Algebraic and Differential Invariants

Evelyne Hubert
INRIA Méditérranée, Sophia Antipolis, France

Published in
Foundations of Computational Mathematics, Budapest 2011,
London Mathematical Society Lecture Note Series (403),
Cambridge University Press.

Abstract

This article highlights a coherent series of algorithmic tools to compute and work with algebraic and differential invariants.

Introduction

Group actions are ubiquitous in mathematics and arise in diverse fields of science and engineering, including physics, mechanics, and computer vision. Invariants of these group actions typically arise to reduce a problem or to decide if two objects, geometric or abstract, are obtained from one another by the action of a group element. [8, 9, 10, 11, 13, 15, 17, 39, 40, 42, 43, 45, 46, 52, 59] are a few recent references of applications. Both algebraic and differential invariant theories have become in recent years the subject of computational mathematics [13, 14, 17, 40, 60]. Algebraic invariant theory studies polynomial or rational invariants of algebraic group actions [18, 22, 23, 54]. A typical example is the discriminant of a quadratic binary form as an invariant of an action of the special linear group. The differential invariants appearing in differential geometry are smooth functions on a jet bundle that are invariant under a prolonged action of a Lie group [4, 16, 34, 48, 53]. A typical example is the curvature of a plane curve, invariant under the action of the group of the isometries on the plane. Curvature is not a rational function, but an algebraic function. Concomitantly the classical Lie groups are linear algebraic groups.

This article reviews results of [14, 28, 29, 30, 31, 32] in order to show their coherence in addressing algorithmically an algebraic description of the differential invariants of a group action. In the first section we show how to compute the rational invariants of a group action and give concrete expressions to a set of algebraic invariants that are of fundamental importance in the differential context. The second section addresses the question of finite representation of differential invariants with invariant derivations, a set of generating differential invariants and the differential relationships among them. In the last section we

describe the algebraic structure that better serves the representation of differential invariants.

1 Algebraic invariants

This section offers a geometric description and the algebraic computation of the invariants of a group action. In the first subsection we provide the geometric description of *normalized invariants* of a Lie group action. This description, based solely on the concept of cross-section, is directly drawn from [32] and is an alternative to the moving frame based description of [14, 40]. In the second subsection we provide an algorithm to compute a generating set of rational invariants for the rational action of an algebraic group. This is a quick presentation of the main results of [31]. In the last subsection we explain how the algorithm also delivers the normalized invariants as algebraic invariants. The details are to be found in [32].

The algorithm to compute rational invariants relies on Gröbner bases. This is a founding stone in algebraic computing. Introduced inthe mid 60s they have been the subject of intensive research and now textbooks [1, 3, 12, 20, 37]. They are implemented in most computer algebra systems. Among their many applications, they algorithmically compute the elimination ideals that appear in the algorithmic construction of a generating set of rational invariants.

1.1 A geometric vision

We consider a Lie group $\mathcal{G}$, with identity denoted by e and dimension r, and a smooth manifold $\mathcal{Z}$ of dimension n. An action of $\mathcal{G}$ on $\mathcal{Z}$ is given by a smooth map $\mathcal{G} \times \mathcal{Z} \to \mathcal{Z}$. The image of a pair (λ, z) is denoted $\lambda \star z$. If $\lambda \cdot \mu$ denotes the product of two elements $\lambda, \mu \in \mathcal{G}$ the action satisfies $\mu \star (\lambda \star z) = (\mu \cdot \lambda) \star z$ and $e \star z = z$ for all $z \in \mathcal{Z}$. To be of practical interest, the notion of an action is often relaxed to being defined on an open subset of $\mathcal{G} \times \mathcal{Z}$ that contains $\{e\} \times \mathcal{Z}$. All the subsequent relationships are understood by restricting them to the locus where the quantities appearing are well defined.

The *orbit* $\mathcal{O}_z$ of a point $z \in \mathcal{Z}$ is the set of points that are the image of z by some $\lambda \in \mathcal{G}$: $\mathcal{O}_z = \{\lambda \star z \,|\, \lambda \in \mathcal{G}\}$. A (global) *cross-section* is an embedded submanifold $\mathcal{P}$ of $\mathcal{Z}$ that intersects each orbit of $\mathcal{Z}$ at a unique point. The *invariants* of the action are the functions that are constant on orbits: They satisfy $f(\lambda \star z) = f(z)$. If a cross-section $\mathcal{P}$ exists, one easily understands that functions on this cross-section are in one-to-one correspondence with invariants. An invariant defines a function on $\mathcal{P}$ by restriction. Conversely, each function $\bar{f} : \mathcal{P} \to \mathbb{R}$ on the cross-section defines an invariant $f : \mathcal{Z} \to \mathbb{R}$ by spreading its values along the orbits: $f(z) = \bar{f}(\bar{z})$ where $\bar{z}$ is the intersection of $\mathcal{O}_z$ with $\mathcal{P}$. Going further with this idea we are led to define the *invariantization* $\bar{\iota} f$ of a function f on $\mathcal{Z}$: $\bar{\iota} f$ is the unique invariant that agrees with f on the cross-section: $\bar{\iota} f(z) = f(\bar{z})$ where $\bar{z}$ is the intersection of $\mathcal{O}_z$ with $\mathcal{P}$. We thus retain the values of f on $\mathcal{P}$ and spread them along the orbits.

The global picture we just drew can not be put easily into practice as the existence of a global cross-section is not secured, not to mention the difficulty of identifying one, if it does exist. Yet if we accept the idea of restricting to the neighborhood of a point where the action is well-behaved, things unravel pretty nicely. Furthermore infinitesimal calculus comes into the picture to help. And indeed the faithful description of Lie group action by its infinitesimal generators has made it successful in applications [47].

The tangent space $T\mathcal{G}|_e$ can be identified with the Lie algebra $\mathfrak{g}$ of $\mathcal{G}$. To every vector $\hat{v}$ in $T\mathcal{G}|_e$ we can associate a smooth vector field v on $\mathcal{Z}$. The integral curves of this vector field are the orbits of a one-dimensional subgroup of $\mathcal{G}$. Such a vector field is called an *infinitesimal generator* and is often understood as a derivation: For a function f on $\mathcal{Z}$, $\mathrm{v}(f)$ measures the variation of f along the integral curve. If f is an invariant of the group action then $\mathrm{v}(f) = 0$.

If $\hat{v}_1, \ldots, \hat{v}_r$ is a basis for the Lie algebra of $\mathcal{G}$, then the associated infinitesimal generators $\mathrm{v}_1, \ldots, \mathrm{v}_r$ span the tangent space to the orbits at each point of $\mathcal{Z}$. The dimension of the orbit of a point z is the rank of $\mathrm{v}_1, \ldots, \mathrm{v}_r$ at z. We shall place ourselves in a neighborhood $\mathcal{U}$ of a point z where this rank is constant and equal to d. Obviously $d \leq r$, the dimension of the group. *Local invariants* are those functions f on $\mathcal{Z}$ for which $\mathrm{v}_1(f) = 0, \ldots, \mathrm{v}_r(f) = 0$ in this neighborhood.

By possibly further restricting the neighborhood $\mathcal{U}$, we can then prove the existence of a *local cross-section* $\mathcal{P}$, that is an embedded submanifold of dimension $n - d$ that intersects transversally the connected part of the orbits of $\mathcal{U}$ at a single point. This submanifold can be described as the zero set of d independent functions $(p_1, \ldots, p_d)$ on $\mathcal{U}$. The condition that those functions define a cross-section is that the rank of the $r \times d$ matrix $V(P) = (\mathrm{v}_i(p_j))_{i=1..r}^{j=1..d}$ is d on $\mathcal{P}$.

One thus sees that a lot of freedom comes into the choice of a local cross-section. In particular, if $(z_1, \ldots, z_n)$ are coordinate functions on $\mathcal{U}$ one shows that we can choose a cross-section as the level set of d of these coordinate functions as a practical choice. The invariantization process we described earlier can be applied by restriction to $\mathcal{U}$ and the invariantization of the coordinate functions $(\bar{\iota}z_1, \ldots, \bar{\iota}z_n)$ are singled out as the *normalized invariants*. They functionally generate all local invariants and the equations of the cross-section describe completely their relationships. We formalize this here as a theorem, but we refer to [32] for a precise statement.

Theorem 1.1. *Let $\mathcal{P}$ be a local cross-section on $\mathcal{U}$, given as the zero set of d independent functions $p_1, \ldots, p_d$. The normalized invariants $(\bar{\iota}z_1, \ldots, \bar{\iota}z_n)$ of the coordinate functions $(z_1, \ldots, z_n)$ satisfy:*

- $p_1(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) = 0, \ldots, p_d(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) = 0$.
- *if a function p is such that $p(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) = 0$ then there exist, around each point of the cross-section, functions $(a_1, \ldots, a_r)$ such that $p = a_1 p_1 + \ldots + a_d p_d$.*

- *if f is a local invariant then $f(z_1, \dots, z_n) = f(\bar{\iota}z_1, \dots, \bar{\iota}z_n)$.*

Example 1.2. *We consider the linear action of $SO(2)$, the group of 2×2 orthogonal matrices with determinant 1, on $\mathbb{R}^2$. The action of an element of the group is a rotation with the origin as center. The orbits are the circles centered at the origin, and the origin itself.*

The positive z_1-axis, $\mathcal{P} = \{(z_1, z_2) | z_2 = 0, z_1 > 0\}$, is a local cross-section on $\mathcal{Z}$. The invariantization of the coordinate functions are the functions $\bar{\iota}z_1$ and $\bar{\iota}z_2$ that associate to a point (z_1, z_2) the coordinates of the intersection of its orbit with the cross-section. Thus

$$\bar{\iota}z_1 : (z_1, z_2) \mapsto \sqrt{z_1^2 + z_2^2} \quad \text{and} \quad \bar{\iota}z_2 : (z_1, z_2) \mapsto 0.$$

By Theorem 1.1, all local invariants can be written in terms of $\sqrt{z_1^2 + z_2^2}$ by carrying out the substitutions $z_1 \to \sqrt{z_1^2 + z_2^2}$ and $z_2 \to 0$

The above example is specific in as much as the dimension of the orbits, outside of the origin, is equal to the dimension of the group. This case is of great importance in the differential context for which the presented geometric construction was first drawn in [14]. We can indeed then introduce the seminal notion of a moving frame. A moving frame $\rho : \mathcal{Z} \to \mathcal{G}$ is a smooth map to the group that is (right) equivariant, i.e. $\rho(\lambda \star z) = \rho(z) \cdot \lambda^{-1}$. When the dimension of the orbits is equal to the dimension of the group, a local cross-section determines a moving frame. For any point z in the neighbourhood of the cross-section we can single out an element λ of the group, close enough to the identity, such that $\lambda \star z$ belongs to the cross-section. The map that associates such a λ to a point z is a moving frame. If the cross-section is given as the zero set of the functions $p_1, \dots, p_r$ then

$$p_1(\lambda \star z) = 0, \dots, p_r(\lambda \star z) = 0$$

implicitly define this moving frame. Indeed, the transversality condition of the cross-section,

$$\det V(P) = \det \left(\mathrm{v}_i(p_j) \right)_{i=1..r}^{j=1..r} \neq 0$$

ensure then that we can apply the implicit function theorem. This actually provides another way of characterizing invariantization as indeed $\bar{\iota}f(z) = f(\rho(z) \star z)$ then.

1.2 Algorithms for rational invariants

In this section $\mathbb{K}$ is a field of characteristic zero, typically $\mathbb{Q}$, $\mathbb{R}$ or even $\mathbb{C}$, while $\bar{\mathbb{K}}$ is an algebraically closed field that contains it. We consider an r-dimensional (affine) algebraic group given as the variety, in $\mathbb{K}^l$ or $\bar{\mathbb{K}}^l$, of an ideal G in $\mathbb{K}[\lambda] = \mathbb{K}[\lambda_1, \dots, \lambda_l]$. The group operation and its inverse are defined by polynomial maps. A rational action of $\mathcal{G}$ on the affine space $\mathcal{Z} = \mathbb{K}^n$ can be given as an n-tuple of rational functions in $\mathbb{K}(\lambda_1, \dots, \lambda_l, z_1, \dots, z_n)$ provided they are well defined on $\{e\} \times \mathcal{Z} \subset \mathcal{G} \times \mathcal{Z}$.

There exists an invariant open subset $\mathcal{Z}_0 \subset \mathcal{Z}$ such that the orbits of the induced action of $\mathcal{G}$ on $\mathcal{Z}_0$ all have the same dimension, say d. This is the dimension of generic orbits. Rational invariants are the rational functions on $\mathcal{Z}$ that are constant on the orbits of the action. They form a subfield $\mathbb{K}(z)^G$ of $\mathbb{K}(z)$, which is therefore finitely generated. The transcendance degree of $\mathbb{K}(z)^G$ over $\mathbb{K}$ is then $n-d$. A generating set of rational invariants thus has at least $n-d$ elements. If there are more than that, then some are algebraically dependent on the others.

These statements, that can be found in [54], can actually be recovered in a constructive way. Assume that $\lambda \star z = \left(\frac{g_1(\lambda,z)}{h_1(\lambda,z)}, \ldots, \frac{g_n(\lambda,z)}{h_n(\lambda,z)}\right)$ where g_i, $h_i \in \mathbb{K}[\lambda, z]$. Let h be the least common multiple of the denominators $h_1, \ldots, h_n$ and introduce a second set of variables $Z_1, \ldots, Z_n$. Consider the elimination ideal $O_z = (G + (h_1\, Z_1 - g_1, \ldots, h_n\, Z_n - g_n)) : h^\infty \cap \mathbb{K}(z_1, \ldots, z_n)[Z_1, \ldots, Z_n]$, that we suggestively write as

$$O_z = (G + (Z - \lambda \star z)) \cap \mathbb{K}(z)[Z]$$

for short. The variety of O_z, for a generic $z \in \mathbb{K}^n$, is the Zariski closure of $\mathcal{O}_z$. For $\lambda \in \mathcal{G}$ and $z \in \mathcal{Z}$ we have $\mathcal{O}_z = \mathcal{O}_{\lambda\star z}$. The ideal O_z of $\mathbb{K}(z)[Z]$ is thus left unchanged when we substitute z by $\lambda \star z$. Any canonical rational representation of this ideal must thus have its coefficients in $\mathbb{K}(z)^G$. The coefficients of the Chow form of O_z were first shown to form a separating set of rational invariants, and hence a generating set [58]. In [31, 44, 35] a reduced Gröbner basis for O_z is used. Its coefficients are shown to form a generating set of rational invariants by exhibiting an algorithm to rewrite any other rational invariants in terms of those.

The distinguishing feature of [31] is to additionaly incorporate the idea of the geometric construction reviewed in the previous section. In the present context, a *cross-section of degree* e is an irreducible subvariety $\mathcal{P}$ of $\mathcal{Z}$ that intersects the generic orbits in e distinct points. If $P \subset \mathbb{K}[Z]$ is a prime ideal of codimension d, its variety $\mathcal{P}$ is a cross-section iff the ideal

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

is radical and zero-dimensional. This is equivalent to saying that the quotient $\mathbb{K}(z)[Z]/I_z$ is finite dimensional as a $\mathbb{K}(z)$-vector space. Its dimension e is then the degree of the cross-section $\mathcal{P}$ and is easily read on a Gröbner basis of I_z. As before $I_{\lambda\star z} = I_z$ and we obtain the same results as for O_z about the coefficients of a canonical representation. Let us give a precise statement [31, Theorem 2.16 and 3.7].

Theorem 1.3. *Consider $\{r_1, \ldots, r_\kappa\} \in \mathbb{K}(z)$ the coefficients of a reduced Gröbner basis Q of O_z or I_z. Then $\{r_1, \ldots, r_\kappa\}$ is a generating set of rational invariants: $\mathbb{K}(z)^G = \mathbb{K}(r_1, \ldots, r_\kappa)$. Furthermore we can rewrite any rational invariant $\frac{p}{q}$, with $p, q \in \mathbb{K}[z]$, in terms of those as follows.*

Take a new set of indeterminates $y_1, \ldots, y_\kappa$ and consider the set $Q_y \subset \mathbb{K}[y, Z]$ obtained from Q by substituting r_i by y_i. Let $a(y, Z) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha(y) Z^\alpha$

Figure 1: Left: The orbits and a cross-section of the goup of rotations (Example 1.4); Right: The orbits of the action of Example 1.5.

and $b(y,Z) = \sum_{\alpha\in\mathbb{N}^n} b_\alpha(y)Z^\alpha$ *in* $\mathbb{K}[y,Z]$ *be the reductions of* $p(Z)$ *and* $q(Z)$ *with respect to* Q_y. *There exists* $\alpha \in \mathbb{N}^n$ *such that* $b_\alpha(r) \neq 0$ *and for any such* α *we have* $\frac{p(z)}{q(z)} = \frac{a_\alpha(r)}{b_\alpha(r)}$.

The first advantage of using I_z instead of O_z is that zero dimensional ideal are more amenable when it comes to computing Gröbner bases. The second advantage that cannot be underestimated, though it does not come forth in the too simple examples we examine below, is that the output is considerably smaller: There are many less non-trivial coefficients in the Grobner basis of I_z than in that of O_z. We thus have a smaller set of generators.

Example 1.4. *We consider the group of rotation of the plane. The group is defined as the circle and given by the ideal* $G = (\lambda_1^2 + \lambda_2^2 - 1) \subset \mathbb{K}[\lambda_1, \lambda_2]$. *Its linear action on* $\mathbb{K}^2$ *is given by:*

$$\lambda \star z = (\lambda_1 z_1 - \lambda_2 z_2,\ \lambda_2 z_1 + \lambda_1 z_2)\,.$$

The reduced Gröbner basis of O_z *is* $\{Z_1^2 + Z_2^2 - r\}$, *where* $r = z_1^2 + z_2^2$. *Hence* $\mathbb{K}(z)^G = \mathbb{K}(r)$. *The variety of* $P = (Z_2)$ *is a cross-section of degree 2 since the reduced Gröbner basis of* I_z *is* $\{Z_2, Z_1^2 - r\}$.

Example 1.5. *We consider the rational action of the additive group* $\mathbb{K}$ *on* $\mathbb{K}^2$ *given by:*

$$\lambda \star z = \left(\frac{z_1}{1+\lambda z_1}, \frac{z_2}{(1+\lambda z_1)^2}\right).$$

Observe that $(\lambda + \mu) \star z = \lambda \star (\mu \star z)$ *as prescribed by the group action axioms.*

Any point on the z_2*-axis is a zero dimensional orbit whereas the generic orbits are one dimensional: They are the level sets of* $\frac{z_2}{z_1^2}$. *Concomitantly a reduced Gröbner basis of* O_z *is* $\{Z_2 - \frac{z_2}{z_1^2} Z_1^2\}$. *A generic line is a cross-section of degree 2. Yet the variety of* $P = (Z_1 - 1)$ *is a cross-section of degree* 1*: The Gröbner basis of* I_z *is* $\{Z_1 - 1, Z_2 - \frac{z_2}{z_1^2}\}$. *The rewriting described in Theorem 1.3 is then a simple replacement:* $z_1 \mapsto 1$, $z_2 \mapsto r$, *where* $r = \frac{z_2}{z_1^2}$.

1.3 Replacement invariants

Cross-sections of degree 1 are of particular interest. The reduced Gröbner basis of the ideal I_z is then $\{Z_1 - r_1, \ldots, Z_n - r_n\}$, for some $r_i \in \mathbb{K}(z)^G$. This was the case in Example 1.5. The rewriting of Theorem 1.3 is then a simple *replacement* of z_i by r_i: If R belongs to $\mathbb{K}(z)^G$ then $R(z_1, \ldots, z_n) = R(r_1(z), \ldots, r_n(z))$. Furthermore we know all the relationships on those invariants: A polynomial p that satisfies $p(r_1, \ldots, r_n) = 0$ belongs to P, the ideal of the cross-section.

This idea of a n-tuple of *replacement invariants* can be generalized for a cross-section of any degree if we allow algebraic invariants, i.e. algebraic functions of rational invariants. The reduced Gröbner basis of the ideal I_z considered in $\mathbb{K}(z)[Z]$ is also a reduced Gröbner basis of this ideal considered in $\mathbb{K}(z)^G[Z]$. If we have a section of degree e, the ideal I_z has e zeros in $\left(\overline{\mathbb{K}(z)}^G\right)^n$. Any such root $\xi = (\xi_1, \ldots, \xi_n)$ satisfies $r(z) = r(\xi)$ when $r \in \mathbb{K}(z)^G$. Furthermore if p is a polynomial such that $p(\xi_1, \cdots, \xi_n) = 0$ then $p \in P$, the ideal of the cross-section.

This fact is of course reminiscent of the property of the normalized invariants that appeared in the geometric construction of Section 1.1. And indeed, normalized invariants, as defined in the neighborhood of a point on the cross-section where the action is well behaved, are zeros of I_z. This is illustrated by the case of rotations in Example 1.2 and then 1.4. It explains why normalized invariants end up being algebraic functions. Proper mathematical statements and further developements are to be found in [32].

The point we are making here is twofold. First, for rational actions of algebraic groups, which cover many a situation, we have an algorithm to represent normalized invariants as algebraic functions. Second, we can work formally with normalized invariants as variables, as long as we subject them to the relationships defining the cross-section.

2 Differential Invariants

The better known differential invariant is the curvature of a plane curve. It is an invariant for the Euclidean group, which consists of rotations and translations. If the curve is given as the graph $(x, u(x))$ of a smooth function $u : \mathbb{R} \to \mathbb{R}$, the curvature is $\sigma(x) = \sqrt{\frac{u_{xx}^2}{(1+u_x^2)^3}}$. It is an algebraic function of the derivatives of u. All other differential invariants can be obtained by differentiating the curvature with respect to arc length. This is an *invariant derivation* that can also be written explicitly in terms of the jet coordinates: $\mathcal{D} = (1 + u_x^2)^{-\frac{1}{2}} \dfrac{d}{dx}$.

If we now look at surfaces in $\mathbb{R}^3$ given as the graphs of a function $(x, y, u(x, y))$, two differential invariants come into play: Either the mean and Gauss curvatures or the principal curvatures. These pairs are not differentially independent of each other. Their derivatives, according to some invariant derivations, satisfy the Codazzi equation. Such a relationship is a *syzygy*.

In this section we describe algorithmic means to pinpoint invariant derivations, a generating set of differential invariants and their syzygies for a group action known solely by its infinitesimal generators. The content draws on [14, 29, 30].

2.1 Prolongations and invariant derivations

We consider a manifold $\mathcal{X} \times \mathcal{U}$, where $\mathcal{X}$ and $\mathcal{U}$ are open subsets of $\mathbb{R}^m$ and $\mathbb{R}^n$, with respective coordinates $x = (x_1, \ldots, x_m)$ and $u = (u_1, \ldots, u_n)$. We are intrinsically looking locally at submanifolds of dimension m in an $m + n$ manifold: The submanifolds are given as the graphs of maps $u : \mathbb{R}^m \to \mathbb{R}^{m+n}$. For $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$, u_α stands for $\frac{\partial^{|\alpha|} u}{\partial\, x^\alpha} = \frac{\partial^{|\alpha|} u}{\partial x_1^{\alpha_1} \ldots \partial x_m^{\alpha_m}}$.

We discuss briefly the prolongation of an action on $\mathcal{X} \times \mathcal{U}$ to its jet space, in a simple coordinatized way. The coordinates for the k-th order jet space,noted $\mathrm{J}^k(\mathcal{X},\mathcal{U})$ or J^k for short, consist of x, u and u_α where $|\alpha| = \alpha_1 + \cdots + \alpha_m \leq k$. The functions on the infinite jet space J are subject to the *total derivations* $\mathrm{D}_1, \ldots, \mathrm{D}_m$ usually written

$$\mathrm{D}_i = \frac{\partial}{\partial x_i} + \sum_{u \in \mathcal{U},\, \alpha \in \mathbb{N}^m} u_{\alpha+\epsilon_i} \frac{\partial}{\partial u_\alpha}, \text{ for } 1 \leq i \leq m, \tag{1}$$

where ϵ_i stands for the m-tuple with 1 at the $i-$th position and 0 otherwise.

An action of a Lie group $\mathcal{G}$ on $\mathrm{J}^0 = \mathcal{X} \times \mathcal{U}$ can be prolonged in a unique geometrically meaningful way to an action $\mathcal{G} \times \mathrm{J}^k \to \mathrm{J}^k$. This prolongation can be made explicit as a change of variables in differential equations. Like many other operations in differential geometry and jet calculus, this can be performed with the Maple library *DifferentialGeometry* written by I. Anderson [2]. Similarly, the infinitesimal generators $\mathrm{v}_1, \ldots, \mathrm{v}_r$ of the action of $\mathcal{G}$ on $\mathcal{X} \times \mathcal{U}$ can be prolonged to vector fields $\mathrm{v}_1^k, \ldots, \mathrm{v}_r^k$ on J^k such that they are the infinitesimal generators for the prolonged action. A differential invariant of order k is then a local invariant of the action prolonged to J^k. We can use their infinitesimal characterisation as a formal definition.

Definition 2.1. *A differential invariant of order k is a function $f : \mathrm{J}^k \to \mathbb{R}$ such that $\mathrm{v}_1^k(f) = 0, \ldots, \mathrm{v}_r^k(f) = 0$.*

For any k, a local cross-section to the orbits in J^k defines an invariantization and a set of normalized invariants:

$$\mathcal{I}^k = \{\bar{\iota} x_1, \ldots, \bar{\iota} x_m\} \cup \{\bar{\iota} u_\alpha \,|\, u \in \mathcal{U},\ |\alpha| \leq k\}.$$

As discussed in Section 1.1, $\mathcal{I}^k$ forms a functionally generating set of local invariants on J^k and any differential invariant of order k and less can be written in terms of those by a simple rewriting.

As we prolong the action, the dimension of the orbits can only increase. It can not go beyond the dimension of the group. The stabilization order $\bar{s}$ is the order at which the maximal dimension of the orbits becomes stationary. With

some mild asumptions on the group action on J^0, we can see that, for all $s \geq \bar{s}$, the orbits of the action on an open subset of J^s have the same dimension r as the group.

If we consider a local cross-section $\mathcal{P}$ on J^s, $s \geq \bar{s}$, given as the zero set of a map $p = (p_1, \ldots, p_r)$, the same equations define a local cross-section on J^{s+k}, for any $k > 0$. Thus, this determines the normalized invariants at any order $s + k$. The equations of the cross-section form a maximal independent set of relationships among them. This leaves us, however, with a rather infinite description of differential invariants.

A finite description of differential invariants can be obtained by introducing the concept of invariant derivations. Formally, these are total derivations that commute with the prolonged infinitesimal generators. When applied to a differential invariant, they give a differential invariant of a higher order.

The key fact is: When the stabilisation order is reached, and the orbits have therefore the same dimension as the group, the local cross-section defines a moving frame. With such a map in hand Fels and Olver [14] made explicit m invariant derivations $\mathcal{D} = (\mathcal{D}_1, \ldots, \mathcal{D}_m)$. Alternatively [29, Theorem 3.4] can be consulted.

2.2 Generators

As discussed above the orbits of the action of $\mathcal{G}$ on J^s have the same dimension r as the group $\mathcal{G}$, when s is greater than the stabilization order. To a local cross-section on J^s we associated

- an invariantization process and thus normalized invariants of order s and greater

  $$\mathcal{I}^{s+k} = \{\bar{\iota}x_1, \ldots, \bar{\iota}x_m\} \cup \{\bar{\iota}u_\alpha \,|\, u \in \mathcal{U},\ |\alpha| \leq s + k\}.$$

  Any differential invariant can be written in terms of these by a simple substitution.

- a moving frame $\rho : \mathrm{J}^s \to \mathcal{G}$ with which we can define invariant derivations $\mathcal{D} = (\mathcal{D}_1, \ldots, \mathcal{D}_m)$.

If applied to a differential invariant of order $s + k$, that can thus be written in terms of $\mathcal{I}^{s+k}$, the invariant derivations produce a differential invariant of order $s + k + 1$. The important fact for a computational approach is that the action of the invariant derivations on the normalized invariants can be made explicit [14, Section 13] (alternatively [29, Theorem 3.6]).

Let the function $(p_1, \ldots, p_r)$ on J^s define the cross-section. Denote by $\mathrm{D}(P)$ the $m \times r$ matrix $\left(\mathrm{D}_i(p_j)\right)_{i,j}$. The entries of $\mathrm{D}(P)$ are thus functions on J^{s+1}. Then $\mathrm{V}(P)$ is the $r \times r$ matrix $\left(\mathrm{v}_i(p_j)\right)_{i,j}$. As $\mathcal{P}$ is transverse to the orbits of the action of $\mathcal{G}$ on J^s, the matrix $\mathrm{V}(P)$ has nonzero determinant along $\mathcal{P}$ and therefore in a neighborhood of each of its points.

Theorem 2.2. *Let K be the $m \times r$ matrix obtained by invariantizing of the entries of $\mathrm{D}(P)\,\mathrm{V}(P)^{-1}$. Then*

$$\mathcal{D}(\bar{\iota} f) = \bar{\iota}(\mathrm{D} f) - K\,\bar{\iota}(\mathrm{v}(f)).$$

The above theorem implies in particular the so called *recurrence formulae*:

$$\bar{\iota}(\mathrm{D}_i u_\alpha) = \mathcal{D}_i(\bar{\iota} u_\alpha) + \sum_{a=1}^{r} K_{ia}\,\bar{\iota}(\mathrm{v}_a(u_\alpha))$$

where $K = \bar{\iota}(\mathrm{D}(P)\mathrm{V}(P)^{-1})$ has entries that are functions of $\mathcal{I}^{s+1}$. An inductive argument shows that any $\bar{\iota} u_\alpha$ can be written as a (rational) function of $\mathcal{I}^{s+1}$ and their derivatives. Combining this with the replacement property, we have a constructive way of rewriting any differential invariant in terms of the elements of $\mathcal{I}^{s+1}$ and their derivatives. A differential invariant of order k is first trivially rewritten in terms of $\mathcal{I}^k$. If $k \leq s+1$ we are done. Otherwise, any element $\bar{\iota} u_\alpha$ of $\mathcal{I}^k$ with $|\alpha| = k$ is a $\bar{\iota}(\mathrm{D}_i u_\beta)$, for some $1 \leq i \leq m$ and $|\beta| = k-1$. We can thus write it as: $\bar{\iota} u_\alpha = \bar{\iota}(\mathrm{D}_i u_\beta) = \mathcal{D}_i(\bar{\iota} u_\beta) + \sum_{a=1}^{r} K_{ia}\,\bar{\iota}\,(\mathrm{v}_a(u_\beta))$. This involves only elements of $\mathcal{I}^{k-1}$ and their derivatives. Carrying on recursively we can rewrite everything in terms of the elements of $\mathcal{I}^{s+1}$ and their derivatives.

Theorem 2.3. *Any differential invariant of order $s+k$ can be written in terms of the elements of $\mathcal{I}^{s+1}$ and their invariant derivatives of order $k-1$ and less.*

A natural question is to determine a smaller set of differential invariants that is generating. A first result, initially stated in [49] in the case of coordinate cross-section and generalized in [29, Theorem 4.2], provides a generating set of at most $m(r+1)+n$ differential invariants if we impose some condition on the cross-section. This condition is actually quite natural: It has to define a cross-section at all orders.

Theorem 2.4. *If $P = (p_1, \ldots, p_r)$ defines a cross-section for the action on J such that $P_k = (p_1, \ldots, p_{r_k})$ defines a cross-section for the action on J^k, for all k, then $\mathcal{E} = \{\bar{\iota}(\mathrm{D}^i(p_j)) \,|\, 1 \leq i \leq m,\ 1 \leq j \leq r\}$ together with $\mathcal{I}^0$ form a generating set of differential invariants.*

The invariants in this generating set were named *edge invariants* in [49]. There is another set of invariants of the same size that was exhibited in [30] that does not require the cross-section to be of minimal order.

Theorem 2.5. *The union of $0-$th order normalized invariants, $\mathcal{I}^0$, and the entries $\mathcal{K} = \{K_{ia} \,|\, 1 \leq i \leq m,\ 1 \leq a \leq r\}$, of the matrix $K = \bar{\iota}(\mathrm{D}(P)\mathrm{V}(P)^{-1})$, form a generating set of differential invariants.*

The generating property of these is actually a rather simple observation on the recurrence formula. These invariants carry an important geometric interpretation. They are the coefficients of the pull-back by the moving frame of the Maurer-Cartan forms on the group and are accordingly named the *Maurer-Cartan* invariants. Rewriting any normalized invariant, and hence any differential invariant, in terms of the Maurer-Cartan invariants and their invariant derivatives can be done by a simple recursive procedure.

2.3 Syzygies

The rewriting of any invariant in terms of the normalized invariants of order $s+1$, or the edge invariants, or the Maurer-Cartan invariants and their invariant derivatives is not unique. At each step of rewriting a $\bar{\iota} u_\alpha$, with $|\alpha| > s+1$, there might be several choices of pairs (i, β) such that $\beta + \epsilon_i = \alpha$ leading to rewriting $\bar{\iota} u_\alpha$ into $\mathcal{D}_i(\bar{\iota} u_\beta)$ with additional terms.

The first source of non-uniqueness comes from the fact that the invariant derivations do not commute. Yet their commutation rules are known explicitly [14, Section 13]. Those commutation rules can always be applied to rewrite any invariant derivatives in terms of monotone derivations $\mathcal{D}^\alpha = \mathcal{D}_1^{\alpha_1} \dots \mathcal{D}_m[\alpha_m]$.

Proposition 2.6. *For all* $1 \le i, j \le m$, $\left[\mathcal{D}_i, \mathcal{D}_j\right] = \sum_{k=1}^{m} \Lambda_{ijk}\, \mathcal{D}_k$ *where*

$$\Lambda_{ijk} = \sum_{c=1}^{r} K_{ic}\, \bar{\iota}(\mathrm{D}_j(\xi_{ck})) - K_{jc}\, \bar{\iota}(\mathrm{D}_i(\xi_{ck})),$$

$K = \bar{\iota}\left(D(P)\, V(P)^{-1}\right)$, *and* $\xi_{ck} = \mathrm{v}_c(x_k)$.

A *differential syzygy* is a relationship among a (generating) set of differential invariants and their monotone derivatives. A set of differential syzygies is complete if any other syzygy is inferred by those and their invariant derivatives.

The main point of [29] was to prove the completeness of the following set of syzygies for the normalized invariants of order $s+1$ in an appropriately formalized setting. The formalization also introduces some heavy notations that we skip to only render the essence. In the following theorem the $\bar{\iota} u_\alpha$ now stand for formal variables.

Theorem 2.7. *Consider a local cross-section given as the zero set of the functions* $p_1, \dots, p_r$ *on* J^s, *where* s *is greater or equal to the stabilization order. A complete set of syzygies for* $\mathcal{I}^{s+1}$, *the normalized invariants of order* $s+1$, *is given by the union of the three following finite subsets:*

- $\mathfrak{R} = \left\{ p_1\left(\bar{\iota} x, \bar{\iota} u, \dots \bar{\iota} u^{(s)}\right) = 0,\ \dots,\ p_r\left(\bar{\iota} x, \bar{\iota} u, \dots \bar{\iota} u^{(s)}\right) = 0 \right\}$
- $\mathfrak{S} = \left\{ S^i_{x_j} \,|\, 1 \le i, j \le m \right\} \cup \left\{ S^i_{u_\alpha} \,|\, |\alpha| \le s,\, 1 \le i \le m \right\}$ *where*

$$S^i_{x_j} : \mathcal{D}_i(\bar{\iota} x_j) = \delta_{ij} - \sum_{a=1}^{r} K_{ia}\, \bar{\iota}(\mathrm{v}_a(x_j))$$

and

$$S^i_{u_\alpha} : \mathcal{D}_i(\bar{\iota} u_\alpha) = \bar{\iota} u_{\alpha+\epsilon_i} - \sum_{a=1}^{r} K_{ia}\, \bar{\iota}(\mathrm{v}_a(u_\alpha))$$

- $\mathfrak{T} = \{\, T^i_{u_\beta} \,|\, |\beta| = s+1 \text{ and } f_\beta < i \leq m \,\}$, *where* $f_\beta = \{\min j \,|\, \beta_j \neq 0\}$ *and* $T^i_{u_\beta}$ *is*

$$\mathcal{D}_i\left(\bar{\iota} u_\beta\right) - \mathcal{D}_{f_\beta}\left(\bar{\iota} u_{\beta+\epsilon_i-\epsilon_{f_\beta}}\right) = \sum_{a=1}^{r} K_{ia}\, \bar{\iota}(\mathrm{v}_a(u_{\beta+\epsilon_i-\epsilon_{f_\beta}})) - K_{f_\beta a}\, \bar{\iota}(\mathrm{v}_a(u_\beta)).$$

The elements of the first set $\mathfrak{R}$ are the relationships on the normalized invariants inherited from the equations of the cross-section. The second set $\mathfrak{S}$ consists of the recurrence formulae between the derivatives of normalized invariants of order s and less and the normalized invariants of order $s+1$. The syzygies $\mathfrak{T}$ consist of a subset of cross-derivatives for the invariants of order $s+1$. If $\alpha + \epsilon_i = \beta + \epsilon_j = \gamma$ then

$$\mathcal{D}_i\left(\bar{\iota} u_\alpha\right) = \bar{\iota} u_\gamma - \sum_{a=1}^{r} K_{ia} \bar{\iota}\left(\mathrm{v}_a(u_\alpha)\right), \quad \mathcal{D}_j\left(\bar{\iota} u_\beta\right) = \bar{\iota} u_\gamma - K_{ja} \bar{\iota}\left(\mathrm{v}_a(u_\beta)\right).$$

The difference thus forms a syzygy on $\mathcal{I}^{s+1}$. The set of all cross-derivatives is redundant since we can obtain some by simple combinations of the others.

The syzygies for the Maurer-Cartan invariants can also be spelt out. Due to their geometric meaning, their syzygies arise as the pullback, by the moving frame, of the structure equation on the group. The structure equations depend on some constants C_{abc} that describe the infinitesimal generators as a Lie algebra:

$$\mathrm{v}_a \mathrm{v}_b - \mathrm{v}_b \mathrm{v}_a = \sum_{c=1}^{r} C_{abc} \mathrm{v}_c.$$

Theorem 2.8. *Beside the relationships stemming from the equations of the cross-section, the Maurer-Cartan invariants, that are the entries of the matrix* $K = \bar{\iota}\left(\mathrm{D}(P)\mathrm{V}(P)^{-1}\right)$*, are subject to the syzygies*

$$\mathcal{D}_j(K_{ic}) - \mathcal{D}_i(K_{jc}) + \sum_{1 \leq a < b \leq r} C_{abc}\left(K_{ia}K_{jb} - K_{ja}K_{ib}\right) + \sum_{k=1}^{m} \Lambda_{ijk}\, K_{kc} = 0,$$

for $1 \leq i < j \leq m$ *and* $1 \leq c \leq r$*, where* C_{abc} *are the structure constants and* Λ_{ijk} *are the coefficients of the commutation rules for the invariant derivations, written in terms of the Maurer-Cartan invariants.*

When it comes to the syzygies of the edge invariants, they can be obtained computationally from the syzygies on the normalized invariants by a differential elimination that takes place in the generalized differential algebra setting described in the next section. Differential elimination algorithms can be applied to further reduce the number of generating differential invariants, as was done in [33, 29]. Indeed, if a differential invariant can be written in terms of the others (and their invariant derivatives) it means that there is such a relationship in the differential ideal generated by the complete set of syzygies. This relationship can be exhibited by computing a representation of this differential ideal with an appropriate *elimination ranking*.

2.4 Example

Many simple examples, as well as computationally challenging ones, are treated in the papers [14, 29, 30] from which the material of this section is drawn as well as in, for instance, [33, 49, 39, 42, 40]. Here we wish to illustrate how the presented material is put into action on a well known example.

We consider the action of $SE(3)$ on surfaces in $\mathbb{R}^3$. We choose coordinate functions (x, y, u) for $\mathbb{R}^2 \times \mathbb{R}$, i.e. we consider x, y as the independent variables and u as the dependent variable. The infinitesimal generators of the classical action of the Euclidean group $SE(3)$ on $\mathbb{R}^3$ are:

$$\begin{array}{lll} \mathrm{v}_1 = \dfrac{\partial}{\partial x}, & \mathrm{v}_2 = \dfrac{\partial}{\partial y}, & \mathrm{v}_3 = \dfrac{\partial}{\partial v}, \\ \mathrm{v}_4 = u\,\dfrac{\partial}{\partial y} - y\,\dfrac{\partial}{\partial u}, & \mathrm{v}_5 = x\dfrac{\partial}{\partial y} - y\dfrac{\partial}{\partial x}, & \mathrm{v}_6 = x\dfrac{\partial}{\partial u} - u\dfrac{\partial}{\partial x}, \end{array}$$

The nonzero structure constants are given by the following commutators of the infinitesimal generators:

$$\begin{array}{c} [\mathrm{v}_1, \mathrm{v}_5] = \mathrm{v}_2,\ [\mathrm{v}_1, \mathrm{v}_6] = \mathrm{v}_3,\ [\mathrm{v}_2, \mathrm{v}_4] = -\mathrm{v}_3,\ [\mathrm{v}_2, \mathrm{v}_5] = -\mathrm{v}_1,\ [\mathrm{v}_3, \mathrm{v}_4] = \mathrm{v}_2, \\ [\mathrm{v}_3, \mathrm{v}_6] = -\mathrm{v}_1,\ [\mathrm{v}_4, \mathrm{v}_5] = \mathrm{v}_6,\ [\mathrm{v}_4, \mathrm{v}_6] = -\mathrm{v}_5,\ [\mathrm{v}_5, \mathrm{v}_6] = \mathrm{v}_4. \end{array}$$

Let us choose the classical cross-section defined by $P = (x, y, u, u_{10}, u_{01}, u_{11})$. The Maurer-Cartan matrix is then

$$K = \begin{pmatrix} 1 & 0 & 0 & 0 & \phi & \kappa \\ 0 & 1 & 0 & -\tau & \psi & 0 \end{pmatrix}$$

where

$$\kappa = \bar{\iota} u_{20}, \quad \tau = \bar{\iota} u_{02}, \quad \phi = \frac{\bar{\iota} u_{21}}{\bar{\iota} u_{20} - \bar{\iota} u_{02}}, \ \text{ and } \ \psi = \frac{\bar{\iota} u_{12}}{\bar{\iota} u_{20} - \bar{\iota} u_{02}}.$$

By Proposition 2.6 we have $[\mathcal{D}_2, \mathcal{D}_1] = \phi\,\mathcal{D}_1 + \psi\,\mathcal{D}_2$. The nonzero syzygies of Theorem 2.8 are:

$$\begin{aligned} \mathcal{D}_2(\kappa) - \phi\,(\kappa - \tau) &= 0, \\ \mathcal{D}_1(\tau) - \psi\,(\kappa - \tau) &= 0, \\ \mathcal{D}_2(\phi) - \mathcal{D}_1(\psi) - \kappa\,\tau - \phi^2 - \psi^2 &= 0. \end{aligned}$$

The first two syzygies imply that

$$\phi = \frac{\mathcal{D}_2(\kappa)}{\kappa - \tau}, \quad \psi = \frac{\mathcal{D}_1(\tau)}{\kappa - \tau}.$$

It follows that $\{\kappa, \tau\}$ forms a generating set. From their analytic expressions [21] we can write the Gauss and mean curvatures in terms of the normalized invariants and eventually in terms of the Maurer-Cartan invariants:

$$\sigma = \frac{u_{20}u_{02} - u_{11}}{(1 + u_{10}^2 + u_{01}^2)^2} = \bar{\iota} u_{20}\,\bar{\iota} u_{02} = \kappa\,\tau,$$

$$\pi = \frac{1}{2}\frac{(1 + u_{01}^2)u_{20} - 2_{10}u_{01}u_{11} + (1 + u_{10}^2)u_{20}}{(1 + u_{10}^2 + u_{01}^2)^{\frac{3}{2}}} = \frac{1}{2}(\bar{\iota} u_{20} + \bar{\iota} u_{02}) = \frac{1}{2}(\kappa + \tau).$$

Our generating invariants $\{\kappa, \tau\}$ are thus the principal curvatures. Substituting ϕ and ψ in the last syzygy we retrieve the Codazzi equation:

$$\mathcal{D}_2\left(\frac{\mathcal{D}_2(\kappa)}{\kappa-\tau}\right) - \mathcal{D}_1\left(\frac{\mathcal{D}_1(\tau)}{\kappa-\tau}\right) = \left(\frac{\mathcal{D}_2(\kappa)}{\kappa-\tau}\right)^2 + \left(\frac{\mathcal{D}_1(\tau)}{\kappa-\tau}\right)^2 + \kappa\tau.$$

3 Generalized Differential Algebras

What we have so far is a characterization of a generating set for the differential invariants of the action of a Lie group, a way to rewrite any differential invariant in terms of their monotone derivatives and a complete set of the differential relationships they satisfy. In the case of the rational action of an algebraic group we also have an algorithm to compute explicitly those generating differential invariants. Importantly though, the complete set of syzygies and the rewriting can actually be obtained independently of the explicit expression of the generating set. We can thus work formally with those.

The set of differential invariants is adequately represented by a differential algebra that is the quotient of a differential polynomial ring by a differential ideal. The differential polynomial ring has a differential indeterminate standing for each generating differential invariant. The syzygies live in this differential polynomial ring. They generate the differential ideal to quotient it with.

After the advent of Gröbner bases as a fundamental tool in computational algebra, efforts were made to provide practical algorithms for differential elimination and completion based on the concepts of differential algebra stemming out of work of J. Ritt and E. Kolchin [57, 36]. Complete lecture notes [25, 26] are available for a detailed understanding of the concepts involved and the algorithms underlying the *diffalg* library in Maple. A representative sample of the original articles is [6, 7, 24, 38, 41, 55, 56] All these address systems of classical differential equations, i.e. work with commuting derivations. Dealing with differential invariants and invariant derivations brought a new algorithmic challenge, first discussed in [39].

In the *algebra of differential invariants*, the derivations do not commute. Furthermore, the commutation coefficients involve the differential indeterminates themselves, or even their derivatives. An adequate concept of differential polynomial ring was provided in [28]. The rather amazing part is that, in the end, it differs very little from the classical case. In particular, all the algorithms that perform differential elimination and completion can be extended to this new context by just changing the way derivations act on derivatives.

Let $\mathcal{Y} = \{y_1, \ldots, y_n\}$ be a set of differential indeterminates. We define $\mathbb{K}[\![\mathcal{Y}]\!] = \mathbb{K}[\![y_1, \ldots, y_n]\!]$ to be the polynomial ring in the infinitely many variables $\{y_\alpha \mid y \in \mathcal{Y},\ \alpha \in \mathbb{N}^m\}$, called the derivatives. $\mathbb{K}$ is a field of characteristic zero to which the derivations can be restricted. In the classical case it is a field of functions in the independent variables. For the algebra of differential invariants, it is a field of constants. We endow $\mathbb{K}[\![\mathcal{Y}]\!]$ with a set of m derivations

$\mathcal{D} = \{\mathcal{D}_1, \ldots, \mathcal{D}_m\}$ defined recursively on $\{y_\alpha\}$ by

$$\mathcal{D}_i\left(y_\alpha\right) = \begin{cases} y_{\alpha+\epsilon_i} & \text{if } \alpha_1 = \ldots = \alpha_{i-1} = 0 \\ \mathcal{D}_j\mathcal{D}_i\left(y_{\alpha-\epsilon_j}\right) + \sum_{l=1}^{m} \Lambda_{ijl}\, \mathcal{D}_l\left(y_{\alpha-\epsilon_j}\right) & \text{where } j < i \text{ is s.t. } \alpha_j > 0 \\ & \text{while } \alpha_1 = \ldots = \alpha_{j-1} = 0 \end{cases}$$

where the family $\{\Lambda_{ijl}\}_{1\leq i,j,l\leq n}$ of elements of $\mathbb{K}\left[\!\left[\mathcal{Y}\right]\!\right]$ is such that

- $\Lambda_{ijl} = -\Lambda_{jil}$
- $\sum_{\mu=1}^{m} \Lambda_{ij\mu}\Lambda_{\mu kl} + \Lambda_{jk\mu}\Lambda_{\mu il} + \Lambda_{ki\mu}\Lambda_{\mu jl} = \mathcal{D}_k(\Lambda_{ijl}) + \mathcal{D}_i(\Lambda_{jkl}) + \mathcal{D}_j(\Lambda_{kil})$.

This latter relationship stands for a Jacobi identity and is quite natural. It insures that the $\{y_\alpha\}$ remain algebraically independent. It is certainly satisfied by the commutation coefficients that arise for the invariant derivations in Section 2.

Definition 3.1. *An* admissible ranking *on $\mathbb{K}\left[\!\left[\mathcal{Y}\right]\!\right]$ is a total order $\prec$ on the set of derivatives $\{y_\alpha\}$ such that*

- $|\alpha| < |\beta| \;\Rightarrow\; y_\alpha \prec y_\beta$, $\forall \alpha, \beta \in \mathbb{N}^m$, $\forall y \in \mathcal{Y}$;
- $y_\alpha \prec z_\beta \;\Rightarrow\; y_{\alpha+\gamma} \prec z_{\beta+\gamma}$, $\forall \alpha, \beta, \gamma \in \mathbb{N}^m$, $\forall y, z \in \mathcal{Y}$;
- $\sum_{l=1}^{m} \Lambda_{ijl}\mathcal{D}_l(y_\alpha) \prec y_{\alpha+\epsilon_i+\epsilon_j}$, *for all* $1 \leq i, j \leq m$, $\forall y \in \mathcal{Y}$.

If $\mathbb{K}\left[\!\left[\mathcal{Y}\right]\!\right]$ can be endowed with an admissible ranking then it is proved in [28] that

- $\mathcal{D}_i\mathcal{D}_j(p) - \mathcal{D}_j\mathcal{D}_i(p) = \sum_{l=1}^{m} \Lambda_{ijl}\mathcal{D}_l(p), \quad \forall p \in \mathbb{K}\left[\!\left[\mathcal{Y}\right]\!\right]$,
- $\mathcal{D}^\beta(y_\alpha) - y_{\alpha+\beta}$ ranks lower than $y_{\alpha+\beta}$.

In this case we shall say that $\mathbb{K}\left[\!\left[\mathcal{Y}\right]\!\right]$ is a *differential polynomial ring with non-trivial commutation rules for the derivations* $\{\mathcal{D}_1, \ldots, \mathcal{D}_m\}$.

Let us make a couple of remarks. If the Λ_{ijl} are differential polynomials that involve derivatives of order one or less then any orderly ranking is admissible. This is automatically the case for the algebra of differential invariants when normalized or Maurer-Cartan invariants are selected as generators. Elimination rankings can also be admissible. If the coefficients Λ_{ijl} involve only derivatives of a subset $\mathcal{Z} \subset \mathcal{Y}$ of the differential indeterminates then we can consider a ranking that eliminates $\mathcal{Y} \setminus \mathcal{Z}$.

In classical differential algebra, i.e. when the derivations commute, rankings are only subject to the conditions

- $y_\alpha \prec y_{\alpha+\gamma}$, $\forall y \in \mathcal{Y}$, $\alpha, \gamma \in \mathbb{N}^m$
- $y_\alpha \prec z_\beta \;\Rightarrow\; y_{\alpha+\gamma} \prec z_{\beta+\gamma}$, $\forall \alpha, \beta, \gamma \in \mathbb{N}^m$, $\forall y, z \in \mathcal{Y}$.

There we can consider rankings that are not semi-orderly as the one given by:

$$y_\alpha \prec y_\beta \;\Leftrightarrow\; \exists i \text{ such that } \alpha_1 = \beta_1, \ldots \alpha_{i-1} = \beta_{i-1} \text{ and } \alpha_i > \beta_i.$$

This type of ranking favors one of the derivations and cannot be handled in a context where derivations do not commute.

As mentioned above, the concepts and main results of classical differential algebra go through with nearly identical proofs. In particular any radical differential ideal is finitely generated and has a unique minimal decomposition into prime differential ideals. The algorithms also work, with the restriction of ranking described above. The Maple library *diffalg* was extended to handle this new type of differential polynomial ring [5, 27]. The concepts and algorithms underlying it are described in great details in [25, 26].

4 Prospects

In Section 1 we pointed out how obtaining a cross-section of degree 1 was interesting. Yet the question remains of when such a cross-section exists, and how to compute one. When no such cross-section can be found, one must still address the issue of determining the relationships on the generating rational invariants we obtained as the coefficients of the reduced Gröbner basis. We can always resort to another algebraic elimination to find them, but some geometric understanding should help the task.

In Section 2 we exhibited different sets of generating differential invariants. An open question is what is the minimal cardinality of such a set. For curves in affine n-space it is known that n differential invariants suffice as generators [19, 47]. One question I cannot answer though is how we can pinpoint n such generators from the Maurer-Cartan invariants. For surfaces in 3-space, under the Euclidean and affine group, two curvatures with a syzygy describe the algebra of differential invariants. Using the tools presented here and their implementation, it was shown that the same is true for the projective and conformal group acting on surfaces [33]. Some cases of 3-dimensional submanifolds in 4-space were also given a computational treatment in [29, Section 7]. For the general question of what is a minimal set of generating differential invariants, further theoretical development would be helpful.

The seminal article [14] offered methodological tools for deciding the equivalence of manifolds, the long standing problem attached to Cartan's moving frame method. My interest in the present subject stemmed out of the demonstration in [39] of how those tools could be used for solving a differential elimination problem through symmetry reduction. An example of how I think symmetry reduction, with a view towards differential elimination, should be tackled is presented as motivation in [28]. While some of the theoretical aspects have been worked out in the mean time, this particular problem has resisted my computational attempts at solving it. There is a need for more computational success on this idea so as to validate the approach.

A natural way to further advance the topic has been initiated in [52, 50, 51]. A methodological theory for pseudo-groups is introduced there in the same way as [14] started the topic for finite dimensional Lie groups.

References

[1] W. Adams and P. Loustaunau. *An introduction to Gröbner bases*. Number 3 in Graduate studies in Mathematics. AMS Providence, 1994.

[2] I. M. Anderson. Maple packages and Java applets for classification problems in geometry and algebra. In *Foundations of computational mathematics: Minneapolis, 2002*, volume 312 of *London Math. Soc. Lecture Note Ser.*, pages 193–206. Cambridge Univ. Press, Cambridge, 2004.

[3] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, 1993.

[4] M. Berger and B. Gostiaux. *Differential geometry: manifolds, curves, and surfaces*, volume 115 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988.

[5] F. Boulier and E. Hubert. DIFFALG*: description, help pages and examples of use*. Symbolic Computation Group, University of Waterloo, Ontario, Canada, 1998.

[6] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In A. H. M. Levelt, editor, *ISSAC'95*. ACM Press, New York, 1995.

[7] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, 20(1):73–121, 2009.

[8] M. Boutin and G. Kemper. On reconstructing configurations of points in $\mathbb{P}^2$ from a joint distribution of invariants. *Appl. Algebra Engrg. Comm. Comput.*, 15(6):361–391, 2005.

[9] P. Chossat and R. Lauterbach. *Methods in equivariant bifurcations and dynamical systems*, volume 15 of *Advanced Series in Nonlinear Dynamics*. World Scientific Publishing Co. Inc., River Edge, NJ, 2000.

[10] K.-S. Chou and C.-Z. Qu. Integrable equations arising from motions of plane curves. II. *J. Nonlinear Sci.*, 13(5):487–517, 2003.

[11] P. Comon and B. Mourrain. Decomposition of quantics in sums of power of linear forms. *Signal Processing*, 52(2):96–107, 1996.

[12] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag, 1992.

[13] H. Derksen and G. Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups I. Springer-Verlag, Berlin, 2002.

[14] M. Fels and P. J. Olver. Moving coframes. II. Regularization and theoretical foundations. *Acta Appl. Math.*, 55(2):127–208, 1999.

[15] J. Flusser, T. Suk, and B. Zitová. *Moments and Moment Invariants in Pattern Recognition*. Wiley and Sons Ltd., 2009.

[16] R. B. Gardner. The method of equivalence and its applications. *SIAM, Philadelphia*, 1989.

[17] K. Gatermann. *Computer algebra methods for equivariant dynamical systems*, volume 1728 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2000.

[18] J. H. Grace and A. Young. *The Algebra of Invariants*. Cambridge Univ. Press, Cambridge, 1903.

[19] M. L. Green. The moving frame, differential invariants and rigidity theorems for curves in homogeneous spaces. *Duke Math. Journal*, 45:735–779, 1978.

[20] G-M. Greuel and G. Pfister. *A* **Singular** *introduction to commutative algebra*. Springer-Verlag, Berlin, 2002.

[21] H. W. Guggenheimer. *Differential geometry*. McGraw-Hill Book Co., Inc., New York, 1963.

[22] G. Gurevich. *Foundations of the theory of algebraic invariants*. Noordhoff, 1964.

[23] D. Hilbert. *Theory of algebraic invariants*. Cambridge University Press, Cambridge, 1993.

[24] E. Hubert. Factorisation free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4-5):641–662, 2000.

[25] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems. In F. Winkler and U. Langer, editors, *Symbolic and Numerical Scientific Computing*, number 2630 in Lecture Notes in Computer Science, pages 1–39. Springer Verlag Heidelberg, 2003.

[26] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems. In F. Winkler and U. Langer, editors, *Symbolic and Numerical Scientific Computing*, number 2630 in Lecture Notes in Computer Science, pages 40–87. Springer Verlag Heidelberg, 2003.

[27] E. Hubert. DIFFALG*: extension to non commuting derivations*. INRIA, Sophia Antipolis, 2005.

[28] E. Hubert. Differential algebra for derivations with nontrivial commutation rules. *Journal of Pure and Applied Algebra*, 200(1-2):163–190, 2005.

[29] E. Hubert. Differential invariants of a Lie group action: syzygies on a generating set. *Journal of Symbolic Computation*, 44(3):382–416, 2009.

[30] E. Hubert. Generation properties of Maurer-Cartan invariants. Preprint `http://hal.inria.fr/inria-00194528`, 2012.

[31] E. Hubert and I. A. Kogan. Rational invariants of a group action. Construction and rewriting. *Journal of Symbolic Computation*, 42(1-2):203–217, 2007.

[32] E. Hubert and I. A. Kogan. Smooth and algebraic invariants of a group action. Local and global constructions. *Foundations of Computational Mathematics*, 7(4), 2007.

[33] E. Hubert and P. J. Olver. Differential invariants of conformal and projective surfaces. *Symmetry Integrability and Geometry: Methods and Applications*, 3(097), 2007.

[34] G. Jensen. *Higher order contact of submanifolds of homogeneous spaces*. Springer-Verlag, Berlin, 1977.

[35] G. Kemper. The computation of invariant fields and a new proof of a theorem by rosenlicht. *Transformation Groups*, 12:657–670, 2007.

[36] E. R. Kolchin. *Differential Algebra and Algebraic Groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press, 1973.

[37] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1*. Springer-Verlag, Berlin, 2000.

[38] E. L. Mansfield. *Differential Gröbner Bases*. PhD thesis, University of Sydney, 1991.

[39] E. L. Mansfield. Algorithms for symmetric differential systems. *Foundations of Computational Mathematics*, 1(4):335–383, 2001.

[40] E. L. Mansfield. *A Practical Guide to the Invariant Calculus*. Cambridge University Press, 2010.

[41] E. L. Mansfield and P. A. Clarkson. Application of the differential algebra package diffgrob2 to classical symmetries of differential equations. *Journal of Symbolic Computation*, 23(5-6):517–533, 1997.

[42] E. L. Mansfield and P. H. van der Kamp. Evolution of curvature invariants and lifting integrability. *J. Geom. Phys.*, 56(8):1294–1325, 2006.

[43] G. Marí Beffa. Projective-type differential invariants and geometric curve evolutions of KdV-type in flat homogeneous manifolds. *Annales de l'Institut Fourier (Grenoble)*, 58(4):1295–1335, 2008.

[44] J. Müller-Quade and T. Beth. Calculating generators for invariant fields of linear algebraic groups. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Computer Science*, pages 392–403. Springer, Berlin, 1999.

[45] J. L. Mundy, A. Zisserman, and D. A. Forsyth, editors. *Applications of Invariance in Computer Vision, Second Joint European - US Workshop, Ponta Delgada, Azores, Portugal, October 9-14, 1993, Proceedings*, volume 825. Springer, 1994.

[46] J.L. Mundy and A. Zisserman, editors. *Geometric Invariance in Computer Vision*. MIT Press, 1992.

[47] P. J. Olver. *Applications of Lie Groups to Differential Equations*. Number 107 in Graduate texts in Mathematics. Springer-Verlag, New York, 1986.

[48] P. J. Olver. *Equivalence, Invariants and Symmetry*. Cambridge University Press, 1995.

[49] P. J. Olver. Generating differential invariants. *Journal of Mathematical Analysis and Applications*, 333:450–471, 2007.

[50] P. J. Olver and J. Pohjanpelto. Moving frames for Lie pseudo-groups. *Canad. J. Math.*, 60(6):1336–1386, 2008.

[51] P. J. Olver and J. Pohjanpelto. Differential invariant algebras of Lie pseudo-groups. *Advances in Mathematics*, 222:1746–1792, 2009.

[52] P.J. Olver and J. Pohjanpelto. Maurer-Cartan forms and the structure of Lie pseudo-groups. *Selecta Mathematica*, 11:99–126, 2005.

[53] L. V. Ovsiannikov. *Group analysis of differential equations*. Academic Press Inc., New York, 1982.

[54] V. L. Popov and E. B. Vinberg. Invariant theory. In *Algebraic geometry. IV*, number 55 in Encyclopaedia of Mathematical Sciences, pages 122–278. Springer-Verlag, 1994.

[55] G. J. Reid. Algorithms for reducing a system of pde to standard form, determining the dimension of its solution space and calculating its taylor series solution. *European Journal Of Applied Mathematics*, 2:293–318, 1991.

[56] G. J. Reid and A. Boulton. Reduction of differential equations to standard form and their integration using directed graphs. In S. M. Watt, editor, *ISSAC'91*, pages 308–312. ACM Press, 1991.

[57] J. F. Ritt. *Differential Algebra*, volume XXXIII of *Colloquium publications*. American Mathematical Society, 1950.

[58] M. Rosenlicht. Some basic theorems on algebraic groups. *American Journal of Mathematics*, 78:401–443, 1956.

[59] C. Shakiban and P. Lloyd. Signature curves statistics of DNA supercoils. In *Geometry, integrability and quantization*, pages 203–210. Softex, Sofia, 2004.

[60] B. Sturmfels. *Algorithms in invariant theory.* Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1993.