Abstract: We provide an algebraic formulation of the moving frame method for constructing local smooth invariants on a manifold under an action of a Lie group. This formulation gives rise to algorithms for constructing rational and replacement invariants. The latter are algebraic over the field of rational invariants and play a role analogous to Cartan’s normalized invariants in the smooth theory. The algebraic algorithms can be used for computing fundamental sets of differential invariants.
<table>
<thead>
<tr>
<th>Smooth construction</th>
<th>Algebraic construction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consider</strong></td>
<td><strong>Alg. grp.</strong> $G \curvearrowright \mathcal{Z} \subset \mathbb{K}^n$ affine variety rational action</td>
</tr>
<tr>
<td>Lie grp. $G \curvearrowright M$ smooth manifold over $\mathbb{R}$ smooth, local, semi-regular action</td>
<td>$\mathbb{K}(\mathcal{Z})^G$ – rational invariants</td>
</tr>
<tr>
<td>$\mathcal{F}(M)^G$-smooth invariants</td>
<td></td>
</tr>
<tr>
<td><strong>Construct</strong></td>
<td></td>
</tr>
<tr>
<td>local cross-section to the orbits</td>
<td>graph-section</td>
</tr>
<tr>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
</tr>
<tr>
<td>moving frame map $\rho : M \to G$</td>
<td>reduced Gröbner basis</td>
</tr>
<tr>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
</tr>
<tr>
<td>fundamental set for $\mathcal{F}(M)^G$</td>
<td>finite generating set for $\mathbb{K}(\mathcal{Z})^G$</td>
</tr>
<tr>
<td>normalized inv. with replacement property</td>
<td>replacement inv. that are $\mathbb{K}(\mathcal{Z})^G$-tuples</td>
</tr>
<tr>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
</tr>
<tr>
<td>projection $\iota : \mathcal{F}(M) \to \mathcal{F}(M)^G$</td>
<td>projection $\iota : \mathbb{K}(\mathcal{Z}) \to \overline{\mathbb{K}(\mathcal{Z})}^G$</td>
</tr>
</tbody>
</table>
Motivation

Smooth construction $\leftrightarrow$ Algebraic construction

- $\rightarrow$ new approaches for computation and study of algebraic invariants.
- $\leftarrow$ computational methods for analyzing the structure of differential algebra of invariants.

Some Applications

- Symmetry reductions of differential and algebraic equations
- Equivalence problems (e.g. computer image recognition)
Smooth construction: \( \mathcal{G} \) is a Lie group, \( M \) is a smooth manifold.

Local action \( \mathcal{G} \ltimes M \) is a smooth map \( g : \Omega \to M \), where \( \Omega \supset \{e\} \times M \) is open in \( \mathcal{G} \times M \) s.t.

(i) \( g(e, \bar{z}) = \bar{z}, \forall \bar{z} \in M \)

(ii) \( g(\bar{\mu}, g(\bar{\lambda}, \bar{z})) = g(\bar{\mu} \bar{\lambda}, \bar{z}) \), for all \( \bar{z} \in M \) and \( \bar{\lambda}, \bar{\mu} \in \mathcal{G} \) s.t. \((\bar{\lambda}, \bar{z}) \) and \((\bar{\mu} \cdot \bar{\lambda}, \bar{z}) \) are in \( \Omega \).

( Notation: \( g(\bar{\lambda}, \bar{z}) = \bar{\lambda} \cdot \bar{z} \) )

Local smooth invariants: \( f \in \mathcal{F}(\mathcal{U}) \), where \( \mathcal{U} \subset M \) is an open subset, s.t. \( f(g(\bar{\lambda}, \bar{z})) = f(\bar{z}), \forall (\bar{\lambda}, \bar{z}) \) in an open subset of \( \Omega \) containing \( e \times \mathcal{U} \).

Infinitesimal criterion: \( \mathbf{v}(f)(\bar{z}) = 0 \) \( \forall \bar{z} \in \mathcal{U}, \forall \) infinitesimal generators \( \mathbf{v} \) of \( \mathcal{G} \ltimes M \).

( \( \mathcal{G} \) connected, \( \mathbf{v}(f)(\bar{z}) = 0, \forall \bar{z} \in M \Rightarrow f \) is global invariant )
Smooth construction:
Local cross-section $\mathcal{K}$ on $\mathcal{U} \subset M$ is a submanifold, s. t.

- $T_{\bar{z}}\mathcal{K} \oplus T|_{\bar{z}}\mathcal{O}_{\bar{z}} = T|_{\bar{z}}M$, $\forall \bar{z} \in \mathcal{K}$ (transversality condition)

- $\mathcal{K}$ intersects each connected component of $\mathcal{O}_{\bar{z}} \cap \mathcal{U}$ at the unique point.

$\mathcal{G} \curvearrowright M$ semi. reg. (i.e. $\exists s, \forall \bar{z} \in M \text{ dim } \mathcal{O}_{\bar{z}} = s$) $\xrightarrow{\text{Frobenius Thm.}}$ $\forall \bar{z} \in M \exists \mathcal{K} \ni \bar{z}$.

Moving frame map (Fels, Olver (1999)) defined by $\rho(\bar{z}) \cdot \bar{z} \in \mathcal{K}$

$\mathcal{G} \curvearrowright M$ free $\Rightarrow$ $\rho$ is smooth, $\mathcal{G}$-equivariant:

$\rho(\bar{\lambda} \cdot \bar{z}) \cdot (\bar{\lambda} \cdot \bar{z}) = \rho(\bar{z}) \cdot \bar{z}$ $\xrightarrow{\text{freeness}}$ $\rho(\bar{\lambda} \cdot \bar{z}) = \rho(\bar{z}) \cdot \bar{\lambda}^{-1}$
Smooth construction: Invariantization: $\iota: \mathcal{F}(U) \to \mathcal{F}^G(U)$

- Defined via the moving frame map $\rho$ (Fels, Olver (1999))

$$\iota f(\bar{z}) = f(\rho(\bar{z}) \cdot \bar{z})$$

$\rho$ is non-constructive – existence relies on the implicit function theorem

- Defined as restriction to a cross-section $\mathcal{K}$

$$\forall \bar{z} \in U \quad \iota f(\bar{z}) = f(\bar{z}_0), \text{ where } \bar{z}_0 = \mathcal{O}_\bar{z}^0 \cap \mathcal{K}.$$  

  i. $\mathcal{K}$ is constructive – $\forall \bar{z} \in \mathcal{Z}$ one can construct c.s. defined as a level set of $n - s$ coord. functions.

  ii. Freeness is not required.

**Theorem 1.**

- If the action is free both definitions are equivalent

- $\iota f$ is the unique smooth local invariant s.t. $\iota f|_\mathcal{K} = f|_\mathcal{K}$
Smooth construction: Normalized and fundamental invariants

**Definition.** If \( z = (z_1, \ldots, z_n) \) are coordinate functions on \( U \) then \( \iota z_1, \ldots, \iota z_n \) are called normalized invariants

**Theorem 2.**

- **Invariantization:** If \( f \in F(U) \) then \( \iota f(z_1, \ldots, z_n) = f(\iota z_1, \ldots, \iota z_n) \in F(U)^G \)

- **Replacement:** If \( f \in F(U)^G \) then \( f(z_1, \ldots, z_n) = f(\iota z_1, \ldots, \iota z_n) = \iota f(z) \).

- **Fundamental set:** Let \( \dim \mathcal{O}_z = s, \forall z \in U \), then \( \{\iota z_1, \ldots, \iota z_n\} \) contains \( n - s \) functionally independent local inv., s.t. any \( f \in F(U)^G \) can be locally expressed as function of these invariants in a unique way.

7
Smooth Example 1: \[ SO(2) = \left\{ \begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix} \right\} \sim M = \mathbb{R}^2/\{(0, 0)\} \]

Action: \[ Z_1 = \cos(\phi) z_1 - \sin(\phi) z_2, \quad Z_2 = \sin(\phi) z_1 + \cos(\phi) z_2 \]

Cross-section: \[ \mathcal{K} = \{(z_1, z_2) | z_1 = 0, \; z_2 > 0\} \Rightarrow \]

Moving frame map is defined by \[ Z_1 = 0 \]

i.e. \[ \rho(z) = \begin{pmatrix} \frac{z_2}{\sqrt{z_1^2 + z_2^2}} & -\frac{z_1}{\sqrt{z_1^2 + z_2^2}} \\ \frac{z_1}{\sqrt{z_1^2 + z_2^2}} & \frac{z_2}{\sqrt{z_1^2 + z_2^2}} \end{pmatrix} \]

Invariantization: \[ f(z_1, z_2) \in \mathcal{F}(M) \rightarrow \]

\[ \iota f(z) = f(\rho(z) \cdot z) = f(0, \sqrt{z_1^2 + z_2^2}) \in \mathcal{F}^G \]

Normalized invariants: \[ \iota z_1 = 0, \quad \iota z_2 = \sqrt{z_1^2 + z_2^2} = r \text{ (fundamental invariant)} \]

Replacement property: \[ f \in \mathcal{F}(M)^G \Rightarrow f(z) = f(\iota z_1, \iota z_2) = f(0, r) \] i.e. \[ z_1^2 + z_2^2 = (\iota z_1)^2 + (\iota z_2)^2 = 0^2 + r^2 \]

Restrictions to the cross-section: \[ \iota f|_{\mathcal{K}} = f|_{\mathcal{K}} = f(0, r) \]
Smooth Example 2: $SE(2) = SO(2) \times \mathbb{R}^2 \sim$ on plane curves $y = y(x)$:

Action: $X = \cos(\phi)x - \sin(\phi)y + a, \quad Y = \sin(\phi)x + \cos(\phi)y + b$

Prolongation to derivatives up to second order:

$$Y_1 = \frac{\sin(\phi) + \cos(\phi)y_1}{\cos(\phi) - \sin(\phi)y_1}, \quad Y_2 = \frac{y_2}{(\cos(\phi) - \sin(\phi)y_1)^3}$$

Cross-section: $\mathcal{K} = \{(x, y, y_1, y_2)| x = 0, y = 0, y_1 = 0, y_2 > 0\} \subset \mathbb{R}^4$

Moving frame map is defined by: $X = 0, Y = 0, Y_1 = 0 \Rightarrow$

$$\cos \phi = \frac{1}{\sqrt{y_1^2 + 1}}, \quad \sin \phi = -\frac{y_1}{\sqrt{1+y_1^2}}, \quad a = -\frac{x+y_1y}{\sqrt{1+y_1^2}}, \quad b = \frac{y_1x-y}{\sqrt{1+y_1^2}}.$$

Normalized invariants: $\iota x = 0, \iota y = 0, \iota y_1 = 0,$

$\iota y_2 = \frac{y_2}{(1+y_1^2)^{3/2}}$ is curvature –differential invariant.
Algebraic construction: $\mathcal{G}$ is an alg. group, $\mathcal{Z}$ is an affine variety.

Rational action $\mathcal{G} \curvearrowright \mathcal{Z}$ is a rational map $g: \mathcal{G} \times \mathcal{Z} \to \mathcal{Z}$ s. t.

(i) $g(e, \bar{z}) = \bar{z}$, $\forall \bar{z} \in \mathcal{Z}$

(ii) $g(\bar{\mu}, g(\bar{\lambda}, \bar{z})) = g(\bar{\mu} \bar{\lambda}, \bar{z})$, $\forall \bar{\lambda}, \bar{\mu} \in \mathcal{G}$ and $\forall \bar{z} \in \mathcal{Z}$ s.t. $g(\bar{\lambda}, \bar{z})$ and $g(\bar{\mu} \bar{\lambda}, \bar{z})$ are defined.

( Notation: $g(\bar{\lambda}, \bar{z}) = \bar{\lambda} \cdot \bar{z}$ )

Rational invariants: $f \in \mathbb{K}(\mathcal{Z})$ s.t. $f(g(\bar{\lambda}, \bar{z})) = f(\bar{z})$, $\forall \bar{z} \in \mathcal{Z}$ and $\forall \bar{\lambda} \in \mathcal{G}$ s.t. $g(\bar{\lambda}, \bar{z})$ is defined.
Algebraic construction: Notation: $\overline{S}$ is Zariski closure of set $S$

Graph of the action $O = \{(\overline{z}, \overline{z}') \subset Z \times Z | \exists \overline{\lambda} \in G : \overline{z}' = \overline{\lambda} \cdot \overline{z}\} \leftrightarrow$ ideal: $O \subset K[Z \times Z]$

extension: $O^e \subset K(Z)[Z]$

Orbit: $O_{\overline{z}} = \{\overline{z}' \in Z | \exists \overline{\lambda} \in G : \overline{z}' = \overline{\lambda} \cdot \overline{z}\} \leftrightarrow$ ideal: $O_{\overline{z}} \subset K[Z]$

Cross-section of degree $d$: an irreducible subvariety $K \subset Z$ s.t. $O_{\overline{z}} \cap K$ consists of $d$ simple points $\forall \overline{z}$ in a dense subset of $Z$ (transversality condition)

$\Uparrow$

ideal: $K$ is prime, s.t. $\text{codim} K = \max_{\overline{z}} \dim O_{\overline{z}} = s$ and $I^e = O^e + K \subset K(Z)[Z]$ is radical zero-dimensional (transversality cond.)

Graph-section: $I = \{(\overline{z}, \overline{z}') \subset Z \times K | \exists \overline{\lambda} \in G : \overline{z}' = \overline{\lambda} \cdot \overline{z}\} \leftrightarrow$ ideal: $I = O + K \subset K[Z \times Z]$
Theorem 3:
Coeff. of a reduced Gröbner basis $Q$ of either $O^e$ or $I^e$ generate $\mathbb{K}(\mathcal{Z})^G$.

Ideas of the proof:

- If $(\bar{z}, \bar{z}') \in \mathcal{O} \Rightarrow (\overline{\lambda} \cdot \bar{z}, \bar{z}') \in \mathcal{O}, \forall \overline{\lambda} \in G$. Hilbert’s Nullstellensatz & uniqueness of the reduced $Q \rightarrow$ coeff. of $Q$ are in $\mathbb{K}(\mathcal{Z})^G$.
- Rewriting algorithm to express $f(z) = \frac{p(z)}{q(z)} \in \mathbb{K}(\mathcal{Z})^G$ in terms of generators by computing normal forms of $p$ and $q$ w.r.t. $Q$.

Previous work. Rosenlicht (1956): ∀ subset set of $\mathbb{K}(\mathcal{Z})^G$ that separates orbits generates $\mathbb{K}(\mathcal{Z})^G$; coeffs. of Chow form of $O^e$ have this property.
Vinberg, Popov (1989): if coeff. of a generating set of $O^e$ are in $\mathbb{K}(\mathcal{Z})^G$, then they generate $\mathbb{K}(\mathcal{Z})^G$; $\exists$ such generating set.

Contribution: Simple algorithm applicable to both $O^e$ and $I^e$. $\dim I^e = 0$ ⇒ computational advantage.
**Algebraic construction:** Replacement invariants

**Lemma.** Let $Q$ be a reduced Gröbner basis of the graph-section ideal $I^e = (O^e + K) \subset K(Z)[Z]$. Then

- $Q$ is a reduced Gröbner basis of $I^G = I^e \cap K(Z)^G[Z]$.
- $I^G \subset K(Z)^G[Z]$ is zero-dimensional and prime.
- If c.-s. $K$ has degree $d$ then $I^G$ has $d$ simple $\overline{K(Z)^G}$-zeros $\xi^{(i)} : [\overline{K(Z)^G}]^n \to Z$, $i = 1..d$, (called replacement invariants associated with $K$.)

**Theorem 4.** Let $\xi^{(i)}$, $i = 1..d$, be replacement invariants associated with $K$ of degree $d$. Then

- $f(z) \in K(Z)^G \Rightarrow f(z) = f(\xi^{(i)})$ for $i = 1..d$. (replacement)
- $K(K) \cong K(\xi^{(i)})$, $i = 1..d$ is the extension of degree $d$ of $K(Z)^G$.
- $\iota_i : K[Z]_K \to \overline{K(Z)^G} : \iota_i f = f(\xi^{(j)})$ for $j = 1..d$ is computable projection (invariantization)

**Corollary.** If $d = 1$ there is a unique rational replacement invariant $\xi : [K(Z)^G]^n \to Z$, that provides a generating set of $K(Z)^G$ (cf. Vinberg, Popov (1989)):

$$K(Z)^G \cong K(\xi) \cong K(K)$$
Algebraic Example 1: (rotation) $SO(2) \sim \mathbb{K}^2$

Group ideal: $G = (\lambda_1^2 + \lambda_2^2 - 1) \subset \mathbb{K}[\lambda_1, \lambda_2]$

Action ideal: $J = (Z_1 - (\lambda_1 z_1 - \lambda_2 z_2), Z_2 - (\lambda_2 z_1 + \lambda_1 z_2)) + G$

Graph ideal: $O = J \cap K[\mathcal{Z} \times \mathcal{Z}]$

$Q = \{Z_1^2 + Z_2^2 - (z_1^2 + z_2^2)\}$ is rGB for $O$ and $O^e$.

Cross-section ideal (of degree 2):

$K = (Z_1)$

Graph-section ideal: $I = O + K$

$Q = \{Z_1, Z_2^2 - (z_1^2 + z_2^2)\}$ is rGB for $I$ and $I^e$

Replacement invariants: are $\mathbb{K}(\mathcal{Z})^G$ roots of $I^e$: $(\xi_{1}^{\pm}, \xi_{2}^{\pm}) = (0, \pm r)$

Replacement property:

$f \in \mathbb{K}(\mathcal{Z})^G \Rightarrow f(z) = f(\xi^{\pm})$ i.e. $z_1^2 + z_2^2 = (\xi_1^{\pm})^2 + (\xi_2^{\pm})^2$
Algebraic Example 2: $SE(2) \looparrowright$ plane curves.

Notation: $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4)$, $z = (x, y, y_1, y_2)$, $Z = (X, Y, Y_1, Y_2)$

Group ideal: $G = (\lambda_1^2 + \lambda_2^2 - 1) \subseteq \mathbb{K}[\lambda]$

Action ideal:

$$J = \left( X - (\lambda_1 x - \lambda_2 y + \lambda_3), Y - (\lambda_2 x + \lambda_1 y + \lambda_4),
Y_1 - \frac{\lambda_2 + \lambda_1 y_1}{\lambda_1 - \lambda_2 y_1}, Y_2 - \frac{y_2}{(\lambda_1 - \lambda_2 y_1)^3} \right) + G \subseteq (\lambda_1 - \lambda_2 y_1)^{-1}\mathbb{K}[\lambda, z, Z]$$

Cross-section ideal: $K = (X, Y, Y_1)$

Graph-section ideal: $I^e = \left( X, Y, Y_1, Y_2^2 - \frac{y_2^2}{(1+y_1^2)^3} \right)$ is generated by rGB of ideal $I = (J + K) \cap \mathbb{K}[z, Z]$, $I^e \in \mathbb{K}(z)[Z]$ and $I^G \in \mathbb{K}(Z)^G[Z]$

Replacement Invariants: $\overline{\mathbb{K}(Z)^G}$-roots if $I^e$: $\xi^\pm_1 = (0, 0, 0, \pm \kappa)$, where $\kappa = \frac{y_2}{(1+y_1^2)^{3/2}}$ is curvature.