, \ldots, x_n]$, k corps parfait.
$\widehat{\Theta}$ endomorphisme multiplicatif de $k[x_1, \ldots, x_n]/I$: $P \mapsto \Theta P$

Polynôme caractéristique de $\widehat{\Theta}$:

$$\chi_{\widehat{\Theta},I} = \prod_{\sigma \in L} (x - (\sigma.\Theta)(\underline{\alpha}))$$

Résolvante de $\underline{\alpha}$ *par* Θ *relative à* L :

$$R_{\Theta,I} = \prod_{\Psi \in L.\Theta} (x - \Psi(\underline{\alpha})) \in k[x]$$

H stabilisateur de Θ dans $L \rightsquigarrow \chi_{\widehat{\Theta},I} = R_{\Theta,I}^{\mathrm{card}(H)}$

Si $R_{\Theta,I}$ est square-free, c'est le polynôme minimal de $\widehat{\Theta}$.

Résolvante par extraction de racine de $\chi_{\Theta,I}$ (1998)

$T = \{f_1(x_1, \ldots, x_n), \ldots, f_{n-1}(x_{n-1}, x_n), f_n(x_n)\}$ engendre I,
$h = \mathrm{card}(H)$

Resolvent(T, Θ, h):
$\chi := x - \Theta$
Pour i de 1 à n Faire
$\chi := \mathrm{Res}_{x_i}(f_i, \chi)$
Fin Pour
Retourner($\chi^{1/h}$)

Idée : $\chi_{\widehat{\Theta},I} = \prod_{\sigma \in L}(x - \Theta(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = R^h_{\Theta,I}$.
Le premier résultant élimine x_1 dans $\chi = x - \Theta(x_1, \ldots, x_n)$, c'est-à-dire, le réécrit en χ dans $k[x_2, \ldots, x_n]$ comme le produit de ses valeurs possibles données par le polynôme f_1. Le second résultant en fait de même avec f_2 et x_2, et ainsi de suite.

Eviter le calcul de $\chi_{\Theta,I}$

Cause de la puissance superflue h :
$\mathrm{Res}_{x_i}(f_i, \chi)$ élimine x_i sans tenir compte des invariances de χ dans $k[x_i, \ldots, x_n]$. Chaque étape crée donc sa puissance superflue m_i :

$$h = m_1 \cdots m_n$$

Objectif : Eliminer m_i après le i-ème résultant.

- Pb 1 : Détermination des m_i
  $\longrightarrow$ à partir du groupe H
- Pb 2 : Extraction de racine m-ième dans un anneau $A[x]$
  $\longrightarrow$ A anneau quotient

Précalcul des m_i

Chaîne de sous-groupes de $H = Stab_L(\Theta)$:

$$\{Id\} = H_1 < H_2 < \ldots < H_n < H_{n+1} = H$$

avec $H_i = \{\tau \in H \mid \forall k \in [\![i, n]\!],\ \tau(k) = k\}$,
ou inductivement $H_i = Stab_{H_{i+1}}(i)$

Puissance superflue du i-ème résultant

$$m_i = \mathrm{card}(H_{i+1})/\mathrm{card}(H_i)$$

Assez intuitif à partir du résultat

$$Zeros(f_i(x, \alpha_{\tau(i+1)}, \ldots, \alpha_{\tau(n)})) = \{\alpha_{\tau\sigma(i)}, \sigma \in L_{i+1}/L_i\}$$

Usage des m_i

Nota : $R_i = \prod_{\sigma \in L_i/H_i} (x - \sigma.\Theta)$

Propriété

Après la i-ème étape de l'algorithme Resolvent on a

$$\chi = {R_{i+1}}^{\mathrm{card}(H_{i+1})} \mod I$$

Rappel:

```
Resolvent(T, Θ, h):
    χ := x − Θ
    Pour i de 1 à n Faire
        χ := Res_{x_i}(f_i, χ)
    Fin Pour
    Retourner(χ^{1/h})
```

Remarque : On ne peut pas se passer du quotient par I en toute généralité.

Cas des résolvantes absolues

Lehobey (1997) : élimination de puissances superflues en cours de calcul pour résolvantes absolues (modules de Cauchy pour T).
$\longrightarrow$ Appel à extraction de racine m-ième dans $k[x_i, \ldots, x_n][x]$.

$\rightsquigarrow$ Pourquoi peut-on s'abstraire du quotient ?

Propriété : Si $L_i. < f_1, \ldots, f_{i-1} > = < f_1, \ldots, f_{i-1} >$ alors

$$\chi = {R_{i+1}}^{\mathrm{card}(H_{i+1})}$$

L'ensemble $T = \{C_1(x_1, \ldots, x_n), \ldots, C_n(x_n)\}$ satisfait la propriété.
Plus précisément,

Propriété des modules de Cauchy :

$$\forall j, 1 \leq j \leq n, \quad \mathfrak{S}_n.C_j \subset \langle C_1, \ldots, C_j \rangle$$

Anneau de base de l'extraction - Exemple

$f = x^6 + 2$. Idéal galoisien avec
$L =< (1,3)(2,4), (1,3,4)(2,5,6), (2,3)(4,5), (3,5)(4,6), (3,4,5,6) >$,

$$\begin{aligned} T \quad = \{ \quad & f_6 = C_6(x_6), f_5 = C_5(x_5, x_6), f_4 = C_4(x_4, x_5, x_6), \\ & f_3 = x_3 - g_3, f_2 = x_2 - g_2, \\ & f_1 = x_1 - g_2 - g_3 + x_4 + x_5 + x_6\} \end{aligned}$$

$H =< (1,2)(3,4)(5,6), (1,3,5)(2,4,6), (3,5)(4,6) >$ et
$\Theta = x_1x_4 + x_1x_6 + x_2x_3 + x_2x_5 + x_3x_6 + x_4x_5$

On a $H_4 = \{\mathrm{Id}\} \Rightarrow m_1 = m_2 = m_3 = 1$.
$m_4 = \mathrm{card}(H_5) = 2$.

Résultant en x_4 de f_4 et $x - \Theta(g_2 + g_3 - x_4 - x_5 - x_6, g_2, g_3, x_4, x_5, x_6)$:
polynôme γ tq $\deg_x(\gamma) = 4$.

γ est un carré dans $k[x_5, x_6]/ < C_5, C_6 >$ mais $\mathrm{pgcd}(\gamma, \gamma') = 1$.

On constate $L_5. < f_1, \ldots, f_4 > \not\subset < f_1, \ldots, f_4 >$

Algorithme 1

Calcul préalable des $m_i = \mathrm{card}(H_{i+1})/\mathrm{card}(H_i)$
Nota : $T_i = \{f_i(x_i, \ldots, x_n), \ldots, f_{n-1}(x_{n-1}, x_n), f_n(x_n)\}$

RelativeResolvent1($T, \Theta, [m_1, \ldots, m_n]$):
  $\mathcal{L} := x - \Theta \mod T$
  Pour i de 1 à n Répéter
    $\gamma := \mathrm{Res}_{x_i}(f_i, \mathcal{L}) \mod T_{i+1}$
    $\mathcal{L} := \mathrm{NthRoot}(\gamma, m_i) \mod T_{i+1}$
    Fin Pour
  Retourner $\mathcal{L}$

Basé sur les propriétés précédentes et propriétés basiques du résultant.

NthRoot - Racine m-ième

Problème : A anneau commutatif unitaire, m entier donné. Soit $g \in A[x]$ de degré n tel que $g = h^m$. Trouver h.

$s = \deg(h) = n/m$.
Soient $p_1(g), \ldots, p_s(g)$ fonctions puissances des racines de g :

$$p_i(g) = \beta_1^i + \cdots + \beta_s^i$$

Les fonctions puissances des racines de h :

$$p_i(h) = p_i(g)/m$$

Solution : avec g et h passage

fonctions sym élémentaires $e_i \longleftrightarrow$ fonctions puissances

par les formules classiques de Girard-Newton

$$p_r - p_{r-1}e_1 + \cdots + (-1)^{r-1}p_1 e_{r-1} + (-1)^r r.e_r = 0$$

NthRoot - Racine m-ième

Calcul de la racine m-ième ci-dessus en $O(s^2)$.
Valide si on peut diviser par les entiers jusqu'à s et par m.

Autres méthodes disponibles venant de la décomposition polynomiale, ou d'inspiration analytique.
A base d'itération de Newton, complexité en $O(M(n)\log(r))$.
Mais les puissances sont en pratique petites.

Eviter le calcul de coefficients inutiles

L'extraction de racine m-ième ne nécessite que les $s = n/m$ coefficients de plus haut degrés de g.
$\Rightarrow$ Les autres coefficients du résultant calculé à chaque étape sont inutiles

$\rightsquigarrow$ Passer par une transformation réciproque des polynômes pour calculer les résultants $\mod x^{s+1}$.

- Degré de $\mathcal{L}$ à la i-ème étape connu : $s = s_i = \frac{\mathrm{card}(L_i)}{\mathrm{card}(H_i)}$

- Commutation résultant-polynôme réciproque :

$$f_i \text{ unitaire en } x_i \text{ et } \gamma \text{ unitaire en } x$$
$$\Rightarrow \mathrm{Res}_{x_i}(f_i, \mathrm{Recip}(\gamma)) = \mathrm{Recip}(\mathrm{Res}_{x_i}(f_i, \gamma))$$

où $\mathrm{Recip}(p)$ polynôme réciproque de p en x

Algorithme 2

RelativeResolvent2($T, \Theta, [m_1, \ldots, m_n], [s_1, \ldots, s_n]$):

$\mathcal{L} := x - \Theta \mod T$

Pour i de 1 à n Répéter

$\Gamma := \mathrm{Recip}(\mathcal{L})$

$T' := T_{i+1} \cup \{x^{s_i+1}\}$

$\Gamma := \mathrm{Res}_{x_i}(f_i, \Gamma) \mod T'$

$\gamma' := \mathrm{Recip}(\Gamma)$

$\mathcal{L} := \mathrm{NthRoot}(\gamma', m_i, s_i) \mod T'$

Fin Pour

Retourner $\mathcal{L}$