Rational and Algebraic Invariants of a Group Action

Evelyne Hubert

IMA, February 2007.

Synopsis

Algorithm to compute a **generating set of rational invariants** of an algebraic group action, together with a simple **rewriting algorithm**.

E. Hubert and I. Kogan, *Rational Invariants of a Group Action. Construction and Rewriting.* Journal of Symbolic Computation 42:1-2, p 203-217 (2007).

Provide **algebraic & algorithmic foundations** to the **moving frame method** for the construction of **differential invariants** [Fels & Olver, 1999].

E. Hubert and I. Kogan. *Smooth and Algebraic Invariants of a Group Action. Local and Global Constructions.*

Original motivation: Symmetry reduction of differential systems [Mansfield 2001]

Contents

1 Rational Invariants of a Group Action

1.1 Definitions

Algebraic Group $\mathcal{G}$

$\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$

$\mathcal{G} \subset \mathbb{K}^l$ an algebraic variety $\qquad G \subset \mathbb{K}[\lambda_1, \ldots, \lambda_l]$ its ideal

$$\begin{array}{rrcl} m: & \mathcal{G} \times \mathcal{G} & \to & \mathcal{G} \\ & (\lambda, \mu) & \mapsto & \lambda \cdot \mu \end{array} \qquad \text{and} \qquad \begin{array}{rrcl} i: & \mathcal{G} & \to & \mathcal{G} \\ & \lambda & \mapsto & \lambda^{-1} \end{array}$$

$$\lambda \cdot \mu \in \mathbb{K}[\lambda, \mu] \qquad \text{and} \qquad \lambda^{-1} \in \mathbb{K}[\lambda]$$

$$e \in \mathcal{G} \quad e \cdot \lambda = \lambda \cdot e = \lambda$$

$\mathcal{G}$	$\mathbb{K}^*$	$\mathbb{K} \times \{-1, 1\}$	$SO(2)$
G	$(\lambda_1 \lambda_2 - 1)$	$(\lambda_2^2 - 1)$	$(\lambda_1^2 + \lambda_2^2 - 1)$
$\lambda \cdot \mu$	$(\lambda_1\mu_1, \lambda_2\mu_1)$	$(\lambda_1 + \mu_1, \lambda_2\mu_2)$	$(\lambda_1\mu_1 - \lambda_2\mu_2, \lambda_1\mu_2 + \lambda_2\mu_1)$
e	$(1, 1)$	$(0, 1)$	$(1, 0)$
λ^{-1}	(λ_2, λ_1)	$(-\lambda_1, \lambda_2)$	$(\lambda_1, -\lambda_2)$

Rational Action on $\mathcal{Z} = \mathbb{K}^n$

$$\begin{array}{rrcl} g: & \mathcal{G} \times \mathcal{Z} & \to & \mathcal{Z} \\ & (\lambda, z) & \mapsto & \lambda \star z = \left(\dfrac{g_1(\lambda, z)}{h(\lambda, z)}, \ldots, \dfrac{g_n(\lambda, z)}{h(\lambda, z)} \right) \end{array} \qquad (\lambda \cdot \mu) \star z = \lambda \star (\mu \star z)$$

Orbit of $z \in \mathcal{Z}$

$$\mathcal{O}_z = \{\lambda \star z \mid \lambda \in \mathcal{G}\}$$

$$h, g_1, \ldots, g_n \in \mathbb{K}[\lambda_1, \ldots, \lambda_l, z_1, \ldots, z_n]$$

$\mathcal{G}$	$\mathbb{K}^*$	$\mathbb{K} \times \{-1, 1\}$	$SO(2)$
G	$(\lambda_1 \lambda_2 - 1)$	$(\lambda_2^2 - 1)$	$(\lambda_1^2 + \lambda_2^2 - 1)$
$\lambda \star z$	$\begin{pmatrix} \lambda_1 z_1 \\ \lambda_1 z_2 \end{pmatrix}$	$\begin{pmatrix} z_1 + \lambda_1 \\ \lambda_2 z_2 \end{pmatrix}$	$\begin{pmatrix} \lambda_1 & -\lambda_2 \\ \lambda_2 & \lambda_1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$
	scaling	translation+reflection	rotation

scaling $\qquad$ translation+reflection $\qquad$ rotation

Field of Rational Invariants $\mathbb{K}(z)^G$

Rational invariant: $\frac{p}{q} \in \mathbb{K}(z)$ $\qquad \frac{p(\lambda \star z)}{q(\lambda \star z)} = \frac{p(z)}{q(z)} \mod G$

Field of rational invariants: $\mathbb{K}(z)^G$

$\mathcal{G}$	$\mathbb{K}^*$	$\mathbb{K} \times \{-1, 1\}$	$SO(2)$
$\mathbb{K}(z)^G$	$\mathbb{K}\left(\frac{z_1}{z_2}\right)$	$\mathbb{K}\left(z_2^2\right)$	$\mathbb{K}\left(z_1^2 + z_2^2\right)$

1.2 Results

Rational Invariants

ALGORITHM

In : $G, \quad (g_1(\lambda, z), \ldots, g_n(\lambda, z), h(\lambda, z)) \in \mathbb{K}[\lambda, z]$

Out : $\{r_1, \ldots, r_\kappa\} \subset \mathbb{K}(z)^G$

$$\longrightarrow_Q : \begin{array}{ccc} \mathbb{K}(z)^G & \to & \mathbb{K}(y_1, \ldots, y_\kappa) \\ r & \mapsto & R \end{array} \qquad r = R(r_1, \ldots, r_\kappa)$$

So : $\mathbb{K}(z)^G = \mathbb{K}(r_1, \ldots, r_\kappa)$

Tool: Gröbner bases

Prop: the field of definition of the ideal is given by its coefficients.

I : unmixed dimensional ideal of dimension s

II : cut down to a zero dimensional ideal

Code: `www.inria.fr/cafe/Evelyne.Hubert/aida`

Algebraic invariants

OP: Describe the quotient: $\mathcal{Q}$ s.t. $\mathbb{K}(z)^G = \mathbb{K}(\mathcal{Q})$.

What are the relationships on $\{r_1, \ldots, r_\kappa\}$?

But: For a generic $\mathcal{P}$ of codimension s $\qquad$ $\mathcal{P}$ a cross-section

$$\mathbb{K}(z)^G \hookrightarrow \mathbb{K}(\mathcal{P}) \hookrightarrow \overline{\mathbb{K}(z)}^G$$

$\mathbb{K}[z]_{\mathcal{P}} \to \mathbb{K}(\mathcal{P})$ $\qquad$ $\mathbb{K}(\mathcal{P}) \cong \mathbb{K}(\xi)$

$\xi = (\xi_1, \ldots, \xi_n), \quad \xi_i \in \overline{\mathbb{K}(z)}^G$

is a zero of a computable ideal.

With: $r(z_1, \ldots, z_n) = r(\xi_1, \ldots, \xi_n) \quad \forall r \in \mathbb{K}(z)^G$

2 Intermezzo

2.1 Equivalence

Separation of orbits

$$g: \begin{array}{ccc} \mathcal{G}\times\mathcal{Z} & \to & \mathcal{Z} \\ (\lambda, z) & \mapsto & \lambda\star z \end{array} \qquad \mathbb{K}(z)^G = \mathbb{K}(r_1,\ldots,r_\kappa)$$

For $z, z' \in \mathcal{Z}\setminus\mathcal{W}$

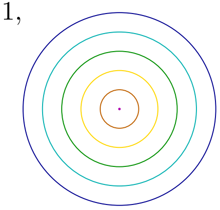
$$\exists\lambda\; z = \lambda\star z' \quad\Leftrightarrow\quad r_1(z) = r_1(z'),\,\ldots,\, r_\kappa(z) = r_\kappa(z')$$

Separation of orbits

$O(2)$ $\qquad \alpha^2+\beta^2 = 1,$

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\mathbb{K}(x,y)^G = \mathbb{K}(x^2+y^2)$$

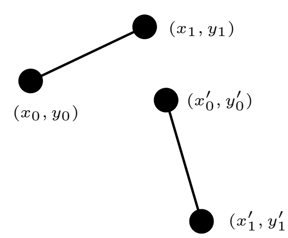


Equivalence of bi-points

$E(2)$ $\qquad \alpha^2+\beta^2 = 1,\ \epsilon^2 = 1$

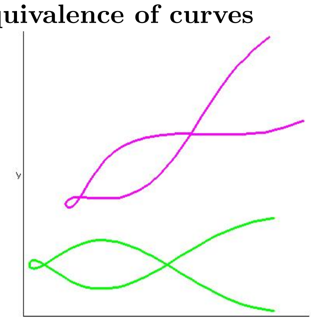
$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha & -\beta \\ \epsilon\beta & \epsilon\alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\mathbb{K}(x,y)^G = \mathbb{K}$$



$$\mathbb{K}(x_0,y_0,x_1,y_1)^G = \mathbb{K}\left((x_1-x_0)^2 + (y_1-y_0)^2\right)$$

Equivalence of curves



$E(2)$ $\qquad\qquad$ $\alpha^2+\beta^2=1,\ \epsilon^2=1$

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha & -\beta \\ \epsilon\beta & \epsilon\alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$$

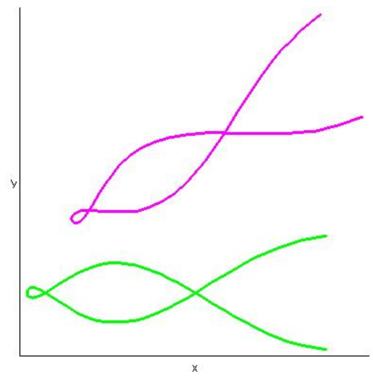
$$Y_X = \epsilon\frac{\beta+\alpha y_x}{\alpha-\beta\, y} \quad Y_{XX} = \epsilon\frac{y_{xx}}{(\alpha-\beta\, y)^3}$$

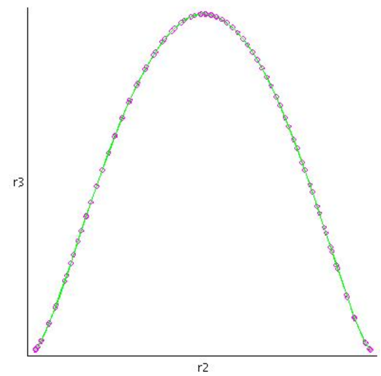
$$\mathbb{K}(x,y,y_x,y_{xx})^G = \mathbb{K}\left(\frac{y_{xx}^2}{(1+y_x^2)^3}\right)$$

Curvature: $\sigma = \sqrt{\frac{y_{xx}^2}{(1+y_x^2)^3}}$

$\rightsquigarrow$ rational actions & algebraic invariants

Signature curve





2.2 Symmetry Reduction

Symmetry reduction

- Symmetric problem = invariant under a group action

  A group element maps a solution to a solution.

- General philosophy 1: a problem that is symmetric can be written in terms of the invariants of the group action.

  Polynomial systems, dynamical systems [Gatermann]

- General Philosophy 2: project the problem on the cross-section

  Differential systems [Mansfield 01]

3 Construction and rewriting of rational invariants

3.1 Graph ideal $\rightsquigarrow$ Rosenlicht (1956),..

Graph of the action & its ideal O

- Graph of the action

$$\mathcal{O} = \{(z,z') \in \mathcal{Z}\times\mathcal{Z} \mid \exists\lambda\in\mathcal{G} \text{ s.t. } z' = \lambda\star z\}$$

- Its ideal: $O = (G + (Z - \lambda \star z)) \cap \mathbb{K}[z, Z]$

$Z = (Z_1, \ldots, Z_n)$ new set of variables

$(Z - \lambda \star z) = (h Z_i - g_i \mid 1 \leq i \leq n) : h^\infty$

- O^e the extension of O to $\mathbb{K}(z)[Z]$.
  $\rightsquigarrow$ the ideal of a generic orbit

Construction of rational invariants

Invariance: $(z, z') \in \mathcal{O} \Rightarrow (\lambda \star z, z') \in \mathcal{O}$

Thm: The reduced Gröbner basis of O^e is contained in $\mathbb{K}(z)^G[Z]$.

Examples

$\mathcal{G}$	$\mathbb{K}^*$	$\mathbb{K} \times \{-1, 1\}$	$SO(2)$

Q	$Z_2 - \frac{z_2}{z_1} Z_1$	$Z_2^2 - z_2^2$	$Z_2^2 + Z_1^2 - (z_1^2 + z_2^2)$

Rewriting & Generation

Q reduced Gröbner basis of O^e

$\{r_1, \ldots, r_\kappa\}$ the coefficients of Q

Theorem:

$$\mathbb{K}(z)^G = \mathbb{K}(r_1, \ldots, r_\kappa)$$

¡2-¿
Rewriting $\frac{p}{q} \in \mathbb{K}(z)^G$

- $y_1, \ldots, y_\kappa$ a new indeterminates

- $Q_y := Q(r_i \leftarrow y_i)$

- $p(Z) \longrightarrow^*_{Q_y} \sum_\alpha a_\alpha(y) Z^\alpha$

- $q(Z) \longrightarrow^*_{Q_y} \sum_\alpha b_\alpha(y)\, Z^\alpha$

- $\dfrac{p(z)}{q(z)} = \dfrac{a_\alpha(r)}{b_\alpha(r)}$

Example of rewriting for the scaling

$$Q = \{Z_2 - \frac{z_2}{z_1} Z_1\} \qquad r = \frac{z_2}{z_1} \qquad Q_y = \{Z_2 - y Z_1\}$$

$$\frac{p}{q} = \frac{z_1^2 + 4z_1z_2 + z_2^2}{z_1^2 - 3z_2^2}$$

$$p(Z) = Z_1^2 + 4Z_1Z_2 + Z_2^2 \quad \longrightarrow_{Q_y} \quad (y^2+4y+1)Z_2^2$$

$$q(Z) = Z_1^2 - 3Z_2^2 \quad \longrightarrow_{Q_y} \quad (y^2-3)Z_2^2$$

$$q(z)p(Z) \equiv p(z)q(Z) \bmod O^e \;\Rightarrow\; q(z)(r^2-3)Z_2^2 = p(z)(r^2+4r+1)Z_2^2$$

$$\frac{z_1^2 + 4z_1z_2 + z_2^2}{z_1^2 - 3z_2^2} = \frac{r^2+4r+1}{r^2-3} \text{ where } r = \frac{z_1}{z_2}$$

Previously

Müller-Quade & Beth 99 • Case of linear group actions.

- Proof: $(Q) = (Z - z) \cap \mathbb{K}(z)^G[Z]$

Vinberg & Popov 89 • There exists a generating set Q of O^e the coefficients $\{r_1, \ldots, r_\kappa\}$ of which are in $\mathbb{K}(z)^G$

- $\{r_1, \ldots, r_\kappa\}$ separate orbits
- A set of rational invariant that separate orbits is a generating set for $\mathbb{K}(z)^G$

Rosenlicht 56 • The coefficients of the Chow form of O^e are rational invariants and separate orbits

- A set of rational invariant that separate orbits is a generating set for $\mathbb{K}(z)^G$

3.2 Graph-section ideal $\rightsquigarrow$ Fels & Olver (1999)

Cross-section of degree d

A variety $\mathcal{P}$ that intersects generic orbits in d simple points.

$$O^e = (G + (Z - \lambda \star z)) \cap \mathbb{K}(z)[Z].$$

$$s = \text{dimension of } O^e = \text{dimension of generic orbits}$$

The ideal P defines a cross-section $\mathcal{P}$ of degree d:

- $P \subset \mathbb{K}[Z]$ prime ideal of codimension s
- $I^e = O^e + P$ radical and zero-dimensional
- $\dim_{\mathbb{K}(z)} \mathbb{K}(z)[Z]/I^e = d$

$$P = (a_{i1}Z_1 + \ldots + a_{in}Z_n - b_i,\ 1 \leq i \leq s)$$

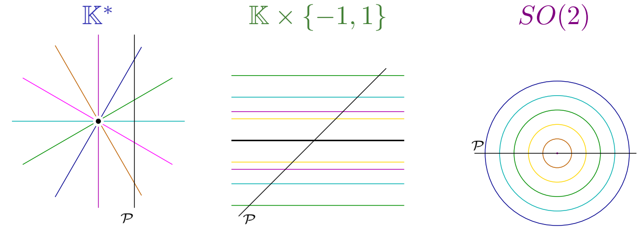
Rational Invariants 2

$$I^e = P + O^e = (\ P + G + (Z - \lambda \star z)\ )\ \cap\ \mathbb{K}(z)[Z]$$

Q a reduced Gröbner basis of I^e $\{r_1, \ldots, r_\kappa\}$ its coefficients

Theorem: $\mathbb{K}(z)^G = \mathbb{K}(r_1, \ldots, r_\kappa)$ + rewriting

$\mathcal{G}$	$\mathbb{K}^*$	$\mathbb{K} \times \{-1, 1\}$	$SO(2)$



Q	$Z_1 - 1,\ Z_2 - \frac{z_2}{z_1}$	$Z_1 - Z_2,\ Z_2^2 - z_2^2$	$Z_2,\ Z_1^2 - (z_1^2 + z_2^2)$

4 Algebraic Moving frame

4.1 Algebraic Replacement invariants

Replacement Invariant ξ

- $\mathcal{P}$ a cross-section of degree $d = 1$ $\mathbb{K}(z)^G = \mathbb{K}(\mathcal{P})$

  $I^e = (\,Z_1 - r_1(z), \ldots, Z_n - r_n(z))$

  $$r(z_1, \ldots, z_n) = r(r_1, \ldots, r_n) \qquad \forall r \in \mathbb{K}(z)^G$$

  Syzygies: P is the ideal of relations on $(r_1, \ldots, r_n)$:

  $$\mathbb{K}(z)^G = \mathbb{K}(\mathcal{P})$$

- $\mathcal{P}$ a cross-section of degree $d > 1$
  $I^G = I^e \cap \mathbb{K}(z)^G[Z] = (Q)$ has d distinct $\overline{\mathbb{K}(z)}^G$-zeros

Thm: $\xi = (\xi_1, \ldots, \xi_n)$ a $\overline{\mathbb{K}(z)}^G$-zero of I^G. $\forall r \in \mathbb{K}(z)^G$, $r(z) = r(\xi)$

$$\mathbb{K}(z)^G\ \subset\ \mathbb{K}(\xi)\mathbb{K}(\xi)\ \cong\ \mathbb{K}(\mathcal{P})\ \subset\ \overline{\mathbb{K}(z)}^G$$

$\mathbb{K}(\mathcal{P})$ is an algebraic extension of $\mathbb{K}(z)^G$ of degree d.

Replacement Invariant ξ. Examples

$\mathcal{P}$ a cross-section of degree d

$I^G = I^e \cap \mathbb{K}(z)^G[Z] = (Q)$ has d distinct $\overline{\mathbb{K}(z)}^G$-zeros

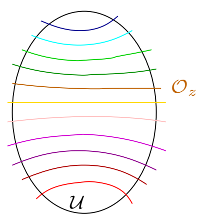
Thm: $\xi = (\xi_1, \ldots, \xi_n)$ a $\overline{\mathbb{K}(z)}^G$-zero of I^G. $r(z) = r(\xi),\ r \in \mathbb{K}(z)^G$

$\mathcal{G}$	$\mathbb{K}^*$	$\mathbb{K} \times \{-1, 1\}$	$SO(2)$
Q	$Z_1 - 1,\ Z_2 - \frac{z_2}{z_1}$	$Z_1 - Z_2,\ Z_2^2 - z_2^2$	$Z_2,\ Z_1^2 - (z_1^2 + z_2^2)$
ξ	$(1,\ \frac{z_2}{z_1})$	$(\pm z_2,\ \pm z_2)$	$\left(\pm\sqrt{z_1^2 + z_2^2},\ 0\right)$

4.2 Cartan Normalized invariants

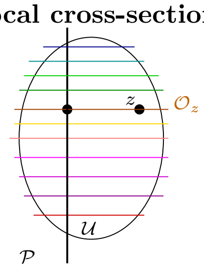
Locally

$\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$



$f : \mathcal{U} \to \mathbb{K}$ smooth/analytic is a local invariant if $f(\lambda \star z) = f(z)$ for λ close to identity.

Local cross-section



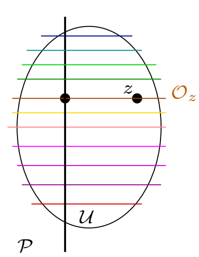
- $\mathcal{P}$ intersect $\mathcal{O}_z^0$ at a unique point, $\forall z \in \mathcal{U}$.
- $\mathcal{P}$ is transverse to $\mathcal{O}_z^0$ at $z \in \mathcal{P}$.

A local invariant is uniquely determined by a function on $\mathcal{P}$.

Local invariants $\cong$ smooth functions on the cross-section.

Invariantization $\bar{\iota} f$ of a smooth function f

$f : \mathcal{U} \to \mathbb{R}$ smooth



$\bar{\iota} f$ is the unique *local* invariant with $\bar{\iota} f|_{\mathcal{P}} = f|_{\mathcal{P}}$

$$\bar{\iota} f(z) = f\left(\mathcal{O}_z^0 \cap \mathcal{P}\right)$$

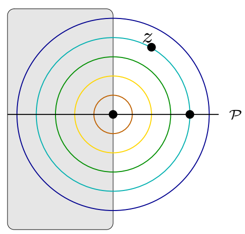
Cartan's normalized invariants: $\bar{\iota}z_1, \ldots, \bar{\iota}z_n$

Prop: f local invariant $\Rightarrow$ $f(z_1, \ldots, z_n) = f(\bar{\iota}z_1, \ldots, \bar{\iota}z_n)$

$\{\bar{\iota}z_1, \ldots, \bar{\iota}z_n\}$ generate local invariants, functionally.

Cartan's normalized invariants. Example.

$\mathcal{G} = SO(2)$, $\mathcal{U} = \{(z_1, z_2) \in \mathbb{R}^2 \mid z_1 > 0\}$



$\mathcal{P} : z_2 = 0$

$$(\bar{\iota}z_1, \bar{\iota}z_2) = \left(\sqrt{z_1^2 + z_2^2}, 0\right)$$

Replacement property:

$$f(z_1, z_2) \text{ local invariant } \Rightarrow f(z_1, z_2) = f\left(\sqrt{z_1^2 + z_2^2}, 0\right).$$

Invariants: algebraic $\sim$ local

Algebraic replacement invariant : $\overline{\mathbb{K}(z)}^G$-zero of I^e

Thm: The normalized invariants $(\bar{\iota}z_1, \ldots, \bar{\iota}z_n)$ form the smooth zero of I^e that agrees with the coordinate functions on $\mathcal{P} \cap \mathcal{U}$.

$\rightsquigarrow$ one replacement invariant is a local invariant

$\rightsquigarrow$ its components generate, functionally, the local invariants.

Merci.

Thanks.