Algorithmique dans les algèbres d'invariants polynomiaux sous un groupe fini

Romain Lebreton

LIX
Laboratoire d'Informatique
École polytechnique
FRANCE

Travaux en cours en collaboration avec
E. Schost (UWO, London, Canada)

Jeudi 6 Mai 2010

Motivation

Le principe de l'algorithmique des polynômes invariants

Tirer partie des symétries d'un problème pour en réduire la complexité.

Quelques lieux de vie de polynômes invariants

- la modélisation de phénomènes physiques avec symétries ;
- la théorie de Galois effective (résolvante de Lagrange) ;
- l'étude de codes correcteurs auto-duaux (polynôme énumérateur des poids)...

Cadre de l'exposé

Dans la suite de l'exposé :

- k corps ;
- $k[\mathbf{X}] = k[X_1, \ldots, X_n]$;
- H sous-groupe fini de $\mathbf{GL}_n(k)$;
- $\operatorname{car} k = 0$ ou $\operatorname{car} k$ premier avec l'ordre de H ;
- Action à droite du groupe $\mathbf{GL}_n(k)$ sur $k[\mathbf{X}]$:

$$\begin{array}{ccccc} k[\mathbf{X}] & \times & \mathbf{GL}_n(k) & \longrightarrow & k[\mathbf{X}] \\ (p & , & A) & \longmapsto & p^A \end{array}$$

avec

$$p^A(\mathbf{X}) := p\,(a_{11}X_1 + \cdots + a_{1n}X_n, \cdots, a_{n1}X_1 + \cdots + a_{nn}X_n)$$

et A la matrice $[a_{i,j}]$.

Action de groupe

- Action à droite du groupe $\mathbf{GL}_n(k)$ sur $k[\mathbf{X}]$: $(p, A) \longmapsto p^A$.
- Action à gauche du groupe $\mathbf{GL}_n(k)$ sur l'espace affine $\mathbb{A}_k^n \simeq k^n$:

$$\begin{array}{ccccc} \mathbf{GL}_n(k) & \times & \mathbb{A}_k^n & \longrightarrow & \mathbb{A}_k^n \\ (A & , & \boldsymbol{x}) & \longmapsto & A\,\boldsymbol{x} \end{array}$$

  avec $A\,\boldsymbol{x}$ produit usuel matrice vecteur.
- Cette action à gauche $\mathbb{A}_k^n$ est cohérente avec l'action à droite sur $k[\mathbf{X}]$, c.-à-d. $p^A(\boldsymbol{x}) = p(A\,\boldsymbol{x})$.

Remarques

- Tout sous-groupe de permutation $H \subset \mathfrak{S}_n$ sera vu comme $H \subset \mathbf{GL}_n(k)$
- On identifiera la permutation τ avec sa *matrice de permutation* $A_\tau = (\delta_{i,\tau(j)})$.

Algèbres des invariants polynomiaux

- $k[\mathbf{X}]^H$ est l'ensemble des polynômes de $k[\mathbf{X}]$ invariants sous l'action de H.
- $k[\mathbf{X}]^H$ est une k-algèbre, graduée pour le degré total.

Exemple

$$\mathfrak{A}_3 = < \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} >, V_3 = (X_3 - X_2)(X_3 - X_1)(X_2 - X_1).$$

On a $V_3 \in k[X_1, X_2, X_3]^{\mathfrak{A}_3}$ mais $V_3 \notin k[X_1, X_2, X_3]^{\mathfrak{S}_3}$.

Opérateur de Reynolds

- L'opérateur de Reynolds

$$\mathcal{R}_H : \begin{array}{rcl} k[\mathbf{X}] & \longrightarrow & k[\mathbf{X}]^H \\ p & \longmapsto & \frac{1}{|H|} \sum_{g \in H} p^g \end{array}$$

  est un morphisme de $k[\mathbf{X}]^H$-module surjectif.

- Les Reynolds de monômes $R_H(m)$ engendrent $k[\mathbf{X}]^H$;

Opérateur de Reynolds - Remarques

Une représentation plus compacte

$$
\begin{aligned}
V_3 &= (X_3 - X_2)(X_3 - X_1)(X_2 - X_1) \\
&= {X_3}^2 X_2 + {X_2}^2 X_1 + {X_1}^2 X_3 - {X_2}^2 X_3 - {X_3}^2 X_1 - {X_3}^2 X_2 \\
&= 3\ \mathcal{R}_{\mathfrak{A}_3}({X_1}^2 X_3) - 3\ \mathcal{R}_{\mathfrak{A}_3}({X_1}^2 X_2)
\end{aligned}
$$

- On a réduit la dimension de l'algèbre linéaire :

$$\dim k[\mathbf{X}]_d^H \underset{d \to \infty}{\sim} \frac{1}{|H|} \dim k[\mathbf{X}]_d.$$

Remarque

Soient m, m' des monômes, alors en général $\mathcal{R}_H(mm') \neq \mathcal{R}_H(m)\mathcal{R}_H(m')$
$\hookrightarrow$ Pas adaptée pour la structure multiplicative.

Formule de Molien

La formule de Molien nous donne la série de Hilbert de $k[\mathbf{X}]^H$:

$$\mathrm{HS}(k[\mathbf{X}]^H, t) := \sum_{d \geq 0} \dim(k[\mathbf{X}]^H_d) t^d = \frac{1}{|H|} \sum_{h \in H} \frac{1}{\det(\mathrm{Id}_n - th)}.$$

Exemple

$$\begin{aligned}
M_{\mathfrak{A}_3}(t) &= \frac{1}{3}\left[\frac{1}{\det(\mathrm{Id}_3 - t.\,\mathrm{Id}_3)} + 2/\det\begin{pmatrix} 1 & -t & 0 \\ 0 & 1 & -t \\ -t & 0 & 1 \end{pmatrix}\right] \\
&= \frac{1}{3}\left(1/(1-t)^3 + 2/(1-t^3)\right) \\
&= 1 + t + 2t^2 + 4t^3 + 5t^4 + 7t^5 + O(t^6)
\end{aligned}$$

Décomposition de Hironaka

Problème

Trouver la structure algébrique de $k[\mathbf{X}]^H$.

Exemple

Soient $e_1, \ldots, e_n \in k[\mathbf{X}]^{\mathfrak{S}_n}$ les polynômes symétriques élémentaires.
Alors $k[\mathbf{X}]^{\mathfrak{S}_n} = k[e_1, \ldots, e_n]$ est une algèbre de polynômes.
$\hookrightarrow$ Ce n'est pas toujours le cas.

Exemple

$k[\mathbf{X}]^{\mathfrak{A}_n} = k[e_1, \ldots, e_n] \oplus k[e_1, \ldots, e_n] V_n$ avec $V_n = \prod_{1 \leq i < j \leq n} (X_j - X_i)$.

Théorème de décomposition de Hironaka

Théorème (Hochster-Eagon, 1971)

Il existe n invariants homogènes $\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_n)$, appelés invariants primaires, tels que $k[\mathbf{X}]^H$ soit un $k[\mathbf{\Pi}]$-module libre.
Les invariants secondaires, notés $\mathbf{\Sigma} = (\Sigma_1 = 1, \ldots, \Sigma_r)$, sont une base de $k[\mathbf{X}]^H$ comme $k[\mathbf{\Pi}]$-module.

$$k[\mathbf{X}]^H = \bigoplus_{i=1}^{r} k[\mathbf{\Pi}]\Sigma_i.$$

Remarque

Le choix des invariants primaires conditionne le nombre d'invariants secondaires :

$$r = \frac{1}{|H|}\left(\prod_{i=1}^{n} \deg(\Pi_i)\right).$$

Algorithme pour les invariants primaires

Test effectif pour les primaires

$\Pi_1, \ldots, \Pi_n$ sont des invariants primaires si et seulement si $\dim k[\mathbf{X}]/(\Pi_1, \ldots, \Pi_n) = 0$.

$\hookrightarrow$ On peut toujours prendre $e_1, \ldots, e_n$ comme invariant primaires pour $H \subset \mathfrak{S}_n$.

Algorithme de recherche d'invariants primaires de Magma [Kemper]

On cherche les invariants primaires dont le produit des degrés est minimal.

Exemple

Pour le groupe $K =< (1,4)(2,3), (1,2)(3,4) >\subset \mathfrak{S}_4$, prenons
$\Pi_1 = X_1 + X_2 + X_3 + X_4$, $\Pi_2 = X_1^2 + X_2^2 + X_3^2 + X_4^2$,
$\Pi_3 = X_1X_2 + X_3X_4$, $\Pi_4 = X_1X_3 + X_2X_4$ et
$\Sigma_1 = 1$, $\Sigma_2 = X_1^3 + X_2^3 + X_3^3 + X_4^3$.

Algorithme pour les invariants secondaires

Test effectif pour les invariants secondaires

$\Sigma_1, \ldots, \Sigma_n$ sont des invariants secondaires si et seulement s'ils forment une base du k-espace vectoriel $k[\mathbf{X}]^H/(\Pi_1, \ldots, \Pi_n) = F$.

Algorithme de recherche d'invariants secondaires de Magma [Kemper]

1. Calculer les $c_j \in \mathbb{N}$ tels que

$$\mathrm{HS}(F,t) = \mathrm{HS}(k[\mathbf{X}]^H, t) \prod_{i=1}^{n} (1 - t^{\deg \Pi_i}) = 1 + c_1 t + \ldots + c_e t^e.$$

2. Pour tout d tel que $c_d \neq 0$, on cherche une base de F_d.

Réduction modulo p du problème

Complexité

Le coût dominant de l'algorithme est celui du calcul d'une base de Gröbner.

Réduction modulo p dans le cas $k = \mathbb{Q}, H \subset \mathbf{GL}_n(\mathbb{Z})$:

Soit $p \in \mathbb{N}$ premier ne divisant pas $|H|$,

$$\bmod p : \begin{array}{ccccc} H \subset \mathbf{GL}_n(\mathbb{Z}) & \text{agit sur} & \mathbb{Z}[\mathbf{X}] & \rightsquigarrow & \mathbb{Z}[\mathbf{X}]^H \\ \downarrow & & \downarrow & & \downarrow \\ \overline{H} \subset \mathbf{GL}_n(\mathbb{F}_p) & \text{agit sur} & \mathbb{F}_p[\mathbf{X}] & \rightsquigarrow & \mathbb{F}_p[\mathbf{X}]^{\overline{H}}. \end{array}$$

Le test amélioré

Test amélioré pour les primaires [L.-Schost]

$\Pi_1, \ldots, \Pi_n \in \mathbb{Z}[\mathbf{X}]^H$ sont des invariants primaires si et seulement si $\dim \mathbb{F}_p[\mathbf{X}]/(\overline{\Pi_1}, \ldots, \overline{\Pi_n}) = 0$.

Test amélioré pour les invariants secondaires [L.-Schost]

$\Sigma_1, \ldots, \Sigma_r \in \mathbb{Z}[\mathbf{X}]^H$ sont des invariants secondaires si et seulement si $(\overline{\Sigma_1}, \ldots, \overline{\Sigma_r})$ est une base du k-espace vectoriel $\mathbb{F}_p[\mathbf{X}]^H/(\overline{\Pi_1}, \ldots, \overline{\Pi_n})$.

$$\Updownarrow$$

Théorème ([L.-Schost, Roth-Wehlau])

Si $\overline{\Pi_1}, \ldots, \overline{\Pi_n}, \overline{\Sigma_1}, \ldots, \overline{\Sigma_r}$ sont des invariants primaires/secondaires de $\mathbb{F}_p[\mathbf{X}]^{\overline{H}}$, alors $\Pi_1, \ldots, \Pi_n, \Sigma_1, \ldots, \Sigma_r$ sont des invariants primaires/secondaires de $\mathbb{Q}[\mathbf{X}]^H$.

Idée de la preuve

Hypothèse

Soient $\Pi_1, \ldots, \Pi_n, \Sigma_1, \ldots, \Sigma_r \in \mathbb{Z}[\mathbf{X}]^H$ avec $\mathbb{F}_p[\mathbf{X}]^{\overline{H}} = \bigoplus_{i=1}^r \mathbb{F}_p[\overline{\mathbf{\Pi}}]\overline{\Sigma_i}$.

Lemme (admis cf. [Derksen-Kemper])

- $\mathrm{HS}(\mathbb{Q}[\mathbf{X}]^H, t) = \mathrm{HS}(\mathbb{F}_p[\mathbf{X}]^{\overline{H}}, t)$.

Alors pour tout degré d, on a

$$\begin{aligned}
\dim_{\mathbb{Q}}(\mathbb{Q}[\mathbf{X}]^H)_d &\geq \dim_{\mathbb{Q}} \left(\sum_{i=1}^r \mathbb{Q}[\mathbf{\Pi}]\Sigma_i \right)_d \\
&\geq \dim_{\mathbb{F}_p} \left(\bigoplus_{i=1}^r \mathbb{F}_p[\overline{\mathbf{\Pi}}]\overline{\Sigma_i} \right)_d = \dim_{\mathbb{F}_p}(\mathbb{F}_p[\mathbf{X}]^{\overline{H}})_d.
\end{aligned}$$

Ainsi $\mathbb{Q}[\mathbf{X}]^H = \bigoplus_{i=1}^r \mathbb{Q}[\mathbf{\Pi}]\Sigma_i$. $\square$

Biliographie (non exhaustive)

Quelques livres :

- Sturmfels B., *Algorithms in invariant theory*, Springer, 93.
- Derksen H., Kemper G., *Computational invariant theory*, Springer, 02.

Articles sur le calcul d'invariants primaires et secondaires :

- Kemper G., *An algorithm to calculate optimal homogeneous systems of parameters*, JSC 99,
- King S., *Fast Computation of Secondary Invariants*, arXiv 07.

Merci pour votre attention ...
et bon appétit !

bouillabaisse3.jpg