Invariant Algebraic Sets and Symmetrization of Polynomial Systems

Evelyne Hubert

Invariant Algebraic Sets and Symmetrization of Polynomial Systems

Evelyne Hubert *

January 17th, 2016

Abstract

Assuming the variety of a polynomial set is invariant under a group action, we construct a set of invariants that define the same variety. Our construction can be seen as a generalization of the previously known construction for finite groups once we introduce the *symmetrizations* of a polynomial w.r.t. a section to the orbits of the group action. The symmetrisations are polynomials in a generating set of rational invariants as constructed in [9]. The results have thus to be understood outside of a proper closed invariant variety, independent of the polynomial set considered.

Keywords: Rational invariants; Polynomial systems with symmetry; Section.

1 Introduction

Consider the variety $\mathcal{F}$ in $\mathbb{C}^n$ of a finite set of polynomials F in $\mathbb{C}[z_1, \ldots, z_n]$. $\mathcal{F}$ can be invariant under the action of a group $\mathcal{G}$ without the polynomials in F being themselves invariant. For a given set F of polynomials as above we shall determine a set of invariant functions $\tilde{F}$ such that the zero set of $\tilde{F}$ is equal to the variety of F outside of some proper closed algebraic set $\mathcal{W}$. The elements of $\tilde{F}$ are polynomials in a fixed finite set of generating rational invariants. The restriction to a dense open set is therefore unavoidable for a general statement. Yet this dense open set is independent of F.

When $\mathcal{G}$ is a finite group acting regularly, a system of polynomial invariants $\tilde{F}$ that have the same variety as F can be determined explicitely. The construction of $\tilde{F}$ can be found for instance in the proof of [24, Proposition 2.6.4] and this construction also applies for $\mathcal{G}$-invariant semi-algebraic sets [2]. The existence of such a $\tilde{F}$ for compact group is proved in [1]. It was nonetheless an open question in [2] whether there exists a constructive approach. The present article aims to provide such a construction for rational actions of any algebraic group.

A polynomial system that does not exhibit the symmetry of its variety can for instance appear as the result of algebraic computations; These rarely preserve the known symmetry of the problem. Determining an equivalent system in terms of a generating set of invariants allows further qualitative analysis and a simplified resolution. Specific methods address the resolution of a polynomial system given by the components of an equivariant map [8]; When the group action is given by orthogonal representations one can construct a set of polynomial invariants with the same variety of the reals [7, 13, 27]. Yet, even in the equivariant case, there is no systematic process to produce a system of invariants with the same set of zeros in general.

The construction of the set $\tilde{F}$ above is based on a concept of *symmetrizations* of a polynomial . This latter builds on the construction of the field of rational invariants [9] that makes central use of the notion of section to the orbits. The construction in [9] was later extended to the construction of the ring of polynomial

*INRIA Méditerranée, 06902 Sophia Antipolis, France. `evelyne.hubert@inria.fr`

invariants of some non reductive groups [5, Section 4.10]. The geometric interpretation of the constructive definition of symmetrization allows us to use an argument analogous to the finite group case to prove that the zero set of the symmetrizations $\tilde{F}$ of the elements of F is equal to the variety of F.

The symmetrizations we introduce is connected to the concept of algebraic invariantization in [10]. The latter was introduced as a constructive approach to the local invariantization process associated to the moving frame construction of differential invariants and invariant derivations [6]. One can also see that the treatment of polynomial systems under a scaling symmetry (in particular multi-homogeneous polynomial systems) in [11] is a special case of symmetrisation.

In next section we define the group actions to be considered as well as the notion of *section of degree* e to the orbits. We show how to compute a finite set of generating rational invariants. They are the coefficients of the reduced Gröbner basis of the *orbit-section* ideal. These are basically the results of [9] for which we provide simplified proofs; Compared to the alternative approach in [5, Section 4.10] the present proofs allow to keep the geometrical meaning of the construction. In Section 3 we give a constructive definition of symmetrization w.r.t. a given section to the orbits: to any polynomial f is associated e *symmetrizations*, where e is the degree of the section to the orbits. These symmetrizations are polynomials in the generating invariants. If F is a set of polynomials whose variety is invariant under the group action then the set $\tilde{F}$ of the symmetrisations of the elements of F have the same zero set. The result has to be understood within a $\mathcal{G}$-invariant open set where the reduced Gröbner basis of the orbit-section ideal specializes well.

Acknowledgments: The authors is grateful to Guillaume Moroz and Fabrice Rouillier for discussions on the specialisation properties of Gröbner bases.

2 Construction of rational invariants

We shall first introduce the notions and notations to be used in the article. We then review the construction of rational invariants that appeared in [9]; We nonetheless introduce a better definition of section to the orbits of the group action and provide a simplified set of proofs. Theorem 2.5 and 2.6 can nonetheless be compared respectively with [9, Theorem 3.5 and 3.7]. The different notions of sections are discussed in the last subsection.

2.1 Rational action of an algebraic group

$\mathbb{K}$ is a field of characteristic zero, $\overline{\mathbb{K}}$ is an algebraically closed field extension of $\mathbb{K}$. To make the constructions simpler, we deal here with $\mathcal{Z}$ an affine space $\overline{\mathbb{K}}^n$ but they can be extended to an irreducible algebraic variety. The groups we consider are affine algebraic groups. They are given by an affine algebraic variety $\mathcal{G}$ endowed with a group operation $\cdot : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$ and an inverse $\mathcal{G} \to \mathcal{G}$ given by regular maps. To be explicit, we assume that $\mathcal{G}$ is embedded in $\overline{\mathbb{K}}^l$ and $G \subset \mathbb{K}[\lambda_1, \dots, \lambda_l]$ is its defining ideal. The coordinate ring $\mathbb{K}[\mathcal{G}]$ can be identified with the quotient algebra $\mathbb{K}[\lambda_1, \dots, \lambda_l]/G$.

A rational action of $\mathcal{G}$ on $\mathcal{Z}$ is defined by a homomorphism ρ from $\mathcal{G}$ to the group of birational maps of $\mathcal{Z}$. In practice it is given by a rational map $\mathcal{G} \times \mathcal{Z} \dashrightarrow \mathcal{Z}$, $(\lambda, z) \mapsto \lambda \star z = \rho(\lambda)(z)$ defined by quotients of polynomials:

$$\lambda \star z = \left(\frac{h_1(\lambda, z)}{h_0(\lambda, z)}, \dots, \frac{h_n(\lambda, z)}{h_0(\lambda, z)} \right)$$

where $h_0, h_1, \dots, h_n \in \mathbb{K}[\lambda, z]$. When we write $(\lambda, z) \in \mathcal{G} \times \mathcal{Z}$ we mean that (λ, z) belongs to the open set of $\mathcal{G} \times \mathcal{Z}$ where $\lambda \star z$ is well defined. The orbit $\mathcal{O}_z$ of $z \in \mathcal{Z}$ is the image of the rational map $\mathcal{G} \dashrightarrow \mathcal{Z}$, $\lambda \mapsto \lambda \star z$.

A rational action of $\mathcal{G}$ on $\mathcal{Z}$ induces an action on the field of rational functions $\mathbb{K}(\mathcal{Z})$ given by $(\lambda \star f)(z) = f(\lambda^{-1} \star z)$. The set of rational invariants $\mathbb{K}(\mathcal{Z})^{\mathcal{G}}$ is the subfield of $\mathbb{K}(\mathcal{Z})$ of rational functions f s.t. $\lambda \star f = f$, for all $\lambda \in \mathcal{G}$.

Lemma 2.1 *If p/q is a rational invariant, with $p, q \in \mathbb{K}[z]$ relatively prime, then the varieties $\mathcal{V}(p)$ and $\mathcal{V}(q)$ are invariant under the action of $\mathcal{G}$.*

PROOF: By hypothesis $p(z)\, q(\lambda \star z) = q(z)\, p(\lambda \star z)$ for all $(\lambda, z) \in \mathcal{G} \times \mathcal{Z}$. Hence $p(\lambda \star z) = 0$ for all $(\lambda, z) \in \mathcal{G} \times \mathcal{V}(p) \setminus \mathcal{V}(q)$. Since p and q are relatively prime, $\mathcal{V}(p) \setminus \mathcal{V}(q)$ is dense in $\mathcal{V}(p)$. Hence $p(\lambda \star z)$ has to vanish on the whole of $\mathcal{G} \times \mathcal{V}(p)$. □

When $\mathcal{G}$ is connected and acts regularly on $\mathcal{Z}$, one can furthermore conclude that p and q are *semi-invariants* with the same *weight*, i.e. $p(\lambda \star z) = \chi(\lambda)\, p(z)$ and $q(\lambda \star z) = \chi(\lambda)\, q(z)$ where $\chi : \mathcal{G} \to \bar{\mathbb{K}}^*$ is a group morphism [22, Theorem 3.1 and 3.3].

2.2 Sections to the orbits

Definition 2.2 *For a given rational action of $\mathcal{G}$, an irreducible variety $\mathcal{P}$ is a* section of degree e *to the orbits if there exists an open dense subset $\mathcal{U}$ of $\mathcal{Z}$ such that the orbits of $\mathcal{U}$ intersect $\mathcal{P}$ at exactly e points.*

Thus a section cannot be contained in a proper $\mathcal{G}$-invariant subvariety of $\mathcal{Z}$. Yet the present notion of section is not restrictive. Most irreducible subvarieties of complementary dimension to the generic orbits are sections. One can always choose an affine linear space as a section [9, Theorem 3.3], or even the level set of some of coordinates [10, Theorem 1.6]. For a generic affine linear space the degree of the section it defines is the degree of the orbits. Sections of lower degree can be obtained by taking into consideration the points at infinity or the singular points of the closure of generic orbits. Section of degree one are of particular interest, as we shall point out at several places.

Proposition 2.3 *Assume the generic orbits have dimension d and take $P \subset \mathbb{K}[Z_1, \ldots, Z_n]$ as a prime ideal of codimension d. Consider*

$$A = (h_0(\lambda, z)\, Z_1 - h_1(\lambda, z),\ \ldots,\ h_0(\lambda, z)\, Z_n - h_n(\lambda, z)) \subset \mathbb{K}[z, Z, \lambda] \tag{1}$$

Then the variety $\mathcal{P}$ of P is a section if the ideal

$$I_{\mathcal{P}} = (G + A + P) : h_0^{\infty} \cap \mathbb{K}(z)[Z]. \tag{2}$$

is zero dimensional. The dimension e of the quotient algebra $\mathbb{K}(z)[Z]/I_{\mathcal{P}}$ as a $\mathbb{K}(z)$-vector space is the degree of the section.

Indeed, by specializing z to a generic point in $\mathcal{Z}$, the ideal $I_{\mathcal{P}}$ becomes the ideal of the intersection of the orbit $\mathcal{O}_z$ of z with the section $\mathcal{P}$. We shall refer to the ideal $I_{\mathcal{P}}$ as the *orbit-section* ideal.

Given the equations of an irreducible variety we can thus determine if it is a section and compute its degree by computing the Gröbner basis[1] of the elimination ideal $I_{\mathcal{P}}$. The degree e of the section $\mathcal{P}$ is the number of monomials *under the staircase* defined by the leading monomials of the Gröbner basis of $I_{\mathcal{P}}$. As we shall see in next section, the reduced Gröbner bases of $I_{\mathcal{P}}$ also delivers a generating set of invariants for the action.

Example 2.4 SCALINGS IN THE PLANE. *Consider the action of the multiplicative group $\mathbb{K}^*$ given by*

$$\begin{array}{rccc} \star : & \mathbb{K}^* \times \mathbb{K}^2 & \to & \mathbb{K}^2 \\ & (\lambda, (x, y)) & \mapsto & (\lambda^a\, x, \lambda^b\, y) \end{array}$$

[1] The reader is invited to consult for instance [3, 4] for the basic concepts and results about Gröbner bases.

where a and b are positive integers that we assume here relatively prime. The ideal of the orbit of $(x,y) \in \mathbb{K}^2 \setminus \{(0,0)\}$ is then given by

$$O = (x^b Y^a - y^a X^b).$$

Note that the orgin is in the closure of all the orbits. There is therefore no non constant polynomial invariant for this action [5, Lemma 2.4.5].

A generic affine line in $\mathbb{K}^2$ is a section of degree $\max(a,b)$. But $P = (X-1)$ defines a section of degree a since the ideal of the intersection of the orbit of $(x,y) \in \mathbb{K}^2 \setminus \{(0,y) \,|\, y \in \mathbb{K}\}$ with the variety $\mathcal{P}$ of P is

$$I = \left(X - 1, Y^a - \frac{y^a}{x^b} \right).$$

Alternatively a section of degree 1 is provided by the Bezout coefficients $\alpha, \beta \in \mathbb{Z}$ s.t. $\alpha\, a - \beta\, b = 1$. For the purpose of this example we can assume that $\alpha, \beta \in \mathbb{N}$. If we choose $P = \left(X^\alpha - Y^\beta\right)$ then the ideal of the intersection of the orbit of $(x,y) \in \mathbb{K}^2 \setminus \{(0,y) \,|\, y \in \mathbb{K}\}$ with the variety $\mathcal{P}$ of P is

$$I_{\mathcal{P}} = \left(X - \left(\frac{y^a}{x^b}\right)^\beta, \; Y - \left(\frac{y^a}{x^b}\right)^\alpha \right).$$

This generalizes for scalings in any dimension, i.e. diagonal linear actions of the algebraic torus $(\mathbb{K}^*)^d$: we can compute the (binomial) equations of a section of degree one with linear algebra over the integers [11, 12].

2.3 Generating invariants and rewriting

As can be observed in the examples presented above, the coefficients of the reduced Gröbner basis of the orbit-section ideal $I_{\mathcal{P}}$ are rational invariants. This basically owes to the simple fact that $\mathcal{O}_z = \mathcal{O}_{\lambda \star z}$ and therefore $\mathcal{O}_z \cap \mathcal{P} = \mathcal{O}_{\lambda \star z} \cap \mathcal{P}$ so that a canonical representation of the orbit-section ideal $I_{\mathcal{P}}$ must be defined over $\mathbb{K}(z)^{\mathcal{G}}$. A reduced Gröbner basis is such canonical representative. We furthermore show that a reduced Gröbner basis allows to rewrite any invariants in terms of its coefficients.

Theorem 2.5 *The coefficients of a reduced Gröbner basis of the orbit-section ideal $I_{\mathcal{P}}$ belong to $\mathbb{K}(z)^{\mathcal{G}}$.*

PROOF: For a given term order, the reduced Gröbner basis of an ideal is unique. Let B be the reduced Gröbner basis for $I_{\mathcal{P}}$ for a given term order on Z. As such it consists of monic polynomials in $\mathbb{K}(z)[Z]$.

There is a closed proper subset $\mathcal{W}$ of $\mathcal{Z}$ s.t. for $z \in \mathcal{Z} \setminus \mathcal{W}$ the image of B under specialization is a (reduced) Gröbner basis for the ideal whose variety is the intersection of $\mathcal{O}_z$ with $\mathcal{P}$. Since $\mathcal{O}_z = \mathcal{O}_{\lambda \star z}$, the specializations of B to z and to $\lambda \star z$ bring the same reduced Gröbner basis, for a generic $\lambda \in \mathcal{G}$. Therefore $B \subset \mathbb{K}(z)^{\mathcal{G}}[Z]$. □

In this construction it is clear that the coefficients of the Gröbner basis of $I_{\mathcal{P}}$ *separate* generic orbits. According to [23, Theorem 2] or [22, Lemma 2.1], we can deduce that they form a generating set. The alternative proof we give next is constructive. We show how to rewrite any invariant in terms of the coefficients of the reduced Gröbner basis.

Theorem 2.6 *Consider $\{r_1, \ldots, r_m\} \in \mathbb{K}(z)^{\mathcal{G}}$ the coefficients of a reduced Gröbner basis B of $I_{\mathcal{P}}$. Then $\mathbb{K}(z)^{\mathcal{G}} = \mathbb{K}(r_1, \ldots, r_m)$ and we can rewrite any rational invariant $\frac{p}{q}$, with $p, q \in \mathbb{K}[z]$ relatively prime, in terms of those as follows.*

Take a new set of indeterminates $y_1, \ldots, y_m$ and consider the set $\bar{B} \subset \mathbb{K}[y, Z]$ obtained from B by substituting r_i by y_i. Let $a(y,Z) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha(y) Z^\alpha$ and $b(y,Z) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha(y) Z^\alpha$ in $\mathbb{K}[y,Z]$ be the normal forms[2] of $p(Z)$ and $q(Z)$ w.r.t. $\bar{B}$. There exists $\alpha \in \mathbb{N}^m$ s.t. $b_\alpha(r) \neq 0$ and for any such α we have $\frac{p(z)}{q(z)} = \frac{a_\alpha(r)}{b_\alpha(r)}$.

[2] For the reductions in $\mathbb{K}[y,Z]$ the term order on Z is extended to a block order $y \ll Z$ so that the set of leading terms of $\bar{B}$ is equal to the set of leading terms of B.

PROOF: We first note that neither $q(Z)$, nor $p(Z)$, belong to P. Indeed $\mathcal{P} \subset \mathcal{V}(q)$ and $\mathcal{V}(q)$ invariant (Lemma 2.1) would imply $q = 0$ since the orbits of the points on $\mathcal{P}$ fill an open dense set of $\mathcal{Z}$ by hypothesis.

We now argue that $I_{\mathcal{P}} \cap \mathbb{K}[Z] = P$. We obviously have $P \subset I_{\mathcal{P}} \cap \mathbb{K}[Z]$ and therefore the projection of $\mathcal{V}(I_{\mathcal{P}} \cap \mathbb{K}[z, Z])$ on the Z-components is included in $\mathcal{P}$. Conversely, for a generic point Z on $\mathcal{P}$, the points $(\lambda \star Z, Z)$, for $\lambda \in \mathcal{G}$ lies $\mathcal{V}(I_{\mathcal{P}} \cap \mathbb{K}[z, Z])$. The projection of this latter on the second component is thus dense in $\mathcal{P}$.

Therefore neither $p(Z)$ nor $q(Z)$ belong to $I_{\mathcal{P}}$. The normal forms of $q(Z)$ and $p(Z)$ w.r.t. B are, respectively, $b(r, Z)$ and $a(r, Z)$ and they are thus both different from zero.

Since p/q is invariant, $p(z)\, q(\lambda \star z) \equiv q(z)\, p(\lambda \star z) \mod G$. Hence $p(z)q(Z) - q(z)p(Z)$ belongs to $I_{\mathcal{P}}$ so that its normal form with respect to B must be zero: $p(z)\, b(r, Z) = q(z)\, a(r, Z)$. The conclusion follows. □

Theorem 2.6 applies in particular to polynomial invariants. We immediately see that:

Corollary 2.7 *Any polynomial invariant can be written as a polynomial in* $\{r_1, \ldots, r_m\}$.

Therefore a case of special interest is when the coefficients of the reduced Gröbner basis have no denominator.

Proposition 2.8 *If the coefficients of a reduced Gröbner basis of* $I_{\mathcal{P}}$ *are polynomials, then they generate the ring of polynomial invariants* $\mathbb{K}[z]^{\mathcal{G}}$.

Example 2.9 *Consider the linear action of* $\mathrm{SO}_2(\overline{\mathbb{K}})$ *on* $\mathcal{Z} = \overline{\mathbb{K}}^3$ *acting by rotation on the* (x, y)*-plane. We have*

$$G = (\lambda^2 + \mu^2 - 1) \quad \text{and} \quad A = (X - (a\,x - b\,y),\; Y - (b\,x + a\,y),\; Z - z)\,.$$

Choose the section $\mathcal{P}$ *of degree* 2 *given by* $P = (\,X\,)$. *Then* $I_{\mathcal{P}} = (X,\, Y^2 - (x^2 + y^2),\, Z - z)$. *Thus* $r = x^2 + y^2$ *and* z *form a generating set for* $\mathbb{K}(x, y, z)^{\mathcal{G}}$, *but also for* $\mathbb{K}[x, y, z]^{\mathcal{G}}$.

More generally, when the coefficients are the quotients of invariant polynomials, they provide generators for a localisation of the invariant ring. The generators of the invariant ring can then be computed following [5, Section 4.1.2].

Section of degree one are of special interest. For these, the reduced Gröbner basis of the orbit-section ideal $I_{\mathcal{P}}$ w.r.t. any term order is of the form $\{Z_1 - r_1(z), \ldots, Z_n - r_n(z)\}$, where $r_i \in \mathbb{K}(z)^{\mathcal{G}}$. The rewriting described in Theorem 2.6 is then a simple substitution: if f is a rational invariant then $f(z_1, \ldots, z_n) = f\,(r_1(z), \ldots, r_n(z))$.

Example 2.10 *Following up on Example 2.4, for any invariant* $f \in \mathbb{K}(z)^{\mathcal{G}}$ *we have* $f(x, y) = f\left(r^{\beta}, r^{\alpha}\right)$, *where* $r = \frac{y^a}{x^b}$.

2.4 Section, quasi-section, cross-section, partial section

We discuss here the different concepts of sections. The present concept of *section of degree e* appears as *quasi-section* in [22]. In [9] were defined *cross-sections of degree e*. As explained next, they differ slightly of the present *section of degree e*

In [9, Definition 3.1] an irreducible ideal P, of complementary dimension to the generic orbits, defines a cross-section if the ideal $O + P$ is zero-dimensional and radical, where $O = (G + A) : h_0^{\infty} \cap \mathbb{K}(z)[Z]$ is the ideal of the generic orbit. The degree of the cross-section is then the dimension of the $\mathbb{K}(z)$-vector space $\mathbb{K}(z)[Z]/(O + P)$. This is the number of points of intersection of the closure of a generic orbit with the variety $\mathcal{P}$ of P. The following example shows how this can differ from the present notion of section.

Example 2.11 *Consider the scaling $\lambda \star (x,y) = (\lambda^2 x, \lambda^3 y)$ and $\mathcal{P}$ as the variety of $P = (Y - X)$. On one hand, the orbit-section ideal is*

$$I_{\mathcal{P}} = \left(Y - \frac{x^3}{y^2},\ X - \frac{x^3}{y^2} \right)$$

so that $\mathcal{P}$ is a section of degree one. On the other hand $O = \left(y^2 X^3 - x^3 Y^2\right)$ so that

$$O + P = \left(X - Y, Y^2 \left(Y - \frac{x^3}{y^2} \right) \right).$$

The closure of the generic orbit contains the origin, as does $\mathcal{P}$. $\mathcal{P}$ fails to be a cross-section because $O + P$ is not radical.

Both concepts lead to valid constructions for the fields of rational invariants. The present concept of section appears nonetheless as more favorable. For instance, sections of degree one can be obtained for any scaling, i.e. diagonal representation of tori [11, 12].

In [9] we also proved Theorem 2.5 and 2.6 for the orbit ideal $O = (G + A) : h_0^\infty$ and it is natural to consider intermediate cases where $\mathcal{P}$ is of lower dimension than the codimension of the generic orbits and thus the ideal $(G + A + P) : h_0^\infty$ is not zero dimensional. The proofs of Theorem 2.5 and 2.6 used the following properties:

- $\mathcal{P}$ is not contained in any invariant hypersurface
- $(G + A + P) : h_0^\infty \cap \mathbb{K}[Z] = P$.

Those properties would be sufficient to define a notion of *partial section* and this line of ideas was molded in another terminology in [5, Section 4.10].

3 Symmetrization

We shall define a concept of symmetrization with respect to a section. The definition is constructive. We then prove that within a $\mathcal{G}$-invariant open set, which depends on the chosen section and a term order, the symmetrization of a polynomial system produces invariants with the same variety. This $\mathcal{G}$-invariant open set is given as the locus of points with good specialisation properties of the reduced Gröbner basis of the orbit-section ideal. We discuss how to determine this locus first.

3.1 Specializations

The variety of the orbit-section ideal $I_{\mathcal{P}}$ defined in previous section is the intersection of the section $\mathcal{P}$ with the generic orbit. The construction of rational invariants makes essential use of the reduced Gröbner basis B of $I_{\mathcal{P}}$ for a given term order on Z.

Recall that G is the ideal in $\mathbb{K}[\lambda]$ defining the group $\mathcal{G}$, that A is the set of polynomials in $\mathbb{K}[z, Z, \lambda]$ describing the action of $\mathcal{G}$ in $\mathcal{Z}$ (see Equation (1) in Proposition 2.3) and that P is the prime ideal defining the section $\mathcal{P}$. If $\tilde{B}$ is a reduced Gröbner basis for $(G + A + P) : h_0^\infty$, as an ideal in $\mathbb{K}(z)[Z, \lambda]$, according to a block order that eliminates λ, then $B = \tilde{B} \cap \mathbb{K}(z)[Z]$ is the reduced Gröbner basis for $I_{\mathcal{P}}$. For $\bar{z} \in \mathcal{Z}$ we write $A_{\bar{z}} \subset \overline{\mathbb{K}}[Z, \lambda]$ for the specialisation of A at $\bar{z}$.

There exists a proper closed set $\mathcal{W}$ in $\mathcal{Z}$ such that for $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$ the specialisation $B_{\bar{z}}$ of B at $\bar{z}$ is precisely the reduced Gröbner basis of $(G + A_{\bar{z}} + P) : h_0^\infty \cap \overline{\mathbb{K}}[Z]$. The variety of this latter ideal is the intersection of $\mathcal{O}_{\bar{z}}$ with $\mathcal{P}$. We can determine such a set $\mathcal{W}$ with specialisation criteria as [14, Theorem 3.1] or [15, Theorem

4.3] that apply to a Gröbner basis of $(G + A + P) : h_0^\infty$ considered as an ideal of $\mathbb{K}[z][Z,\lambda]$. Yet, to compute a minimal such $\mathcal{W}$ it is necessary to resort to the computation of a comprehensive Gröbner basis [15, 25] or of a Gröbner cover [26, 17].

In the present situation, $B_{\bar{\lambda}\star\bar{z}} = B_{\bar{z}}$ for any $\bar{\lambda} \in \mathcal{G}$ so that the minimal such $\mathcal{W}$ is $\mathcal{G}$-invariant. It is left for future research to examine if this property can bring a computational advantage in determining $\mathcal{W}$, in combination with the geometric information that can be read directly on the Gröbner basis [16, 19, 20]. Let us just make one observation. Obviously the varieties of the denominators of the coefficients in B, which are $\mathcal{G}$-invariant, are contained in $\mathcal{W}$. Yet the following example shows that it is not enough to consider the product of those denominators. Among other considerations one might have to consider the denominators in $\tilde{B}$.

Example 3.1 *Consider the action of $\mathcal{G} = \overline{\mathbb{K}}^*$ on the plane given by $\lambda \star (x,y) = \left(\lambda^{-1} x, \lambda y\right)$. We have $G = (\lambda\mu - 1)$ in $\mathbb{K}[\lambda,\mu]$, $A = (X - \mu x, Y - \lambda y)$ and let us take the section defined by $P = (X - 1)$.*

The reduced Gröbner basis of $J = G + A + P$ in $\mathbb{K}(x,y)[X,Y,\lambda,\mu]$ for a block term order $\{X,Y\} \ll \{\lambda,\mu\}$ is

$$\tilde{B} = \left\{X - 1, Y - x y, \lambda - x, \mu - \frac{1}{x}\right\}.$$

When $\bar{x} \neq 0$, the Gröbner basis for the ideal of $\mathcal{O}_{(\bar{x},\bar{y})} \cap \mathcal{P}$ is obtained by specializing $B = \tilde{B} \cap \mathbb{K}(x,y)[X,Y] = \{X - 1, Y - x y\}$. Hence for this section $\mathcal{W} = \mathcal{V}(x)$. This is also what appears when computing the Gröbner cover [17]. This corroborates the fact that the orbits of the points $(0,\bar{y})$ do not intersect the section defined by P.

Example 3.2 *Following on Example 2.9. The implementation of the Gröbner cover [17, 18] shows that we have to take $\mathcal{W} = \mathcal{V}\left(x^2 + y^2\right)$.*

The above examples could nonetheless be deceptive in that it leads us to think that the denominators of $\tilde{B}$ provide a description of $\mathcal{W}$. Some denominators in $\tilde{B}$ are spurious in the description of $\mathcal{W}$.

3.2 Symmetrizations of a polynomial

Consider a rational action of $\mathcal{G}$ on $\mathcal{Z} = \overline{\mathbb{K}}^n$ and $\mathcal{P}$ a section of degree e. We fix a term order on the variables $Z = \{Z_1,\ldots,Z_n\}$ and consider the reduced Gröbner basis B of the orbit-section ideal $I_\mathcal{P}$ in $\mathbb{K}(z)[Z]$. The coefficients of B belong to and generate $\mathbb{K}(z)^\mathcal{G}$ (Theorem 2.5 and 2.6). $\mathbb{K}(z)^\mathcal{G}$ is thus the field of definition of the orbit-section ideal $I_\mathcal{P}$ and we can consider $I_\mathcal{P}^\mathcal{G} = I_\mathcal{P} \cap \mathbb{K}(z)^\mathcal{G}[Z]$. It is a zero dimensional ideal in $\mathbb{K}(z)^\mathcal{G}[Z]$ and the dimension of $\mathbb{K}(z)^\mathcal{G}[Z]/I_\mathcal{P}^\mathcal{G}$ as a $\mathbb{K}(z)^\mathcal{G}$-vector space is e.

A polynomial $f \in \mathbb{K}(z)^\mathcal{G}[Z]$ defines an element $\bar{f}$ in the quotient $\mathbb{K}(z)^\mathcal{G}[Z]/I_\mathcal{P}$. The multiplication map

$$\begin{array}{rccc} m_f : & \mathbb{K}(z)^\mathcal{G}[Z]/I_\mathcal{P} & \to & \mathbb{K}(z)^\mathcal{G}[Z]/I_\mathcal{P} \\ & \bar{g} & \mapsto & \overline{f\,g} \end{array}$$

is a linear mapping [4, Proposition 4.1]. Note that $m_{fg} = m_f \circ m_g = m_g \circ m_f$. When f is not a zero divisor modulo $I_\mathcal{P}$ then there exists $f_1 \in \mathbb{K}(z)^\mathcal{G}[Z]$ s.t. $f f_1 \equiv 1 \mod I_\mathcal{P}^\mathcal{G}$. It follows that $\det m_f \neq 0$ and $m_{f_1} = (m_f)^{-1}$. We shall thus define $m_{g/f}$ as $m_{g f_1} = m_g (m_f)^{-1}$ when f is not a zero divisor modulo $I_\mathcal{P}^\mathcal{G}$.

$\mathbb{K}[Z]_P$ denotes the localisation of $\mathbb{K}[Z]$ at the complement of P in $K[Z]$. No element of $\mathbb{K}[Z] \setminus P$ are zero divisors modulo $I_\mathcal{P}^\mathcal{G}$. The following is thus well defined.

Definition 3.3 *For $f \in \mathbb{K}[Z]_P$ we consider the characteristic polynomial*

$$f_\mathcal{P}(z,\zeta) = \zeta^e - f_\mathcal{P}^{(1)}(z)\zeta^{e-1} + \ldots + (-1)^j f_\mathcal{P}^{(j)}(z)\,\zeta^{e-j} + \ldots + (-1)^e f_\mathcal{P}^{(e)}(z)$$

of the multiplication map m_f by f in $\mathbb{K}(z)^{\mathcal{G}}[Z]/I^{\mathcal{G}}_{\mathcal{P}}$. The coefficients $f^{(1)}_{\mathcal{P}}(z), \ldots, f^{(e)}_{\mathcal{P}}(z) \in \mathbb{K}(z)^{\mathcal{G}}$ are the symmetrizations *of f w.r.t. the section $\mathcal{P}$.*

Given a reduced Gröbner basis of $I_{\mathcal{P}}$, we can identify a set of monomials that forms a basis of the $\mathbb{K}(z)^{\mathcal{G}}$-vector space $\mathbb{K}(z)^{\mathcal{G}}[Z]/I^{\mathcal{G}}_{\mathcal{P}}$ and explicitely write down the matrix of m_f in this basis. The symmetrizations of f defined above can thus be computed algorithmically. At no additional cost, the symmetrizations $f^{(1)}_{\mathcal{P}}(z), \ldots, f^{(e)}_{\mathcal{P}}(z) \in \mathbb{K}(z)^{\mathcal{G}}$ are written in terms of the generators $\{r_1, \ldots, r_m\}$ of $\mathbb{K}(z)^{\mathcal{G}}$ that are read from the reduced Gröbner basis of $I_{\mathcal{P}}$ according to Theorem 2.6.

Proposition 3.4 *If the coefficients of the reduced Gröbner basis of $I_{\mathcal{P}}$ can be written as polynomials in $\{r_1, \ldots, r_m\} \subset \mathbb{K}(z)^{\mathcal{G}}$ then, for any $f \in \mathbb{K}[Z]$, we can determine polynomials $\tilde{f}^{(j)}_{\mathcal{P}}$, $1 \le j \le e$, in $\mathbb{K}[y_1, \ldots, y_m]$ such that the symmetrizations of f are*

$$f^{(j)}_{\mathcal{P}}(z_1, \ldots, z_n) = \tilde{f}^{(j)}_{\mathcal{P}}\left(r_1(z), \ldots, r_m(z)\right).$$

The case where $\mathcal{P}$ is a section of degree 1 is particularly favorable. Then $I_{\mathcal{P}} = (Z_1 - r_1(z), \ldots, Z_n - r_n(z))$ with $r_1, \ldots, r_n \in \mathbb{K}(z)^{\mathcal{G}}$ and therefore $f_{\mathcal{P}}(z, \zeta) = \zeta - f^{(1)}_{\mathcal{P}}$ with $f^{(1)}_{\mathcal{P}}(z_1, \ldots, z_n) = f\left(r_1(z), \ldots, r_n(z)\right)$.

Example 3.5 Scalings in the plane. *We follow up on Example 2.4. We choose $P = (X^{\alpha} - Y^{\beta})$. It defines a section of degree one and the reduced Gröbner of $I^{\mathcal{G}}_{\mathcal{P}}$ is $B = \left\{X - r^{\beta},\ Y - r^{\alpha}\right\}$ where $r = \frac{y^a}{x^b}$. Thus the symmetrization of f is $f^{(1)}_{\mathcal{P}}(x, y) = f(r^{\beta}, r^{\alpha})$.*

Example 3.6 *Following on Example 2.9 where we considered a linear action of $\mathrm{SO}_2(\overline{\mathbb{K}})$ on $\mathcal{Z} = \overline{\mathbb{K}}^3$ and chose the section defined by $P = (\,X\,)$ so that $I_{\mathcal{P}} = (X,\, Y^2 - r,\, Z - z)$ where $r = x^2 + y^2$.*

Consider the polynomials $f_1 = -x\left(x^2 + y^2 - 1\right) - y\,z$ and $f_2 = -y\left(x^2 + y^2 - 1\right) + x\,z$. Neither f_1 nor f_2 is invariant.

A basis for $\mathbb{K}(x,y)[X,Y]/I_{\mathcal{P}}$ is given by the set of monomials $\{1, Y\}$. In this basis, the multiplication matrix of $f_1(X,Y,Z)$ and $f_2(X,Y,Z)$ are respectively

$$M_1 = \begin{bmatrix} 0 & -z\,r \\ -z & 0 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} 0 & r\,(1-r) \\ 1-r & 0 \end{bmatrix}.$$

Hence

$$f_1^{(1)} = -Tr(M_1) = 0,\ f_1^{(2)} = Det(M_1) = -z^2\,r,$$

and

$$f_2^{(1)} = -Tr(M_2) = 0,\ f_2^{(2)} = Det(M_2) = r\,(1-r)^2.$$

Note that $f^{(1)}_{\mathcal{P}}(z)$ is the trace of m_f and the map $f \mapsto f^{(1)}_{\mathcal{P}} \in \mathbb{K}(z)^{\mathcal{G}}$ is a $\mathbb{K}(z)^{\mathcal{G}}$-linear map. But in general $(\lambda \star f)^{(1)}_{\mathcal{P}} \neq f^{(1)}_{\mathcal{P}}$, contrary to the Reynolds operator.

Example 3.7 *In the case of Example 3.5, $(\lambda \star f)^{(1)}_{\mathcal{P}}(x, y) = f(\lambda^{-a} r^{\beta}, \lambda^{-b} r^{\alpha})$ while $f^{(1)}_{\mathcal{P}}(x, y) = f(r^{\beta}, r^{\alpha})$.*

3.3 Geometric interpretation and connections

Let $\mathcal{W}$ be a proper $\mathcal{G}$-invariant closed set such that for $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$, the specialisation $B_{\bar{z}}$ of B is a Gröbner basis for an ideal whose variety is $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$. We discussed how to determine such a $\mathcal{W}$ in Section 3.1. For $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$ the ideal $(B_{\bar{z}})$ has e zeros $\left\{z^{(1)}, \ldots, z^{(e)}\right\}$. They form $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$, possibly with multiplicities.

Proposition 3.8 *Consider $f \in \mathbb{K}[Z]_P$ and $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$. Let $\{z^{(1)}, \dots, z^{(e)}\}$ be the e zeros of $B_{\bar{z}}$. For $1 \le j \le e$,*

$$f_{\mathcal{P}}^{(j)}(\bar{z}) = S_j\left(f(z^{(1)}), \dots, f(z^{(e)})\right)$$

where S_j is the j-th symmetric polynomial in e variables.

PROOF: The eigenvalues of m_f are the evaluations of f at the roots of $(B_{\bar{z}})$, with matching multiplicities [4, Theorem 4.5]. Hence $f_{\mathcal{P}}(z,\zeta) = \prod_{i=1}^{e}\left(\zeta - f(z^{(j)})\right)$. □

Corollary 3.9 *If $f \in \mathbb{K}(z)^{\mathcal{G}}$ then $f_{\mathcal{P}}^{(j)} = \begin{pmatrix} j \\ e \end{pmatrix} f^j$.*

PROOF: By Proposition 2.1, $\mathbb{K}(z)^{\mathcal{G}} \subset \mathbb{K}[z]_P$ since $\mathcal{P}$ cannot be included in any invariant hypersurface. As an invariant, f is constant on orbits: $f(\bar{z}) = f(z^{(1)}) = \ldots = f(z^{(e)})$ □

The characteristic polynomial $f_{\mathcal{P}}(z,\zeta)$ of the multiplication map m_f is a polynomial in the elimination ideal $(I_{\mathcal{P}} + (\zeta - f(Z))) \cap \mathbb{K}(z)[\zeta]$. It thus corresponds to the *invariantization* defined in [10, Section 2.6] for algebraic functions. The purpose of this latter was to provide a constructive approach to the *local* invariantization process that is central in the moving frame construction of differential invariants and invariant derivations in [6]; [10, Theorem 3.9] makes explicit the connection. The meaning of this theorem in the present context is the following : $f_{\mathcal{P}}(z,\zeta)$ is the defining polynomial of a smooth algebraic function that is the unique *local invariant*[3] that agrees with the values of f on the section $\mathcal{P}$ in the neighborhood of one of its point. Proposition 3.10 below can be seen as a global analogue of a result known locally.

On the other hand, Proposition 3.10 can also be seen as a generalization of the construction known in the case of finite groups. Indeed, in the case where $\mathcal{G}$ is a finite group acting regularly and faithfully, we should consider $\mathcal{P} = \mathcal{Z}$ as the section and its degree e is the order of group $\mathcal{G}$. For $\bar{z} \in \mathcal{Z}$, $\{z^{(1)}, \dots, z^{(e)}\} = \{\lambda \star \bar{z} \,|\, \lambda \in \mathcal{G}\}$. Thus

$$f_{\mathcal{P}}(z) = \zeta^e - f^{(1)}(z)\zeta^{e-1} + \ldots + (-1)^j f^{(j)}(z)\,\zeta^{e-j} + \ldots + (-1)^e f^{(e)}(z) = \prod_{\lambda \in \mathcal{G}} (\zeta - f(\lambda \star z))$$

where $f^{(j)}(z)$ is simply the i-th symmetric function on $\{f(\lambda \star z) \,|\, \lambda \in \mathcal{G}\}$. The symmetrization $f^{(j)}(z)$, for $1 \le j \le e$, are invariant polynomials. As can be read in [24, Proposition 2.6.4], if the variety $\mathcal{V}(F)$ of a finite set of polynomials F is invariant then

$$\mathcal{V}(F) = \mathcal{V}\left(f^{(i)} \,|\, f \in F,\ 1 \le i \le e\right).$$

This proves that any variety invariant under the action of a finite group is the variety of a set of invariant polynomials. The notion of symmetrization w.r.t. a section $\mathcal{P}$ we introduced for algebraic groups of positive dimension allows us to provide an analogous result for the rational action of an algebraic group of positive dimension.

3.4 Polynomial systems with symmetry

It follows from Proposition 3.8 that

$$z \in \mathcal{V}\left(f_{\mathcal{P}}^{(1)}, \dots, f_{\mathcal{P}}^{(e)}\right) \setminus \mathcal{W} \;\Leftrightarrow\; \mathcal{O}_z \cap \mathcal{P} \subset \mathcal{V}(f) \setminus \mathcal{W}.$$

The proof of the following result is then similar to the proof in the case of finite groups. The only caveat is that the result is valid outside of the proper closed set $\mathcal{W}$ determined by the specialisation properties discussed in Section 3.1.

[3] See [10] for the definitions.

Proposition 3.10 *Let F be a set of polynomials in $\mathbb{K}[z]$ and assume that its variety $\mathcal{F}$ is $\mathcal{G}$-invariant. Consider a section $\mathcal{P}$ of degree e. Then*

$$\mathcal{V}\Big(f_{\mathcal{P}}^{(i)} \,|\, f \in F,\ 1 \leq i \leq e\Big) \setminus \mathcal{W} \ = \ \mathcal{F} \setminus \mathcal{W},$$

where $\mathcal{W}$ is the $\mathcal{G}$-invariant variety discussed in Section 3.1.

In the above proposition, $\mathcal{V}\Big(f_{\mathcal{P}}^{(i)} \,|\, f \in F,\ 1 \leq i \leq e\Big)$ stands for the variety of the numerators. The varieties of the denominators arising in $f_{\mathcal{P}}^{(j)}$ actually lies in $\mathcal{W}$ due to Proposition 3.4.

PROOF: For $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$, we note $\left\{z^{(1)}, \ldots, z^{(e)}\right\}$ the zeros of $(B_{\bar{z}})$. Each $z^{(i)}$ belongs to $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$. As $\mathcal{F}$ is $\mathcal{G}$-invariant we thus have $\bar{z} \in \mathcal{F} \setminus \mathcal{W} \Leftrightarrow \left\{z^{(1)}, \ldots, z^{(e)}\right\} \subset \mathcal{F} \setminus \mathcal{W}$.

Since

$$\prod_{j=1}^{e} \left(\zeta - f(z^{(j)})\right) = \zeta^e - f_{\mathcal{P}}^{(1)}(\bar{z})\zeta^{e-1} + \ldots + (-1)^j f_{\mathcal{P}}^{(j)}(\bar{z})\,\zeta^{e-j} + \ldots + (-1)^e f_{\mathcal{P}}^{(e)}(z)$$

we have $\left(f(z^{(1)}) = 0, \ldots, f(z^{(e)}) = 0\right) \Leftrightarrow \left(f^{(j)}(\bar{z}) = 0, \forall\ 1 \leq j \leq e\right)$. □

The above proposition combined with Proposition 3.4 thus allows us to provide the following general statement that is the main claim of this article.

Theorem 3.11 *Assume $\mathcal{P}$ is a section of degree e to the orbits of the rational action of an algebraic group $\mathcal{G}$ on $\mathcal{Z}$. We can determine a $\mathcal{G}$-invariant algebraic set $\mathcal{W}$ and $r_1, \ldots, r_m \in \mathbb{K}(z)^{\mathcal{G}}$ such that $\mathbb{K}(z)^{\mathcal{G}} = \mathbb{K}(r_1, \ldots, r_m)$ with the following properties: If the variety $\mathcal{V}(F)$ of a finite set of polynomials F in $\mathbb{K}[z]$ is $\mathcal{G}$-invariant then there exists a finite set of polynomials $\tilde{F} \subset \mathbb{K}[y_1, \ldots, y_m]$ such that for any $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$*

$$f(\bar{z}) = 0,\ \forall f \in F \quad \Leftrightarrow \quad \tilde{f}\,(r(\bar{z})) = 0,\ \forall \tilde{f} \in \tilde{F}.$$

Several examples of polynomial systems whose varieties are invariant under a scaling were treated in [11]. These include system of polynomials that are multi-homogeneous according to a set of weights. Indeed [11, Theorem 5.3] can be seen as a special case of the above results.

Example 3.12 *Following on Example 2.9, 3.2 and 3.6, one observes that $\mathcal{V}(f_1, f_2)$ is invariant under the action of $\mathrm{SO}_2(\overline{\mathbb{K}})$ since $(f_1, f_2)^t$ is an equivariant map. We determined that outside $\mathcal{W} = \mathcal{V}\big(x^2 + y^2\big)$ the reduced Gröbner basis of $I_{\mathcal{P}}$ specialises to the reduced Gröbner basis of the intersection of the orbit of that point with the section $\mathcal{P}$. Applying the above construction we obtain*

$$\mathcal{V}(f_1, f_2) \setminus \mathcal{W} = \mathcal{V}\Big(f_1^{(1)},\, f_1^{(2)},\, f_2^{(1)},\, f_2^{(2)}\Big) \setminus \mathcal{W} = \mathcal{V}\big(z^2,\, (x^2 + y^2 - 1)^2\big).$$

Note that when the action is given by an orthogonal representation of the group and F consists of the components of an equivariant map there is an alternative approach to produce a system of polynomial invariants whose real variety is equal to the real variety of F [7, 13, 27], [8, Lemma 4.1.4]

Example 3.13 *Consider the action of SL_2 on the vector space of 2×2 matrices M_2:*

$$\begin{array}{ccc} \mathrm{SL}_2 \times \mathrm{M}_2 & \to & \mathrm{M}_2 \\ (a, z) & \mapsto & a\,z\,a^{-1} \end{array}$$

We write

$$z = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix} \quad \text{and} \quad Z = \begin{bmatrix} Z_{11} & Z_{12} \\ Z_{21} & z_{22} \end{bmatrix}.$$

and consider the section defined $P = (Z_{11},\ Z_{21}-1)$*. It is a section of degree* 1 *: The Gröbner basis of the orbit-section ideal is*

$$Q = (Z_{11},\ Z_{21}-1,\ Z_{22}-t,\ Z_{21}+d) \quad \text{where} \quad t = z_{11}+z_{22}, \ \text{ and } \ d = z_{22}\,z_{11}-z_{12}\,z_{21}.$$

One recognizes the invariants to be the trace and the determinant of z*. One checks that the Gröbner basis specializes well everywhere. Hence* $\mathcal{W}=\varnothing$*.*

Consider the set F *consisting of the three polynomials*

$$16\,z_{21}z_{12}+8\,{z_{11}}^2+8\,{z_{22}}^2-9, \quad 8\,z_{11}z_{12}z_{21}-8+24\,z_{22}z_{12}z_{21}-8\,{z_{22}}^2z_{11}+8\,{z_{22}}^3+9\,z_{11},$$
$$128\,{z_{21}}^2{z_{12}}^2-81+512\,{z_{22}}^2z_{21}z_{12}-256\,{z_{22}}^3z_{11}+128\,{z_{22}}^4+72\,z_{21}z_{12}+216\,z_{11}z_{22}+144\,{z_{22}}^2+64\,z_{11}-192\,z_{22}.$$

The polynomials are not invariant, except for the first one. Yet, by construction, we know that the variety of F *is invariant -* F *is actually a Gröbner basis for the ideal* $\left(8\,\mathrm{tr}(z^2)-9,\ \mathrm{tr}(z^3)-1\right)$*. By Proposition 3.10 the variety of* F *is equal to the variety of*

$$\tilde{F} = \left\{8\,t^2-16\,d-9,\ 8\,t^3-8-24\,td,\ 128\,d^2-81-512\,t^2d+128\,t^4-72\,d+144\,t^2-192\,t\right\}.$$

where $\tilde{F}$ *is simply obtained from* F *with the substitution dictated by* Q*, that is*

$$z_{11}\to 0, \quad z_{21}\to 1, \quad z_{22}\to t, \quad z_{21}\to -d.$$

A Gröbner basis for $(\tilde{F})$ *considered as an ideal in* $\mathbb{K}[t,d]$*, is given by:* $(\tilde{F}) = \left(16-27\,t+8\,t^3, 16\,d+9-8\,t^2\right)$.

The above generalizes to SL_n *acting on the the vector space of* $n\times n$ *matrices* M_n*. The invariants* $r_1 = -\mathrm{tr}(z), \ldots, r_n = (-1)^n\det(z)$ *are the coefficients of the characteristic polynomial of* $z = (z_{ij})_{1\le i,j\le n}$*. Any polynomial system whose variety is invariant is equivalent to a system of polynomials in* $r_1,\ldots,r_n$ *that is obtained by applying the following substitution:*

$$[Z_{ij}]_{1\le i,j\le n} \longrightarrow \begin{bmatrix} 0 & 0 & \ldots & 0 & -r_n \\ 1 & 0 & \ldots & 0 & -r_{n-1} \\ \vdots & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & & 1 & -r_n \end{bmatrix}.$$

The right hand side corresponds to the Frobenius normal form of $(z_{ij})_{1\le i,j\le n}$ *in the generic case.*

As illustrated in the previous example, our construction is particularly practical when we have a section of degree 1. In this case, the equivalent invariant system is obtained by a simple substitution. The set $\tilde{F}$ has thus the same number of elements as F and is of similar degree when looked as a system in the generating invariants.

Let us conclude by noting that Theorem 3.11 could be extended to invariant semi-algebraic set $\mathcal{K} = \{x\in\mathbb{R}^n \,|\, f_1(x)\ge 0,\ \ldots,\ f_m(z)\ge 0\}$ if we could ensure that the orbits in $\mathcal{K}\cap\mathcal{W}$ intersect the section $\mathcal{P}$ in e points (counting multiplicities), *i.e.* the intersection points are not complex. This is the case in the two examples above, or any time we have a section of degree 1 defined over $\mathbb{R}$. The argument of [2, Proposition 3.15] that addresses finite groups would indeed generalize to the present context thanks to the analogy drawn in Section 3.3 between the finite group case and the case of algebraic group of positive dimension.

References

[1] L. Bröcker. On symmetric semialgebraic sets and orbit spaces. In *Singularities Symposium—Łojasiewicz 70 (Kraków, 1996; Warsaw, 1996)*, volume 44 of *Banach Center Publ.*, pages 37–50. Polish Acad. Sci., Warsaw, 1998.

[2] J. Cimprič, S. Kuhlmann, and C. Scheiderer. Sums of squares and moment problems in equivariant situations. *Trans. Amer. Math. Soc.*, 361(2):735–765, 2009.

[3] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. An introduction to computational algebraic geometry and commutative algebra.

[4] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[5] H. Derksen and G. Kemper. *Computational invariant theory*. Springer-Verlag, 2 edition, 2015. Encyclopaedia of Math. Sc., 130.

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

[7] K. Gatermann. Semi-invariants, equivariants and algorithms. *Appl. Algebra Engrg. Comm. Comput.*, 7(2):105–124, 1996.

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

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

[10] E. Hubert and I. Kogan. Smooth and algebraic invariants of a group action. Local and global constructions. *Foundations of Computational Mathematics*, 7(4):355–393, 2007.

[11] E. Hubert and G. Labahn. Rational invariants of scalings from Hermite normal forms. In *ISSAC 2012*, pages 219–226. ACM Press, 2012.

[12] E. Hubert and G. Labahn. Scaling invariants and symmetry reduction of dynamical systems. *Foundations of Computational Mathematics*, 13(4):479–516, 2013.

[13] M. V. Jarić, L. Michel, and R. T. Sharp. Zeros of covariant vector fields for the point groups: invariant formulation. *J. Physique*, 45(1):1–27, 1984.

[14] M. Kalkbrener. On the stability of Gröbner bases under specializations. *J. Symbolic Comput.*, 24(1):51–58, 1997.

[15] D. Kapur, Y. Sun, and D. Wang. An efficient method for computing comprehensive Gröbner bases. *Journal Symbolic Computation*, 52:124–142, 2013.

[16] D. Lazard and F. Rouillier. Solving parametric polynomial systems. *Journal of Symbolic Computation*, 42(6):636–667, 2007.

[17] A. Montes and M. Wibmer. Gröbner bases for polynomial systems with parameters. *J. Symbolic Comput.*, 45(12):1391–1425, 2010.

[18] A. Montes and M. Wibmer. Software for discussing parametric polynomial systems: the Gröbner cover. In *Mathematical software—ICMS 2014*, volume 8592 of *Lecture Notes in Comput. Sci.*, pages 406–413. Springer, Heidelberg, 2014.

[19] G. Moroz. Complexity of the resolution of parametric systems of polynomial equations and inequations. In *ISSAC 2006*, pages 246–253. ACM, New York, 2006.

[20] G. Moroz. Properness defects of projection and minimal discriminant variety. *J. Symbolic Comput.*, 46(10):1139–1157, 2011.

[21] A. N. Parshin and I. R. Shafarevich, editors. *Algebraic Geometry. IV*, volume 55 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1994.

[22] V. Popov and E. Vinberg. Invariant theory. In *Algebraic geometry. IV*, pages 122–278. Springer, 1994.

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

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

[25] V. Weispfenning. Comprehensive Gröbner bases. *J. Symbolic Comput.*, 14(1):1–29, 1992.

[26] M. Wibmer. Gröbner bases for families of affine or projective schemes. *Journal of Symbolic Computation*, 42(8):803 – 834, 2007.

[27] P. A. Worfolk. Zeros of equivariant vector fields: algorithms for an invariant approach. *J. Symbolic Comput.*, 17(6):487–511, 1994.