Gröbner Bases, Invariant Theory and Equivariant Dynamics

KARIN GATERMANN[†§] AND FRÉDÉRIC GUYARD[‡¶]

[†]*Konrad-Zuse-Zentrum, Takustr. 7, D-14195 Berlin, Germany,* or *Inst. für Math. I,*
FU Berlin, Arnimallee 2-6, D-14195 Berlin, Germany
[‡] *Universite de Nice-Antipolis, Institut Non Linéaire de Nice, 1361 Rte des Lucioles,*
Sophia-Antipolis, F-06560 Valbonne, France

This paper is about algorithmic invariant theory as it is required within equivariant
dynamical systems. The question of generic bifurcation equations (arbitrary equivariant
polynomial vector) requires the knowledge of fundamental invariants and equivariants.
We discuss computations which are related to this for finite groups and semi-simple Lie
groups. We consider questions such as the completeness of invariants and equivariants.
Efficient computations are gained by the Hilbert series driven Buchberger algorithm
because computation of elimination ideals is heavily required. Applications such as orbit
space reduction are presented.

© 1999 Academic Press

1. Introduction

This paper deals with algorithmic invariant theory with an emphasis on efficiency of the
involved algorithms. Elimination ideals are computed with Gröbner bases (Buchberger,
1985). When a given group action is considered, it is often needed to solve the following
problems.

A. Given a set of homogeneous invariants:

   (1) What are the relation in the invariants? (This knowledge is needed for the
       subsequent questions)
   (2) Does the set of invariants generate the invariant ring?
   (2b) Do the homogeneous invariants generate the ring up to a certain degree?
   (3) How is a given invariant represented in terms of fundamental invariants?
   (3b) How is the given invariant represented if the fundamental invariants form a
       Hironaka decomposition?

B. Given a set of homogeneous invariants $\pi_1, \ldots, \pi_r$ and a set of homogeneous equi-
   variants $b_1, \ldots, b_s$.

   (1) What are the relations?

[§]E-mail: `gatermann@zib.de`
[¶]E-mail: `guyard@doublon.unice.fr`

(2) Do the given equivariants generate the module of equivariants over the ring generated by the given invariants $\pi_1, \ldots, \pi_r$?

(2b) Is the module generated up to a certain degree?

(3) How does one represent a given equivariant in terms of fundamental invariants and equivariants?

C. Given a representation of a finite group.

(1) How can one determine the fundamental invariants algorithmically such that they form a Hironaka decomposition? (This means that for each invariant there is a unique representation in terms of fundamental invariants which is linear in the secondary invariants.)

(2) How does one determine the fundamental equivariants such that they form a free module over the ring generated by the primary invariants?

D. Given a representation of a compact Lie group. The groups one is interested in dynamical systems are linear reductive groups. Their invariant ring is Cohen–Macaulay, see Bruns and Herzog (1993) and Hochster and Roberts (1974).

(1) How can one compute a homogeneous invariant for a given degree? (Observe that the Reynolds operator for finite groups (projection onto invariants) does not exist or can not be evaluated for continuous groups in this form.)

(2) How can one compute a fundamental set of invariants?

(3) How can one modify a fundamental set of invariants into a Hironaka decomposition? Then each invariant can be written in terms of the fundamental invariants in a unique way.

(4) How does one determine a homogeneous equivariant of a given degree?

(5) How can one compute a generating set of equivariants over a ring generated by a given set of invariants?

(6) Given a set of fundamental invariants and equivariants, how is a Stanley decomposition determined?

There is a lot of information in the literature about all these questions. Table 1 gives an overview of implementations and summarizes the relevant books and articles so far as to whether they contain efficient algorithms. The packages *Invar* (Kemper, 1993) and *Symmetry* (Gatermann and Guyard, 1997) are implemented in Maple while implementations for C. 1.) in Singular (Heydtmann, 1997) and Magma (Kemper and Steel, 1997) exist as well.

The new contributions of this paper are the use of the *multi-graded Hilbert series driven Buchberger algorithm* (Caboara *et al.*, 1996; Gianni *et al.*, 1996) for computation of relations, completeness of equivariants (B. 2), restriction of completeness to certain degree (A. 2b, B. 2b), and membership of free module. Restriction with respect to various gradings is the key for efficiency in the partial completeness questions. This is illustrated by examples which have been computed on a Dec Alpha workstation. These new ideas mainly improve the efficiency of existing algorithms. The algorithmic treatment for continuous groups has been implemented and tested for the first time.

A motivation of this work and the associated software was to provide *efficient* tools to perform tasks as they arise in equivariant bifurcation theory, equivariant dynamics,

Table 1. Literature containing algorithms answering questions in invariant theory and their implementations.

Question	Task	Literature	Invar	Symmetry
A.	Given invariants			
(1)	Relations	Becker and Weispfenning (1993, p. 269)	x	x
(2)	Generation	Sturmfels (1993, p. 32)	x	x
(2b)			x	x
(3)	Representation	Becker and Weispfenning (1993, p. 269)	x	x
(3b)	Hironaka repr.	Sturmfels (1993, p. 52)	x	x
B.	Given invs. + equis.			
(1)	Relations			x
(2)	Generation			x
(2b)				x
(3)	Representation	Gatermann (1996b, p. 115)		x
C.	Given finite group			
(1)	Compute invs.	Sturmfels (1993, p. 57), Kemper (1996)	x	x
(2)	Compute equis.	Worfolk (1994), Gatermann (1996b)		x
D.	Given Lie group			
(1)	Reynolds projection			x
(2)	Compute invs.			x
(3)	Compute parameters	Eisenbud and Sturmfels (1994)		
(4)	Equiv. projection			x
(5)	Compute equis.			x
(6)	Stanley decomposition	Sturmfels and White (1991)		

exact solution of symmetric systems of equations by elimination methods, etc. Indeed, these domains appear to be a natural application of algorithmic invariant theory:

(i) The first step in equivariant bifurcation theory (Golubitsky *et al.*, 1988) is to set up a *generic equivariant vector field* (the bifurcation equations) for a given action of a group. In order to build these equation, one needs nothing else but a set of generators of the module of equivariants for this action. On the theoretical level the famous theorems by Schwarz and Poénaru are an essential ingredient, see Golubitsky *et al.* (1988, p. 46 and p. 51). Examples of local bifurcation theory are presented in Lari-Lavassani *et al.* (1997) and a singularity theory approach is done in Gatermann and Lauterbach (1998).

(ii) A special method in equivariant dynamics is known as *orbit space reduction*. The solutions of a differential equation with symmetry are linked to the solutions of a system of differential equations for a set of fundamental invariants. By this method the group action is ruled out. Although the reduction leads to differential equations on an algebraic variety (restricted to a semi-algebraic set) it has been applied successfully (Chossat, 1993; Chossat and Dias, 1995; Lauterbach and Sanders, 1995; Leis, 1995) because the number of differential equations is often smaller than in the original system. For theoretical results see also Koenig (1997) and Rumberger and Scheurle (1996). The reduced phase space in Hamiltonian systems is similar to the orbit space above.

(iii) Systems of algebraic equations can be solved by the Gröbner basis method such that all solutions are found exactly. If symmetry is present the use of invariant theory is helpful, see Sturmfels (1993, p. 58). In case one is interested in real solutions only, one might as well consider a result involving the fundamental equivariants, see Gatermann (1996b), Jaric *et al.* (1984) and Worfolk (1994).

For these reasons, the examples and applications in the paper are mainly related to problems occurring in equivariant dynamics. As a tool we use Gröbner bases for the computation of elimination ideals (Buchberger, 1985).

2. Preliminaries: Computations with Ideals and Modules

This section gives an overview of the computations including Gröbner bases. They are necessary in order to understand the sections on algorithmic invariant theory. Moreover, we are using a special variant which proves to be very efficient. For those who want to learn more about it we refer to Becker and Weispfenning (1993), Caboara *et al.* (1996), Cox *et al.* (1992), Mishra (1993), and the references therein.

2.1. GRÖBNER BASES AND SYZYGIES

We are dealing with ideals in a polynomial ring $K[x_1, \ldots, x_n]$ where the field K is in most practical computations $\mathbb{Q}$. A Gröbner basis is a special ideal basis depending on an order of the monomials.

DEFINITION 2.1. (BECKER AND WEISPFENNING, 1993, P. 189) $\leq$ is called a term order, if $\forall x^\alpha, x^\beta, x^\gamma \in K[x_1, \ldots, x_n]$

$$
\begin{aligned}
x^\alpha &\leq x^\alpha \\
x^\alpha &\leq x^\beta \quad \text{and} \quad x^\beta \leq x^\gamma \quad \Rightarrow \quad x^\alpha \leq x^\gamma \\
x^\alpha &\leq x^\beta \quad \text{and} \quad x^\beta \leq x^\alpha \quad \Rightarrow \quad x^\alpha = x^\beta \\
x^\alpha &\leq x^\beta \quad \text{or} \quad x^\beta \leq x^\alpha \\
1 &\leq x^\alpha \\
x^\alpha &\leq x^\beta \quad \Rightarrow \quad x^\alpha x^\gamma \leq x^\beta x^\gamma.
\end{aligned}
$$

EXAMPLE 2.2. Let the matrix $M \in \mathbb{Z}^{n,n}$ have the following properties:

(i) for each column j the first nonzero entry is positive.

$$\forall j \exists k \text{ with } m_{ij} = 0 \quad \forall i < k \quad \text{and} \quad m_{kj} > 0$$

(ii) M has full rank.

By $M\alpha < M\beta$ ($\Leftrightarrow \exists k$ with $(M\alpha)_i = (M\beta)_i \ \forall i < k, (M\alpha)_k < (M\beta)_k$) is a term order defined. Although term orders might be defined in a different way they are almost all equivalent to such a matrix order (Robbiano, 1985; Weispfenning, 1987).

For a polynomial $f \in K[x]$ we denote by $ht(f)$ its leading term, i.e. the monomial with highest order and nonvanishing coefficient $hc(f)$ in f:

$$f = hc(f) \cdot ht(f) + \text{lower order terms.}$$

DEFINITION 2.3. An ideal basis $\{f_1, \ldots, f_m\}$ of $I = (f_1, \ldots, f_m)$ is called a Gröbner basis, if the ideal of the leading terms equals the ideal generated by all leading terms of elements of I:

$$(ht(f_1), \ldots, ht(f_m)) = (ht(f))_{f \in I}.$$

So, the theory of Gröbner bases is closely related to the theory of monomial ideals. Gröbner bases are used to solve systems of equations. From a mathematical point of view it is even more important that the quotient ring $K[x]/I$ with respect to a term order has unique representatives which are computable by a division algorithm modulo on a Gröbner basis. The division algorithm is defined for a set of polynomials F. Then $normalf(f, F)$ or short $\bar{f}^F$ denotes the result of the division applied to f and is called *normal form*. The result may still depend on how the division is done. It is an important fact that the result of the division algorithm modulo a Gröbner basis is unique.

DEFINITION 2.4. A Gröbner basis $\{f_1, \ldots, f_m\}$ such that $\{ht(f_1), \ldots, ht(f_m)\}$ forms a minimal basis of the monomial ideal and the f_i are inter-reduced is called a *reduced Gröbner basis*.

A reduced Gröbner basis is unique. Although there exists infinitely many term orders for each ideal only a finite number of reduced Gröbner basis exists (Bayer and Morrison, 1988; Mora and Robbiano, 1988; Sturmfels, 1996).

DEFINITION 2.5. Given a set $F = \{f_1, \ldots, f_m\}$ with leading terms $ht(f_i)$ a *syzygy* is a tuple $(s_1, \ldots, s_m) \in K[x]^m$ such that

$$\sum_{i=1}^{m} s_i \cdot hc(f_i) ht(f_i) = 0.$$

The set of all syzygies form a $K[x]$-module denoted by $S(F)$. Each syzygy s corresponds to a polynomial in the ideal generated by F by defining $s \cdot F = \sum_{i=1}^{m} s_i f_i$. The Buchberger algorithm is based on the fact that special sparse syzygies

$$S^{ij} \in S(F), \qquad 1 \le i < j \le m, \tag{2.1}$$

form a module basis, where $S_k^{ij} = 0, \ \forall k \ne i, k \ne j$, and

$$S_i^{ij} = \frac{\operatorname{lcm}(ht(f_i), \ ht(f_j))}{ht(f_i)} lc(f_j), \qquad S_j^{ij} = -\frac{\operatorname{lcm}(ht(f_i), \ ht(f_j))}{ht(f_j)} lc(f_i).$$

$S(f_i, f_j) := S^{ij} \cdot F$ is called *S-polynomial*.
   F is a Gröbner basis if

$$normalf(s \cdot f, F) = 0, \qquad \forall s \in S(F).$$

This condition is satisfied if it holds for a module basis of $S(F)$, e.g. for the basis $S^{ij}, 1 \le i < j \le m$. It turns out that S^{ij} do not form a minimal basis. Some can be dropped by the Buchberger criteria.

(1) BUCHBERGER CRITERION: If $ht(f_i), ht(f_j)$ are coprime then S^{ij} is superfluous.

(2) BUCHBERGER CRITERION: If $ht(f_j) \operatorname{lcm}(ht(f_i), ht(f_k))$ and S^{ij}, S^{jk} are considered then S^{ik} is superfluous.

2.2. GRADED RINGS AND GRADED MODULES

DEFINITION 2.6. (EISENBUD, 1995, P. 25) A ring is called *graded* if a direct sum decomposition $R = \bigoplus_{i=0}^{\infty} R_i$ exists such that

$$R_i \cdot R_j \subseteq R_{i+j},$$

holds for all $i, j \in \mathbb{N}$.

EXAMPLE 2.7. The polynomial ring $K[x]$ with the usual degree is a graded ring. Besides this natural grading there are other gradings: let $w_1, \ldots, w_n \in \mathbb{N}$ be weights on the variables $x_1, \ldots, x_n$. $(W : \{x_1, \ldots, x_n\} \to \mathbb{N}, W(x_i) = w_i)$. The *weighted degree* is defined by

$$\deg_W(x^\alpha) = \sum_{i=1}^{n} w_i \alpha_i.$$

Polynomials $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ with the property $\deg_W(x^\alpha)$ equal for all $\alpha \in A$ are called W-*homogeneous*. Homogeneous polynomials of a certain degree form vector spaces yielding the graded structure

$$K[x] = \bigoplus_{i=0}^{\infty} H_i^W(K[x]).$$

The weights $1, \ldots, 1$ refer to the natural grading. All gradings of $K[x]$ are given in this way (Becker and Weispfenning, 1993, p. 467). If all $w_i > 0$ then $H_0^W(K[x]) = K$ and all K-vector spaces $H_i^W(K[x])$ have finite dimension.

Of course a ring may be graded several times.

DEFINITION 2.8. (EISENBUD, 1995, P. 42) Let R be a graded ring. A module M is called graded, if it is the direct sum $M = \bigoplus_{j=0}^{\infty} M_j$ such that $R_i M_j \subset M_{i+j} \forall i, j \in N$.

EXAMPLE 2.9. (i) Let $K[x_1, \ldots, x_n]$ be graded with weights $w_1, \ldots, w_n$. If $z_1, \ldots, z_m$ are additional variables then $\Gamma : \{x_1, \ldots, x_n, z_1, \ldots, z_m\} \to \mathbb{N}$

$$\Gamma(x_i) = 0, \ i = 1, \ldots, n, \qquad \Gamma(z_j) = 1, j = 1, \ldots, m,$$

defines a grading on $K[x_1, \ldots, x_n, z_1, \ldots, z_m]$ yielding

$$K[x, z] = \bigoplus_{i=0}^{\infty} H_i^\Gamma(K[x, z]).$$

Each $H_i^\Gamma(K[x, z])$ is a $K[x]$-module. $H_1^\Gamma(K[x, z])$ is especially interesting because each finitely generated, free $K[x]$-module is isomorphic to a $H_1^\Gamma(K[x, z])$.
The grading W on $K[x]$ may be extended to $K[x, z]$ by weights on z_j:

$$\Theta : \{z_1, \ldots, z_m\} \to N, \Theta_{|K[x]} = W.$$

A restriction is a grading of the module $H_1^\Gamma(K[x, z])$:

$$K[x, z] = \bigoplus_{k=0}^{\infty} H_k^\Theta(K[x, z]), \tag{2.2}$$

$$H_1^\Gamma(K[x,z]) = \bigoplus_{k=0}^\infty H_{1,k}^{\Gamma,\Theta}(K[x,z]) \qquad \text{with } H_{1,k}^{\Gamma,\Theta}(K[x,z]) = H_1^\Gamma(K[x,z]) \cap H_k^\Theta(K[x,z]).$$

$$(2.3)$$

(ii) A second example for a graded module is an ideal I of a Θ-graded ring $K[x]$ which is generated by Θ-homogeneous polynomials.

DEFINITION 2.10. A Θ-*homogeneous ideal* I of $K[x]$ where $K[x]$ is Θ-graded, is an ideal which respects the grading, i.e. is a Θ-graded module.

For each Θ-homogeneous ideal I the quotient ring $K[x]/I$ is a graded module over $K[x]$ as well.

DEFINITION 2.11. (ATIYAH AND MACDONALD, 1969, P. 116) Let M be a finitely generated, graded module ($M = \bigoplus_{i=0}^\infty M_i$) over a Noetherian graded ring $R = \bigoplus_{i=0}^\infty R_i$ such that $R_0 = K$ is a field. Then

$$\mathcal{HP}(\lambda) = \sum_{i=0}^\infty \dim(M_i)\lambda^i,$$

is called the Hilbert–Poincaré series of M. Here $\dim(M_i)$ denotes the dimension of the K-vector space M_i.

If M is multi-graded the multiple Hilbert series is defined in a similar way.

DEFINITION 2.12. (CABOARA ET AL., 1996) A tuple of gradings $(W_1, \ldots, W_r)$ of $K[x]$ is a *weight system* if for all $i = 1, \ldots, n$ exists $j \in \{1, \ldots, r\}$ with $W_j(x_i) > 0$.

EXAMPLE 2.13. If $K[x]$ is graded by W such that all values $W(x_i) = w_i$ are positive then this grading is a weight system. Then all K-vector spaces $H_i(K[x]/I)$ have finite dimension which equals the codimension of $H_i(I)$ in $H_i(K[x])$. Thus the Hilbert series $\mathcal{HP}_{K[x]/I}^W$ is well defined.

For monomial ideals the corresponding Hilbert series (single graded or multi-graded) may be computed by an algorithm described in Bayer and Stillman (1992). It is implemented in Macaulay and in Maple in the moregroebner package (Gatermann, 1996a). The input consists of a finite set of monomials and a list of gradings forming a weight system.

It is an important and well-known fact about Gröbner bases that they enable the computation of Hilbert series of homogeneous ideals as was already pointed out in Buchberger (1965).

LEMMA 2.14. (MACAULAY, 1927) *Let* $(W_1, \ldots, W_r)$ *be a weight system for* $K[x]$ *and* I *a* W-*homogeneous ideal. Let* $LT(I)$ *be the monomial ideal generated by all leading terms* $ht(f)$ *of* $f \in I$ *with respect to a term order of* $K[x]$. *Then the Hilbert series of* I *and* $LT(I)$ *are equal.*

As the leading terms $\{ht(f), f \in \mathcal{GB}\}$ of a Gröbner basis $\mathcal{GB}$ generate the monomial ideal $LT(I)$ the series $\mathcal{HP}_{K[x]/I}$ is easily computed.

2.3. Hilbert series driven Buchberger algorithm

DEFINITION 2.15. Let $U = \{U_1, \ldots, U_r\}$ be a set of gradings of $K[x]$ and I a homogeneous ideal with respect to U. Let $d \in \mathbb{N}^r$ be a fixed degree. A finite set of U-homogeneous polynomials $F \subset I$ is called a d-truncated Gröbner basis of I with respect to U and denoted by $\mathcal{GB}(\bigoplus_{j \leq d} H_j^U(I))$, if

$$\{ht(f) \mid f \in F \text{ and } \deg_{U_i}(f) \leq d_i, i = 1, \ldots, r\},$$

generates (as an ideal, but restricted in degree)

$$\bigcap_{i=1}^{r} \bigoplus_{j_i=0}^{d_i} H_{j_i}^{U_i}(LT(I)) = \bigoplus_{j \leq d} H_j^U(LT(I)).$$

Observe that this definition only makes sense for homogeneous ideals and that there is no restriction on the term order.

This definition is useful in at least two ways.

DEFINITION 2.16. (BECKER AND WEISPFENNING, 1993) Consider $K[x, z]$ with the grading $\Gamma(x_i) = 0, \Gamma(z_j) = 1$. A *module Gröbner basis* of a submodule of $H_1^\Gamma(K[x, z])$ is a truncated Gröbner basis of degree 1 with respect to Γ.

LEMMA 2.17. *Let $U = \{U_1, \ldots, U_r\}$ be a set of gradings of $K[x]$ and $d \in \mathbb{N}^r$ a fixed degree. Assume $\mathcal{GB} \subset K[x]$ is a d-truncated Gröbner basis of a U-homogeneous ideal I with respect to U. Let $f \in K[x]$ be a polynomial with $\deg_{U_i}(f) \leq d_i, i = 1, \ldots, r$. Then*

$$f \in I \Leftrightarrow normalf(f, \mathcal{GB}) = 0.$$

This is the generalization of Theorem 10.39, p. 471 in Becker and Weispfenning (1993) from one grading to multiple grading.

The gradings $U = \{U_1, \ldots, U_r\}$ give rise to gradings on the module of syzygies $S(F)$ for a set $F = \{f_1, \ldots, f_m\}$ in the following way:

$$S \in H_{j_1 \ldots j_r}^{U_1 \ldots U_r}(S(F)) :\Leftrightarrow S_k \cdot ht(f_k) \in H_{j_1 \ldots j_r}^{U_1 \ldots U_r}(K[x]), \qquad k = 1, \ldots, m.$$

The syzygies S^{kl} as defined in (2.1) are especially homogeneous of degree

$$\deg_U(\operatorname{lcm}(ht(f_k), ht(f_l))).$$

If the Hilbert series in known information on the structure of the ideal is available it is exploited in order to gain efficiency. Superfluous S-polynomials may be dropped.

THEOREM 2.18. *Let $U = \{U_1, \ldots, U_r\}$ be a set of gradings of $K[x]$ and the gradings $W = (W_1, \ldots, W_s)$ be a weight system of $K[x]$. Let $I \subset K[x]$ be an ideal which is U-homogeneous and W-homogeneous. Let $d \in \mathbb{N}^r$ be a degree, $F = \{f_1, \ldots, f_m\} \subset I$ a set of U-homogeneous, W-homogeneous polynomials. Assume the Hilbert series $\mathcal{HP}_{K[x]/I}^W(\lambda) = \sum_{i \in \mathbb{N}^s} a^i \lambda^i$ is given. Let the Hilbert series of $(LT(F))$ be denoted by $\mathcal{HP}_{K[x]/(LT(F))}^W(\lambda) = \sum_{i \in \mathbb{N}^s} b^i \lambda^i$. Assume for all degrees $i \in \mathbb{N}^s$*

$$a^i = b^i \qquad or \qquad for \; all \; syzygies \; S := S^{kl}$$

with

$$\deg_{U_j}(S) \le d_j, j = 1, \ldots, r,$$

and

$$\deg_{W_\nu}(S) \le i_\nu, \nu = 1, \ldots, s \qquad normalf(S \cdot F, F) = 0.$$

Then F is a d-truncated Gröbner basis of I with respect to U.

PROOF. In order to show that F is a d-truncated Gröbner basis we need to show that for all $j \le d$

$$\forall S \in H_j^U(S(F)) \quad normalf(S \cdot F, F) = 0 \quad \text{holds.}$$

We take advantage of the weight system W and look at the decomposition

$$H_j^U(S(F)) = \bigoplus_{i \in \mathbb{N}^s} H_{i,j}^{W,U}(S(F)).$$

We need to show for all $j \le d$ and all $i \in \mathbb{N}^s$

$$\forall S \in H_{i,j}^{W,U}(S(F)) \quad normalf(S \cdot F, F) = 0 \quad \text{holds.} \tag{2.4}$$

Consider one fixed pair (i, j). The vector space $H_{i,j}^{W,U}(S(F))$ is part of a module which is generated by the syzygies S^{kl}. Only syzygies S^{kl} of degree $\deg_U(S^{kl}) \le j \le d$ and $\deg_W(S^{kl}) \le i$ generate elements in $H_{i,j}^{W,U}(S(F))$. This implies: if $normalf(S \cdot F, F) = 0$ for all S^{kl} of degree $\deg_U(S^{kl}) \le j \le d$ and $\deg_W(S^{kl}) \le i$ then for all $S \in H_{i,j}^{W,U}(S(F))$ $normalf(S \cdot F, F) = 0$ holds. So condition (2.4) is satisfied for this particular pair (i, j). But there is a second possibility to check condition (2.4) which avoids the computation of the normal forms of S-polynomials. This argumentation uses a second decomposition

$$H_i^W(S(F)) = \bigoplus_{\nu \in \mathbb{N}^r} H_{i,\nu}^{W,U}(S(F)). \tag{2.5}$$

We are interested in the case $\nu = j$ for the moment. Considering the two Hilbert series $\mathcal{HP}_{K[x]/I}^W(\lambda) = \sum_{i \in \mathbb{N}^s} a^i \lambda^i$ and $\mathcal{HP}_{K[x]/(LT(F))}^W(\lambda) = \sum_{i \in \mathbb{N}^s} b^i \lambda^i$ the equality of dimensions $a^i = b^i$ implies

$$\forall S \in H_i^W(S(F)) \quad normalf(S \cdot F, F) = 0.$$

The decomposition (2.5) tells us that particularly for $\nu = j$

$$\forall S \in H_{i,j}^{W,U}(S(F)) \quad normalf(S \cdot F, F) = 0,$$

which is condition (2.4). Since the argumentation is similar for all degrees (i, j) with $j \le d$ and we used only the assumptions in the theorem the proof is complete. $\square$

An implementation using this theorem motivated by the nontruncated version of the multi-graded Hilbert series driven Buchberger algorithm in Caboara *et al.* (1996) is available by on-line, (Gatermann, 1996a). The basic idea is to climb up by W-degree and to exploit the Hilbert series. At degree i there are $b^i - a^i$ polynomials missing in order to form a nontruncated Gröbner basis. If $b^i = a^i$ then the remaining S-polynomials S-polynomials of W-degree i are discarded. As S-polynomials of U-degree $> d$ are neglected one may not come to the point where S-polynomials are discarded because of the Hilbert series information. In this case the normal form computation for all S-polynomials needs to be carried out.

Observe that the exploitation of the Buchberger criteria is not affected by the truncation because the gradings give rise to gradings on the module of syzygies.

2.4. ELIMINATION

Let $I \subset K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ be an ideal.

DEFINITION 2.19. $\tilde{I} = I \cap K[y]$ is called the *elimination ideal* of I in $K[y]$.

DEFINITION 2.20. A monomial order $\leq$ of $K[x, y]$ is called an elimination order, if

$$x^\alpha y^\gamma \geq y^\delta$$

for all cases with $x^\alpha \neq 1$.

By Becker and Weispfenning (1993, p. 257 Lemma 6.14) it is sufficient to demand

$$x^\alpha \geq y^\delta \qquad \forall x^\alpha \neq 1, y^\delta.$$

EXAMPLE 2.21. Elimination orders on $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ include

(a) the lexicographical order.
(b) all matrix orders with matrix $M = (M_{ij})$ with first column $M_{1i} = 1, i = 1, \ldots, n$, $M_{1i} = 0, i = n + 1, \ldots, n + m$. This includes the elimination order by Bayer and Stillman.
(c) block orders $\geq$ consisting of orders $\geq_x$ and $\geq_y$ on $K[x]$ and $K[y]$, respectively. ($x^\alpha y^\gamma > x^\beta y^\delta \Leftrightarrow x^\alpha >_x x^\beta$ or $x^\alpha = x^\beta$ and $y^\gamma >_y y^\delta$).

LEMMA 2.22. (BECKER AND WEISPFENNING, 1993, P. 269; COX ET AL., 1992, P. 329) *Let $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ and $\leq$ be an elimination order for $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Let $\mathcal{GB}$ be a Gröbner basis of*

$$I = (f_1(x) - y_1, \ldots, f_m(x) - y_m).$$

Then $\mathcal{GB} \cap K[y]$ is a Gröbner basis of the elimination ideal with respect to $\leq_{|K[y]}$.

(i) $f(x) \in K[f_1, \ldots, f_m] \Leftrightarrow normalf(f, \mathcal{GB})(x, y) \in K[y]$.
(ii) *if $f \in K[f_1, \ldots, f_m]$ then $g := normalf(f, \mathcal{GB}) \in K[y]$ gives a rewriting $f(x) = g(f_1(x), \ldots, f_m(x))$.*

Observe that $normalf(f, \mathcal{GB})$ depends in general on the term order. The relevance of Lemma 2.22 is that $K[f_1(x), \ldots, f_m(x)]$ and $K[y]/\tilde{I}$ are isomorphic as rings.

3. Gröbner Bases for Invariants and Equivariants

In equivariant dynamics we are concerned with the invariant ring and the module of equivariants. Assume G is a group and $\vartheta : G \to GL(K^n)$ its representation. Let $\rho : G \to GL(K^m)$ be another representation. (Of course the field K is $\mathbb{R}$ in theory, but for practical computations it often will be $\mathbb{Q}$ or an extension of it.) Moreover, we assume that ϑ, ρ are orthogonal.

$p \in K[x]$ is called *invariant*, if

$$p(\vartheta(g)x) = p(x), \qquad \forall g \in G.$$

By $K[x]_\vartheta$ we denote the invariant ring. $f \in K[x]^m$ is called *ϑ-ρ-equivariant*, if

$$f(\vartheta(g)x) = \rho(g)f(x), \qquad \forall g \in G.$$

The $K[x]_\vartheta$-module of ϑ-ρ-equivariants is denoted by $K[x]_\vartheta^\rho$.

In equivariant dynamical systems one studies

$$\dot{x} = f(x),$$

where f is a generic equivariant vector field. f is polynomial if a truncation of the Taylor expansion has been performed. So the knowledge of generators of the invariant ring and the module are the key for investigation of generic equivariant dynamical systems.

3.1. RELATIONS

Let $\{p_1, \ldots, p_k\}$ denote the Hilbert basis of the invariant ring $K[x]_\vartheta$. The relations among the basis elements are easily determined with the help of Gröbner bases. Recall that the relations are polynomials $r \in K[y_1, \ldots, y_k]$ with $r(p_1(x), \ldots, p_k(x)) \equiv 0$. They form an ideal.

ALGORITHM 3.1. (RELATIONS IN FUNDAMENTAL INVARIANTS UP TO DEGREE d)

INPUT: *Invariant polynomials $p_1(x), \ldots, p_k(x) \in K[x]$,*
homogeneous with respect to the natural grading N on $K[x]$

OUTPUT: *relations $r_1, \ldots, r_l \in K[y_1, \ldots, y_k]$*

(i) Compute the Hilbert series $\mathcal{HP}_{K[x,y]/(y_1,\ldots,y_k)}$ with respect to the induced grading $W : \{x, y\} \to \mathbb{N}, W_{|\{x\}} = N, W(y_i) = \deg_N(p_i(x)), i = 1, \ldots, k$.
(ii) Choose an elimination order $\leq$ on $K[x, y]$ which eliminates x.
(iii) Compute a Gröbner basis $\mathcal{GB}(\bigoplus_{i \leq d} H_i^W(I))$ of the ideal

$$I := (p_1(x) - y_1, \ldots, p_k(x) - y_k) \subset K[x, y],$$

with respect to the elimination order, using the Hilbert series driven Buchberger algorithm with the Hilbert series under (i), truncate with respect to the grading W up to degree d. The polynomials $\mathcal{GB} \cap K[y]$ are $W_{|\{y\}}$-homogeneous and form a truncated Gröbner basis of degree d with respect to W of the ideal of relations $\tilde{I} \subset K[y]$.

PROOF. Without exploiting homogeneity the correctness of the algorithm is given by Lemma 2.22. As the polynomials $p_i(x) - y_i, i = 1, \ldots, k$ are homogeneous with respect to the induced grading W, it makes sense to use truncation and the Hilbert series driven Buchberger algorithm. By the 1. Buchberger criterion the polynomials $p_i(x) - y_i$ form a Gröbner basis of I with respect to a term order which select y_i as leading terms. The Hilbert series $\mathcal{HP}_{K[x,y]/I}^W(\lambda)$ is given by the series of the monomial ideal $(y_1, \ldots, y_k)$ by Lemma 2.14. The restriction $W_{|\{y\}}$ is a weighted grading on $K[y]$. As $p_i - y_i$ are homogeneous all other polynomials in the Buchberger algorithm are homogeneous, especially $\mathcal{GB}(\tilde{I})$. Thus the ideal of relations is W-homogeneous and it makes sense to consider the part up to degree d. $\square$

REMARK 3.2. (i) Different choices of elimination term orders in (ii) give different sets of output polynomials. Nevertheless, the same space $\bigoplus_{i=0}^{d} H_i^W(\tilde{I})$ is generated. (ii) In case no Hilbert series driven Buchberger algorithm is available, special choices of an elimination order greatly influence the cpu time. Good experience has been gained with a matrix order with first row given by W. As $p_i - y_i$ are W-homogeneous this does not affect the final Gröbner basis, but gives good exploitation of the Buchberger criteria because the S-polynomials are ordered with respect to sugar and then ties are broken by the term order.

Given some homogeneous invariant polynomials $p_1(x), \ldots, p_k(x)$ and some homogeneous equivariants $f_1(x), \ldots, f_l(x) \in K[x]_{\vartheta}^{\rho}$ one denotes by relations the set of polynomials

$$\mathcal{R} = \{r \in K[y, u] \mid r(p(x), f(x)) \equiv 0, r \in H_1^{\Gamma}(K[y, u])\},$$

where $\Gamma : \{y, u\} \to \mathbb{N}, \Gamma_{|\{y\}} = 0, \Gamma_{|\{u\}} = N$ is a Kronecker grading.

It is interesting to know a generating set of $\mathcal{R}$ since the $K[p(x)]$-module generated by $f_1, \ldots, f_l$ is isomorphic to the $K[y]/\tilde{I}$-module $H_1^{\Gamma}(K[y, u])/\mathcal{R}$, where $\tilde{I}$ is the ideal of relations in the invariants.

A Gröbner basis $\mathcal{GB}(\tilde{I})$ gives some generators $u_i \cdot g, g \in \mathcal{GB}(\tilde{I})$, $i = 1, \ldots, l$, of $\mathcal{R}$. By the following algorithm these are completed to a generating set of $\mathcal{R}$.

ALGORITHM 3.3. (RELATIONS IN FUNDAMENTAL INVARIANTS AND EQUIVARIANTS UP TO DEGREE d)

INPUT: *homogeneous invariants $p_1(x), \ldots, p_k(x)$*
homogeneous equivariants $f_1(x), \ldots, f_l(x) \in K[x]^m$
degree d
OUTPUT: *relations $r_1, \ldots, r_s \in H_1^{\Gamma}(K[y, u])$*
(i) Choose slack variables $z_1, \ldots, z_m$.
(ii) Choose a term order $\leq$ on $K[x, z, y, u]$ which eliminates x and z.
(iii) $W : \{x, z, y, u\} \to \mathbb{N}$, $W_{|\{x\}} = N$, $W_{|\{z\}} = 0$, $W(y_i) = \deg_N(p_i(x))$, $i = 1, \ldots, k$, $W(u_i) = \deg_N(f_i(x))$, $i = 1, \ldots, l$.
(iv) Compute $\mathcal{GB}(\bigoplus_{i \leq d} H_i^W(I))$ with respect to $\leq_{|K[x,y]}$ of $I = (p_1(x) - y_1, \ldots, p_k(x) - y_k) \subset K[x, y]$ by Algorithm 3.1.
(v) Use grading $U : \{x, z, y, u\} \to \mathbb{N}$, $U_{|\{x,y\}} = 0$, $U_{|\{z,u\}} = N$.
(vi) $g_i(x, z) := \sum_{j=1}^{m} (f_i(x))_j z_j$, $i = 1, \ldots, l$. Define

$$J = (p_1(x) - y_1, \ldots, p_k(x) - y_k, g_1(x, z) - u_1, \ldots, g_l(x, z) - u_l) \subset K[x, z, y, u].$$

(vii) Compute the Hilbert series $\mathcal{HP}_{K[x,z,y,u]/J}^{W+U,W}$ equal to the Hilbert series given by $(y_1, \ldots, y_k, u_1, \ldots, u_l)$.
(viii) Compute $\mathcal{GB}(\bigoplus_{(i,j) \leq (d,1)} H_{i,j}^{W,U}(J))$ with respect to $\leq$ of J. Use the Hilbert series driven Buchberger algorithm with Hilbert series $\mathcal{HP}_{K[x,z,y,u]/J}^{W+U,W}$ as under (vii) and as input use

$$\mathcal{GB}\left(\bigoplus_{i \leq d} H_i^W(I)\right) \text{ and } normalf\left(g_i(x, z) - u_i, \mathcal{GB}\left(\bigoplus_{i \leq d} H_i^W(I)\right)\right), \qquad i = 1, \ldots, l.$$

(ix) The relations are $\mathcal{GB} \cap H_1^U(K[y, u])$.

PROOF. By using the slack variables the relations in p_i and g_j of degree 1 equals the set $\mathcal{R}$, the relations in p_i and f_j. The grading U enables the restriction to the module. The Gröbner basis of J gives a Gröbner basis of $\tilde{J} = J \cap K[y,u]$ by Lemma 2.22. With U one obtains a Gröbner basis of $\bigoplus_{i=0}^{1} H_i^U(\tilde{J})$ where $H_0(\tilde{J}) = \tilde{I}$. As $I \subset J$ one can first compute a Gröbner basis of I. Because J is homogeneous with respect to W and the Buchberger algorithm preserves homogeneity one can restrict to degree d. $\square$

REMARK 3.4. (i) If no Hilbert series driven Buchberger algorithm is available Remark 3.2 is valid analogously.

(ii) If the representation $\rho : G \to GL(K^m)$ contains no trivial irreducible representation in its isotypic decomposition the efficiency can be improved significantly by using a term order which eliminates x only. If ρ contains not the trivial representation the slack variables are eliminated automatically. ρ induces an action on z as $\rho^t : G \to GL(K^m), g \mapsto \rho(g)^t$. The polynomials $g_i(x,z)$ are $(\rho + \rho^t)$-invariant. $J \cap H_1^U(K[z,y])$ is generated over $K[y]$ by the ρ^t-invariant in $K[z]$ of degree 1. As ρ has no trivial irreducible representation there exists no ρ^t-invariant of degree 1 and thus $J \cap H_1^U(K[z,y])$ is empty. Because of the symmetry this is equivalent to $J \cap H_1^U(K[z,y,u]) = J \cap H_1^U(K[y,u])$.

(iii) If ρ contains the trivial representation then one should use an elimination order which first eliminates x and in a second step z.

(iv) It is preferable to use the weight system $[U+W, W]$ instead of $[U,W]$ because $U+W$ is already a weight system. This is used in the Hilbert series driven version of the Buchberger algorithm.

EXAMPLE 3.5. In order to investigate a Takens–Bogdanov point with D_3-symmetry in Matthies (1996) a generic equivariant vector field is investigated for the action of D_3 generated by

$$\text{flip}(v,w) = (\bar{v}, \bar{w}), \qquad \text{and} \qquad \text{rotation } (v,w) = (e^{i\frac{2\pi}{3}} v, e^{i\frac{2\pi}{3}} w),$$

which decomposes as two times the natural two-dimensional action. The invariants and equivariants in these coordinates are suggested as

$$s_1 = v\bar{v}, \qquad s_2 = w\bar{w}, \qquad t_0 = w^3 + \bar{w}^3, \qquad t_3 = v^3 + \bar{v}^3,$$
$$s_3 = v\bar{w} + \bar{v}w, \qquad t_1 = vw^2 + \bar{v}\bar{w}^2, \qquad t_2 = v^2 w + \bar{v}^2 \bar{w}.$$
$$g_0 = \begin{pmatrix} v \\ 0 \end{pmatrix}, \qquad g_1 = \begin{pmatrix} 0 \\ v \end{pmatrix}, \qquad g_2 = \begin{pmatrix} w \\ 0 \end{pmatrix}, \qquad g_3 = \begin{pmatrix} 0 \\ w \end{pmatrix},$$

and

$$f_j = \begin{pmatrix} \bar{v}^j \bar{w}^{3-j-1} \\ 0 \end{pmatrix}, \qquad h^j = \begin{pmatrix} 0 \\ \bar{v}^j \bar{w}^{3-j-1} \end{pmatrix}, \qquad j = 0, 1, 2.$$

The complex notation is chosen since this is common in analysis and is appropriate for hand calculations. For computation in a Computer Algebra Package one chooses different coordinates: $v = v_r + i \cdot v_i, w = w_r + i \cdot w_i$. Then the invariants and equivariants are

$$s_1 = v_r^2 + v_i^2, \qquad s_2 = w_r^2 + w_i^2, \qquad t_0 = 2w_r^3 - 6w_r w_i^2,$$
$$t_3 = 2v_r^3 - 6v_r v_i^2, \qquad s_3 = 2v_r w_r + 2v_i w_i,$$
$$t_1 = 2v_r w_r^2 - 2v_r w_i^2 - 4v_i w_r w_i, \qquad t_2 = 2v_r^2 w_r - 4v_r v_i w_i - 2v_i^2 w_r,$$
$$g_0 = [v_r, v_i, 0, 0], \qquad g_1 = [0, 0, v_r, v_i], \qquad g_2 = [w_r, w_i, 0, 0], \qquad g_3 = [0, 0, w_r, w_i],$$

Table 2. Computation of relations in invariants and equivariants for $D_3 + D_3$ with and without use of Hilbert series and as in Algorithm 3.3.

	Relations in invariants		Relations in equivariants		
	No HP	With HP	1 GB no HP	1 GB with HP	GB Alg. 3.3
Total nr of pairs	3003	1743	26478	16775	15419
Elim. pairs by trunc.			39952	21148	23362
Elim. pairs by criteria	2502	1276	23126	13558	12681
Elim. pairs by HP		322		2469	2290
Treated pairs	501	145	3352	748	448
CPU	807 s	239 s	10.5 h	6.2 h	4.9 h

$$f_0 = [w_r^2 - w_i^2, -2w_r w_i, 0, 0], \qquad f_1 = [v_r w_r - v_i w_i, -v_r w_i - v_i w_r, 0, 0],$$
$$f_2 = [v_r^2 - v_i^2, -2v_r v_i, 0, 0],$$
$$h_0 = [0, 0, w_r^2 - w_i^2, -2w_r w_i], \qquad h_1 = [0, 0, v_r w_r - v_i w_i, -v_r w_i - v_i w_r],$$
$$h_2 = [0, 0, v_r^2 - v_i^2, -2v_r v_i].$$

Table 2 shows some statistics of the computations of the relations. With the algorithms in Subsection 3.2 it could be shown that the invariant ring and the module of equivariants are generated completely, which Matthies had previously done using polar coordinates.

3.2. COMPLETENESS

Given some homogeneous invariants it is easily checked by using Gröbner bases whether the invariant ring $K[x]_\vartheta$ is generated up to degree d. Without restriction in degree this is Algorithm 2.2.5 p. 32 in Sturmfels (1993).

ALGORITHM 3.6. (COMPLETENESS OF INVARIANTS UP TO DEGREE d)

INPUT: *Molien series of invariant ring* $\mathcal{HP}_{K[x]_\vartheta}(z)$,
homogeneous invariants $p_1(x), \ldots, p_k(x)$,
degree d

OUTPUT: *true or minimal degree of missing invariant*

(i) *Compute relations* $\mathcal{GB}(\bigoplus_{i \leq d} H_i^W(\tilde{I}))$ *by Algorithm 3.1.*
(ii) $LT := \{ht(f) | f \in \mathcal{GB}\}$
(iii) *Compute* $\mathcal{HP}_{K[y]/(LT)}^W(z)$
(iv) *If* $\mathcal{HP}_{K[y]/(LT)}^W(z) \equiv \mathcal{HP}_{K[x]_\vartheta}^W(z)$ *then* "invariants generate invariant ring completely".
    If $series(\mathcal{HP}_{K[y]/(LT)}^W(z), d) \equiv series(\mathcal{HP}_{K[x]_\vartheta}^W(z), d)$ *then* true
        else mindeg$(series(\mathcal{HP}_{K[x]_\vartheta}^W(z) - \mathcal{HP}_{K[y]/(LT)}^W(z), d)$

PROOF. As $p_1, \ldots, p_k$ are invariants we have $K[p(x)] \subset K[x]_\vartheta$. As p_i are homogeneous in the natural grading N we have, moreover,

$$H_i^N(K[p]) \subset H_i^N(K[x]_\vartheta), \qquad i = 0, \ldots,$$

and thus

$$\dim H_i^N(K[p]) \leq \dim H_i^N(K[x]_\vartheta), \qquad i = 0, \ldots.$$

Thus one only needs to compare $\mathcal{HP}_{K[p]}^N(z)$ and $\mathcal{HP}_{K[x]_\vartheta}^N(z)$ (up to degree d). As the ideal of relations $\tilde{I} \subset K[y]$ is homogeneous with respect to the induced grading W the residue ring $K[y]/\tilde{I}$ is graded by $W_{|\{y\}}$ as well. Moreover, $K[y]/\tilde{I}$ with respect to W and $K[p(x)]$ with respect to the natural grading are isomorphic as graded rings. Thus $\mathcal{HP}_{K[p]}^W(z) = \mathcal{HP}_{K[y]/\tilde{I}}^W(z)$. By Lemma 2.14 the Gröbner basis $\mathcal{GB}$ of $\tilde{I}$ yields $\mathcal{HP}_{K[p]}^N(z) = \mathcal{HP}_{K[y]/LT(\tilde{I})}^W(z)$. If one truncates the Gröbner basis to degree d the last equality is only valid for degrees $0, 1, \ldots, d$. □

For the equivariants the algorithmic treatment is analogous.

ALGORITHM 3.7. (COMPLETENESS OF FUNDAMENTAL EQUIVARIANTS UP TO DEGREE d)

INPUT: *Hilbert–Poincaré series $\mathcal{HP}_{K[x]_\vartheta^\rho}^N(z)$ of $K[x]_\vartheta$-module of equivariants $K[x]_\vartheta^\rho$,*
homogeneous invariants $p_1(x), \ldots, p_k(x)$,
homogeneous equivariants $f_1(x), \ldots, f_l(x)$, degree d

OUTPUT: *true, if $K[x]_\vartheta^\rho$ is generated by $f_1, \ldots, f_l$ as $K[p]$-module up to degree d else minimal degree of missing part.*

(i) *Compute $\mathcal{GB}(\bigoplus_{(i,j)\leq(d,1)} H_{i,j}^{W,U}(\tilde{J}))$ as in Algorithm 3.3.*
(ii) *Define $LT := \{ht(f)|f \in \mathcal{GB}\}$.*
(iii) *Compute the Hilbert series of the $K[p]$-module M generated by $f_1, \ldots, f_l$ by*
hp := 0

for j from 1 to l do
$\quad T_i = \{y^\alpha \in K[y]|y^\alpha \in LT \text{ or } u_i y^\alpha \in LT\}$
$\quad hp := hp + z^{\deg(f_i)} \cdot \mathcal{HP}_{K[y]/(T_i)}^W(z)$
$\quad \mathcal{HP}_M^N(z)_{|0..d} = \mathcal{HP}_{H_1^U(K[y,u])/\mathcal{R}}^W(z)_{|0..d} := hp(z)_{|0..d}$

(iv) *If $\mathcal{HP}_M^N(z) = \mathcal{HP}_{K[x]_\vartheta^\rho}^N(z)$ then "module is generated completely".*
$\quad$ *If $series(\mathcal{HP}_M^N(z), d) = series(\mathcal{HP}_{K[x]_\vartheta^\rho}^N(z), d)$ then true*
$\quad\quad$ *else $\text{mindeg}(series(\mathcal{HP}_M^N(z) - \mathcal{HP}_{K[x]_\vartheta^\rho}^N(z), d))$.*

PROOF. As in the proof of correctness of Algorithm 3.6 we use that $K[p]$ and $K[y]/\tilde{I}$ are isomorphic as graded rings with respect to the natural grading N and $W_{|\{y\}}$, respectively. For $\tilde{J} := J \cap K[y, u]$ the submodule $H_1^U(\tilde{J}) = \mathcal{R}$ is a module over $K[y]$ and as $H_0^U(\tilde{J}) = \tilde{I}$ and $\bigoplus_{i=0}^l u_i \tilde{I} \subset H_1^U(\tilde{J})$ the module is a $K[y]/\tilde{I}$-module. As $H_1^U(\tilde{J})$ is generated by $W_{|\{y,u\}}$-homogeneous elements the quotient $H_1^U(K[y,u]/H_1^U(\tilde{J})$ is graded by the quotient grading of W over the graded ring $K[y]/\tilde{I}$.

In fact, the K-vector spaces

$$H_i^W\left(H_1^U(K[y,u])/H_1^U(\tilde{J})\right) \text{ and } H_i^N(M)$$

are isomorphic for all i. Together U, W form a weight system. Thus the spaces have the same dimension and the Hilbert series are equal.

In a generalization of Lemma 2.14 the $K[y]/\tilde{I}$-module $H_1^U(K[y,u])/H_1^U(\tilde{J})$ and the $K[y]/LT(\tilde{I})$-module $H_1^U(K[y,u])/LT(H_1^U(\tilde{J}))$ are isomorphic as W-graded modules. The

Table 3. Timings for completeness of invariants and equivariants for $O(2) \times S^1$.

Degree	Invariants		Equivariants	
	Cpu	Complete up to	Cpu	Complete up to
5	9 s	5	18 min	5
6	20 s	6	53 min	6
7	28 s	7	2.0 h	8
8	47 s	∞	4.6 h	10
11			21.9 h	∞
∞	265 s	∞		

monomial module $LT(H_1^U(\tilde{J}))$ is easily determined from the Gröbner basis $\mathcal{GB}(H_0^U(\tilde{J}) + H_1^U(\tilde{J}))$. The monomials $\bigcup_{i=1}^l u_i LT(\mathcal{GB}(H_0^U))$ and

$$\{m \in LT(\mathcal{GB}(H_0^U(\tilde{J}) + H_1^U(\tilde{J})))| \deg_U(m) = 1\}$$

generate $LT(H_1^U(\tilde{J}))$.

By exploiting $LT(H_1^U(\tilde{J})) = \bigoplus_{i=1}^l u_i \cdot (T_i)$ the modules $H_1^U(K[y, u])/H_1^U(\tilde{J})$ and $\bigoplus_{i=1}^l K[y]/(T_i)$ are isomorphic. As graded modules one needs to take into account the shifts in the gradings by $\deg_W(u_i) = \deg_N(f_i)$.

In case the Gröbner basis is only computed up to degree d the computed Hilbert series is of course only valid up to degree d. $\square$

EXAMPLE 3.8. In Leis (1995) a Hopf bifurcation with $O(3)$ symmetry is investigated. After reduction to a fixed point space one is left with the action

$$r_\theta(z_{-2}, z_0, z_2) = (e^{-i\theta} z_{-2}, z_0, e^{i\theta} z_2),$$
$$\kappa(z_{-2}, z_0, z_2) = (z_2, z_0, z_{-2}),$$
$$\phi(z_{-2}, z_0, z_2) = (e^{i\phi} z_{-2}, e^{i\phi} z_0, e^{i\phi} z_2),$$

of $O(2) \times S^1$ where S^1 comes in due to the Hopf bifurcation. The invariants are suggested as

$$\pi_1 = |z_0|^2, \qquad \pi_2 = |z_{-2}|^2 + |z_2|^2, \qquad \pi_3 = |z_{-2}|^2 \cdot |z_2|^2,$$
$$\pi_4 = \frac{1}{2}(\overline{z_0}^2 z_{-2} z_2 + z_0^2 \overline{z_{-2}}\, \overline{z_2}), \qquad \pi_5 = \frac{i}{2}(\overline{z_0}^2 z_{-2} z_2 - z_0^2 \overline{z_{-2}}\, \overline{z_2}).$$

For the equivariants Leis has given

$$e_1 = \begin{pmatrix} 0 \\ z_0 \\ 0 \end{pmatrix}, \qquad e_2 = \begin{pmatrix} z_{-2} \\ 0 \\ z_2 \end{pmatrix}, \qquad e_3 = \begin{pmatrix} z_{-2}|z_2|^2 \\ 0 \\ z_2|z_{-2}|^2 \end{pmatrix},$$

$$e_4 = \frac{1}{2}\begin{pmatrix} z_0^2 \bar{z}_2 \\ 2z_{-2}z_2 \overline{z_0} \\ z_0^2 \overline{z_{-2}} \end{pmatrix}, \qquad e_5 = -\frac{i}{2}\begin{pmatrix} z_0^2 \bar{z}_2 \\ -2z_{-2}z_2 \overline{z_0} \\ z_0^2 \overline{z_{-2}} \end{pmatrix},$$

such that the equivariants are $E_i = (e_i, \bar{e}_i)$. These coordinates are very common in dynamical systems. Then the multiplication for a complex number c is meant to be $c \cdot E_i = (c \cdot e_i, \bar{c} \cdot \bar{e}_i)$. In order to be able to compute one needs to change coordinates: $z_{-2} = \frac{1}{2}\sqrt{2}(x_1 + i \cdot y_1), z_0 = \frac{1}{2}\sqrt{2}(x_2 + i \cdot y_2), z_2 = \frac{1}{2}\sqrt{2}(x_3 + i \cdot y_3)$ or equivalently $(z, \bar{z}) = A \cdot (x, y)$. The transformed equivariants are

$$A^{-1} \cdot E_i(A \cdot (x, y)), \qquad A^{-1} \cdot (i \cdot e_i(A \cdot (x, y)) - i \cdot e_i(A \cdot (x, y))), \qquad i = 1, \ldots 5,$$

which gives 10 equivariants. The Molien series and the equivariant Molien series have been computed in Leis (1995) with the Weyl integral formula and theorem of residues to be

$$\mathcal{HP}_{O(2)\times S^1}(\lambda) = \frac{1+\lambda^4}{(1-\lambda^2)^2 \cdot (1-\lambda^4)^2}, \qquad \mathcal{HP}_{O(2)\times S^1}^{O(2)\times S^1}(\lambda) = \frac{4\lambda + 6\lambda + 2\lambda^5}{(1-\lambda^2)^2 \cdot (1-\lambda^4)^2}.$$

The completeness question for the equivariants turned out to be a hard problem. Table 3 gives some timings. In Leis (1995) the question has been considered up to degree 5 only. Our procedure allows to make the calculation of complete generation of the module for the first time.

3.3. ORBIT SPACE REDUCTION

In equivariant dynamics there is one method known as orbit space reduction, see Chossat (1993), Chossat and Dias (1995), Lauterbach and Sanders (1995) and Koenig (1997). Assume an equivariant system

$$\dot{x} = f(x), \qquad x \in \mathbb{R}^n, \tag{3.1}$$

where $f \in \mathbb{R}[x]_\vartheta^\vartheta$. Without restriction we may assume that ϑ is orthogonal because this is true for compact Lie groups, see Fulton and Harris (1991). Let $p_1(x), \ldots, p_k(x)$ be the fundamental invariants which generate $\mathbb{R}[x]_\vartheta$. Then the dynamic of (3.1) is closely related to the dynamic of a system

$$\dot{y} = g(y), \qquad y \in \mathbb{R}^k + \text{ algebraic relations} \tag{3.2}$$

because

$$\frac{\partial}{\partial t}p_i(x) = \left(\frac{dp_i}{dx}\right)^t \dot{x} = \left(\frac{dp_i}{dx}\right)^t f(x) = \left(\frac{dp_i}{dx}, f(x)\right) = h_i(x) = g_i(p_1(x), \ldots, p_k(x)),$$

for $i = 1, \ldots, k$, where $g_i \in R[y]$ exist with this property because h_i is invariant. The gradient of an invariant is equivariant and the inner product of two equivariants is an invariant because the inner product $(\cdot, \cdot)$ is invariant for orthogonal representations. There is a lot to say about the topological structure but that is beyond the scope of this paper. Here we are only interested in those calculations which are often done by hand but can be done by computer.

The algebraic relations are computed by Algorithm 3.1. It is well known in Computer Algebra but not in Analysis that the rewriting of h_i in $g_i(p(x))$ is done with Gröbner bases, see Lemma 2.22.

ALGORITHM 3.9. (ORBIT SPACE REDUCTION)

INPUT: *equivariant* $f(x) \in K[x]_\vartheta^\vartheta$,
homogeneous invariants $p_1(x), \ldots, p_k(x)$ *generating* $K[x]_\vartheta$

OUTPUT: $\dot{y} = g \in K[y_1, \ldots, y_k]^k$, *relations*

$d := \max(\deg(p_1), \ldots, \deg(p_k)) + \deg(f) - 1$
Compute the Gröbner basis $\mathcal{GB}(\bigoplus_{i=0}^d H_i^W(I))$ *as in Algorithm 3.1.*
Then compute the normal forms $g_i(y) = normalf(\frac{dp_i(x)}{dx} \cdot f(x), \mathcal{GB}), i = 1, \ldots, k.$

Table 4. Timings of Algorithm 3.9 (orbit space reduction) for examples from literature.

Example	Group	Cpu time
(Chossat, 1993)	$O(2)$	5 s
(Chossat and Dias, 1995)	$O(2) \times S^1$	72 s
(Leis, 1995)	$O(3) \times S^1$	160 s

REMARK 3.10. (i) Observe that we do not need a full Gröbner basis in Algorithm 3.9.

(ii) In case the invariants form a Hironaka decomposition (that means that the secondary invariants $p_{s+1}, \ldots, p_k$ form a free module over the ring $\mathbb{R}[p_1, \ldots, p_s]$ and thus each invariant has a unique representation $\sum_{i=s+1}^{k} a_i(p_1, \ldots, p_s) \cdot p_i$) one would like to compute the unique representations $\sum a_i p_i$ in Algorithm 3.9. This is done, if the eliminating term order $\leq$ on $K[x, y]$ is such that the matrix representing the order $\leq_{|K[y]}$ starts with first row with 0's for $y_1, \ldots, y_s$ and 1's for $y_{s+1}, \ldots, y_k$ (Sturmfels, 1993, p. 52).

(iii) The polynomial g_i may also be found by linear algebra technique. But the advantage of Gröbner bases is the *unique* way of representation once a term order has been chosen.

3.4. computing invariants

For finite groups there is one famous algorithm in Sturmfels (1993) for the computation of invariants which appeared first in Sturmfels and White (1991). It makes use of the fact that the invariant ring $K[x]_\vartheta$ is Cohen–Macaulay, which means whenever we have polynomials $p_1, \ldots, p_n$ such that $K[x]_\vartheta$ is a finitely generated module over the subring $K[p(x)]$ then it is a free module.

The generators are called *secondary invariants* in contrast to the *primary invariants* p_i. The algorithm searches first primary invariants until the set of common zeros of $p_1, \ldots, p_n$ is $\{0\}$ (the *nullcone*). The degrees of the secondaries are then known by the Molien series of $K[x]_\vartheta$.

ALGORITHM 3.11. (STURMFELS, 1993, P. 57)
INPUT: *finite group* $\vartheta : G \to GL(K^n)$

(i) find primary invariants $p_1, \ldots, p_n$
(ii) find secondary invariants: for degrees d_i there are c_i many, $i = 1, \ldots, m$

$S = \{1\}$
for $i = 1, \ldots, m$
  for $j = 1, \ldots, c_i$
    $q :=$ *nextcandidate* $\in H_{d_i}^N(K[x]_\vartheta)$
    while $q(x)$ *is not an element of the free* $K[p]$*-module generated by* S
      $q :=$ *nextcandidate*
    $S := S \cup \{q\}$

There are at least four ways in performing the task

$$q(x) \in^? \bigoplus_{s \in S} s(x) K[p_1(x), \ldots, p_n(x)],$$

Table 5. Timings for Algorithm 3.11 for various variants.

Group	Ref.	Degrees of		Up to	Invariants			
		primary	secondary		a	b	c	d
$D_3(\vartheta^2 + \vartheta^3)$	Gatermann and Werner (1996)	2,2,3	4	all	6 s	9 s	9 s	6 s
$D_3 + D_3$	Matthies (1996)	2,2,3,3	2,3,3,4,6	all	23 s	243 s	343 s	19 s
$D_4(\vartheta^2 + \vartheta^5)$	Campbell and Holmes (1992)	2,2,4	3	all	4 s	5 s	5 s	4 s
$Z_4 \cdot Z_2^4$	Worfolk (1994)	2,4,4,8	6,6,6, 8,8,8,14	8 all	108 s 213 s	466 s >1 h	529 s >1 h	107 s 179 s

whether q is a member of the free module generated by $S = \{1, s_2, \ldots, s_l\}$ over $K[p]$. It is used that q_i is homogeneous of degree $d_i = \deg_N(q(x))$.

(a) Pure linear algebra:
Build all terms $sp_1^{j_1} \cdots p_n^{j_n}$ with $s \in S$, $j = (j_1, \ldots, j_n)$ such that $\deg_N(sp^j) = d_i$ and determine linear dependence of $q(x)$ on these polynomials by comparing coefficients.
(b) Normal form with respect to Hironaka decomposition:
Compute a Gröbner basis $\mathcal{GB}(\bigoplus_{j=1}^{d_i} H_j^N(I))$ of

$$I = (p_1(x) - y_1, \ldots, p_n(x) - y_n, \eta_2 - s_2(x), \ldots)$$

with respect to a term order which eliminates first x and on $K[y, \eta]$ eliminates η, starting with natural degree on η, see Sturmfels (1993, p. 52). (Use the Hilbert series driven Buchberger algorithm with $\mathcal{HP}_{K[x,y,\eta]/I}^W$ given by $(y_1, \ldots, y_n, \eta_2, \ldots, \eta_l)$.) If $normalf(q, \mathcal{GB}) \in K[y, \eta]$ and is linear in η then $q \in \bigoplus_{s \in S} s \cdot K[p]$. Once a new secondary invariant is found the Gröbner basis needs to be updated.
(c) Restriction to module with slack variable: choose a variable z and consider the gradings $W : \{x, y, \eta, z\} \to \mathbb{N}$ $W_{|\{x\}} = N$, $W(y_i) = \deg_N(p_i(x))$, $i = 1, \ldots, n$, $W(\eta_i) = \deg_N(s_i(x))$, $i = 2, \ldots, l$, $W(z) = 0$ for restriction in degree and $U : \{x, y, \eta, z\} \to \mathbb{N}$, $U_{|\{x,y\}} = 0$, $U_{|\{\eta\}} = N$, $U(z) = 1$ for restriction to the module. For

$$I := (y_1 - p_1(x), \ldots, y_n - p_n(x), \eta_2 - z \cdot s_2, \ldots, \eta_l - z \cdot s_l),$$

compute $\mathcal{GB} = \mathcal{GB}(\bigoplus_{k \leq d_i, j=0,1} H_{k,j}^{W,U}(I))$. (Use the Hilbert series $\mathcal{HP}_{K[x,y,\eta,z]/I}^{W,U}$ given by $(y_1, \ldots, y_n, \eta_2, \eta_l)$.) If $g(x, y, \eta, z) = normalf(z \cdot q, \mathcal{GB})$ does not depend on x then q is a member of the module and $g(p(x), s(x), 1) = q(x)$. Like method (b) the Gröbner basis needs updating after a new secondary invariant was found.
(d) Using one Gröbner basis: the Gröbner basis $\mathcal{GB}(\bigoplus_{j=0}^{\max(d_i)} H_j^N((p_1(x), \ldots, p_n(x))))$ with respect to any term order is computed once in the beginning. Consider the set of normal forms $\tilde{S} = \{normalf(s, \mathcal{GB}) | s \in S\}$ and $\tilde{q} := normalf(q, \mathcal{GB}) \in K[x]$.
If $\tilde{q}$ is K-linear dependent on $\tilde{S}$ (on those of degree d_i) then $q(x) = \bigoplus_{s \in S} s(x) \cdot B^s(x)$ with $B^s(x) \in (p_1(x), \ldots, p_n(x))$ members of the ideal. Because of the invariance $B^s(x)$ can be assumed to be invariant and thus to be members of $K[p]$. Here one can use restriction to actual degree.

In *Invar* (Kemper, 1993) method (d) is used. We tested these methods for various examples and give their timings in Table 5. Methods (b) and (c) need more time because more information than needed, namely the representation in $p(x)$ and $s \in S$, is computed.

Table 6. Timings for computation of equivariants for various variants.

Group	Ref.	degrees of equivariants	up to	equivariants a	equivariants c	equivariants d
$D_3(\vartheta^2 + \vartheta^3)$	Gatermann and Werner (1996)	1,1,2,2,3,3	all	37 s	85 s	35 s
$D_3 + D_3$	Matthies (1996)	1,1,1,1,2,2,2,2,2,2,	2	45 s	185 s	46 s
		3,3,3,3,4,4,4,4,4,5,5,5,5	all	324 s	>1 h	229 s
$D_4(\vartheta^2 + \vartheta^5)$	Campbell and Holmes (1992)	1,1,2,2,3,4	all	70 s	129 s	69 s
$Z_4 \cdot Z_2^4$	Worfolk (1994)	1,3,3,3,3,(7*5),	3	158 s	274 s	164 s
		(8*7), (7*9), (4*11),13	all	4290 s	>3 h	2581 s

Method (d) is most efficient because it exploits the underlying structure as much as possible.

3.5. EQUIVARIANTS

As the module of equivariants is Cohen–Macaulay for finite groups the second part of the Algorithm 3.11 transfers immediately to the equivariant case, see Gatermann (1996b) and Worfolk (1994).

Only the task $q(x) \in^? \bigoplus_{e \in E} e(x)K[p(x)]$ where $q(x) \in K[x]^r$ and $E \subset K[x]^r$ of order m needs to be discussed. The methods (a), (c) and (d) are valid analogously, but (b) has no generalization. Timings are given in Table 6.

4. Invariants and Equivariants for Continuous Groups

The algorithms given in Section 3.4 cannot be generalized straightforward to continuous groups. We will consider here a different method based on properties of the Lie algebra associated to a compact Lie group. This is a direct extension of a method already used in Sattinger (1978) for the computation of the equivariants for $SO(3)$ and $O(3)$. It holds for the class of *semi-simple* Lie groups which includes most of the common classical groups ($SO(n)$ and $O(n)$ with $n > 2$, $SU(n)$ and $U(n)$, ...). There is a huge amount of bibliography concerning Lie groups and Lie algebras. Let us cite, for example, Bröcker and tom Dieck (1985), Humphreys (1980), Humphreys (1982), or Fulton and Harris (1991).

From now on, the group G will be a connected Lie group, i.e. a connected subgroup of $GL(n)$. Our approach can also be generalized to cases where a finite group H is involved. We indicate at the end of this section how to generalize the algorithms of this section in some particular cases. In equivariant dynamics problems, we are often interested in subgroups of $GL(n, \mathbb{R})$ acting on real vector spaces. However, for most of the interesting groups (including $SO(n)$, $SL(n)$, $Sp(2n)$) the real representations of subgroups of $GL(n, \mathbb{R})$ can be obtained by restriction to the real part of complex representations of subgroups of $GL(n, \mathbb{C})$.

4.1. LIE GROUP—LIE ALGEBRA

For a connected compact Lie group G let $\vartheta : G \to GL(\mathbb{C}^n)$ and $\rho : G \to GL(\mathbb{C}^m)$ be two linear representations where ϑ is faithful. The aim of the following sections is

the computation of a generic homogeneous equivariant of degree d, i.e. one computes a vector space basis of $H_d^N(\mathbb{C}[x]_\vartheta^\rho)$. Observe that for $m = 1, \rho(g) = 1$ the case of invariants is included.

The key for the algorithm is the use of a associated Lie algebra. Recall that a connected Lie group is a manifold and the tangent space at the identity $T_e G$ has the special meaning of the Lie algebra $\mathbf{g}$, i.e. $T_e G$ is a vector space and additionally is provided with a Lie bracket.

Each $Y \in \mathbf{g}$ is thus given by a path $\gamma : [-1, 1] \to G, \gamma(0) = e, \frac{d}{ds}\gamma(s)_{|s=0} = Y$. The group action ϑ induces by the representation $\Theta : G \to \text{Aut}(\mathbb{C}[x]^m)$,

$$\Theta(g)(f(x)) = f(\vartheta(g^{-1})x), \qquad g \in G,$$

to an action of the Lie algebra on the polynomial vectors. Elements of the tangent space of $T_{\vartheta(e)}\vartheta(G)$ are given by paths

$$\gamma : [-1, 1] \to G, \qquad \gamma(0) = e, \qquad \gamma'(0) = Y \in \mathbf{g},$$

$$\zeta : \mathbf{g} \to GL(\mathbb{C}^n), \zeta(Y) = \frac{d}{ds}\vartheta(\gamma(s))_{|s=0}.$$

Analogously, we have $T_{\Theta(e)}\Theta(G)$ by $\theta : \mathbf{g} \to \text{Aut}(\mathbb{C}[x]^m)$

$$\theta(Y)(f(x)) = \frac{d}{ds}\Theta(\gamma(s))(f(x))_{|s=0} = \frac{d}{ds}f(\vartheta(\gamma(s)^{-1})x)_{|s=0}$$

$$= \frac{d}{dx}f(x) \cdot \frac{d}{ds}\vartheta(\gamma(s)^{-1})_{|s=0} \cdot x = \frac{d}{dx}f(x) \cdot \zeta(-Y) \cdot x$$

$$= -\frac{d}{dx}f(x) \cdot \zeta(Y) \cdot x.$$

Let the Lie algebra action associated to ρ be denoted by ϱ. The main ingredient in the algorithmic treatment is the following well-known lemma.

LEMMA 4.1. $f \in \mathbb{C}[x]^m$ is ϑ-ρ equivariant iff for all generators Y of $\mathbf{g}$

$$\theta(-Y)(f(x)) = \varrho(Y) \cdot f(x).$$

Special structure of the Lie algebra allows for more simplification as described in the following section. Besides this two simplifications are obvious. Assume ϑ decomposes into subrepresentations and the coordinates are such that the representation matrices have block diagonal form

$$\vartheta(g) = \begin{pmatrix} \vartheta^1(g) & & 0 \\ & \ddots & \\ 0 & & \vartheta^r(g) \end{pmatrix}.$$

The set of variables then decomposes into r subsets $x = (x^1, \ldots, x^r)$. Then the Kronecker gradings $N_i : \{x_1, \ldots, x_n\} \to \mathbb{N}$,

$$N_i(x_j) = \begin{cases} 1, & \text{if } x_j \in x^i \\ 0, & \text{else} \end{cases}$$

define a grading of $\mathbb{C}[x]$ such that the invariant ring is multi-graded by $\underline{N} = (N_1, \ldots, N_r)$ as well:

$$H_d(\mathbb{C}[x]_\vartheta) = \bigoplus_{k_1 + \cdots + k_r = d} H_{\underline{k}}^{\underline{N}}(\mathbb{C}[x]_\vartheta).$$

The module of equivariants is multi-graded analogously.

The second simplification is given by a decomposition of ρ in block diagonal form $\rho(g) = \mathrm{diag}(\rho_1(g), \ldots, \rho_s(g))$. The ϑ-ρ-equivariants are given by the ϑ-ρ_i-equivariants $\tilde{f}$ since $(0, \ldots, \tilde{f}, 0, \ldots, 0)$ is a ϑ-ρ-equivariant.

Observe that the case $\vartheta = \rho = \vartheta^1 + \vartheta^2$ includes the case which in the theory of dynamical systems is known as mode interaction.

4.2. PROPERTIES OF SEMI-SIMPLE LIE ALGEBRAS

We consider now the case where the group G is a finite dimensional complex semi-simple Lie group G. Let us recall that a connected Lie group is called *semi-simple* if it does not contain any nontrivial solvable normal subgroup. Similarly, a Lie algebra is called *semi-simple* if it contains no proper nontrivial Abelian ideal. Now a connected Lie group is semi-simple iff its Lie algebra $\mathbf{g}$ is semi-simple (Humphreys, 1980, p. 89). The classical complex Lie algebras $sl_n(\mathbb{C}), so_n(\mathbb{C})$ $(n > 2)$ and $sp_{2n}(\mathbb{C})$ are semi-simple. A maximal Abelian subalgebra $\mathbf{g}_0$ of $\mathbf{g}$ is called a *Cartan subalgebra*. Let us recall that the adjoint representation of $\mathbf{g}$ is the action of $\mathbf{g}$ on itself using the Lie bracket i.e.

$$\mathrm{ad} : \mathbf{g} \longrightarrow GL(\mathbf{g}),$$

such that for $X, Y \in \mathbf{g}$, $\mathrm{ad}(X)(Y) = [X, Y]$.

The action of $\mathbf{g}_0$ on $\mathbf{g}$ can be thought of as diagonal (Theorem 9.20 in Fulton and Harris (1991)) i.e. all matrices $\mathrm{ad}(X)$ for $X \in \mathbf{g}_0$ can be simultaneously diagonalized. This property suggests a so-called *Cartan decomposition* of $\mathbf{g}$

$$\mathbf{g} = \mathbf{g}_0 \oplus_\alpha \mathbf{g}_\alpha, \tag{4.1}$$

where each *root space* $\mathbf{g}_\alpha$ is a one-dimensional eigenspace for the elements of $\mathbf{g}_0$ in the adjoint action of $\mathbf{g}$. Each α occurring in the Cartan decomposition (4.1) is a linear form on $\mathbf{g}_0$. We denote by $\mathcal{R}$ the set of these linear forms which are called *roots*. For any root space $\mathbf{g}_\alpha$, the form $\alpha \in \mathbf{g}_0^*$ is defined by

$$\alpha(X)Y = \mathrm{ad}(X)\ Y = [X, Y], \ X \in \mathbf{g}_0, Y \in \mathbf{g}_\alpha.$$

If $\mathbf{g}_\alpha$ is a root space then $\mathbf{g}_{-\alpha}$ is also a root space. Furthermore, there exists a particular basis of $\mathbf{g}$ such that the elements of root spaces act in a nice way via the adjoint action.

THEOREM 4.2. (THE CARTAN–WEYL FORM) *Let* $\mathbf{g}$ *be a complex semi-simple Lie algebra with the Cartan decomposition (4.1). There exists a basis* $\{H_i : i = 1, \ldots, r\}$ *of* $\mathbf{g}_0$ *and for each* $\alpha \in \mathcal{R}$ *some* E_α *generates* $\mathbf{g}_\alpha$ *such that*

(i) $\mathrm{ad}(H_i)\ E_\alpha = [H_i, E_\alpha] = \alpha(H_i)\ E_\alpha,$

(ii) $\mathrm{ad}(E_\alpha)\ E_{-\alpha} = [E_\alpha,\ E_{-\alpha}] = \sum_{i=1}^{r} \alpha(H_i)\ H_i = H_\alpha,$

(iii) $\mathrm{ad}(E_\alpha)\ E_\beta = [E_\alpha\ E_\beta]\ = N_{\alpha,\beta}\ E_{\alpha+\beta}$ *with* $N_{\alpha,\beta} = 0$ *unless* $\alpha + \beta \in \mathcal{R}$,

with $N_{\alpha,\beta} = -N_{\beta,\alpha} = N_{-\beta,-\alpha} = -N_{-\alpha,-\beta}$.

EXAMPLE 4.3. The Cartan subalgebra of $so(3)$ is generated by J^3 and there are two root spaces generated by J^+ and J^-. Then

$$[J^3, J^\pm] = \pm J^\pm, \qquad [J^+, J^-] = 2J^3.$$

Now consider an action $\varrho : \mathbf{g} \to GL(V)$ where V is a complex vector space. V can be provided with a decomposition similar to (4.1). More precisely,

$$V = \bigoplus_{\beta \in \mathcal{W}} V_\beta, \qquad (4.2)$$

where $\mathcal{W}$ is a subset of the linear forms on $\mathbf{g}_0$. Each *weight space* V_β is characterized by

$$\forall v \in V_\beta, \qquad \forall X \in \mathbf{g}_0, \qquad \varrho(X)(v) = \beta(X)v.$$

and the elements β in $\mathcal{W}$ are called the *weights* of the representation. The dimension of a weight space V_β is called its *multiplicity*. If $\dim V_\beta = 1$ then the weight β is said *simple*. In some sense the adjoint action is a special case of this. So the roots α of the algebra are the weights of the adjoint representation.
The rest of the Lie algebra $\mathbf{g}$ acts on V in the following way

$$\varrho(\mathbf{g}_\alpha)(V_\beta) \subset V_{\beta+\alpha} \qquad \text{if } \alpha + \beta \in \mathcal{W}, \qquad \varrho(\mathbf{g}_\alpha)(V_\beta) = 0 \qquad \text{if } \alpha + \beta \notin \mathcal{W}.$$

Now, the set $\mathcal{R}$ can be decomposed as $\mathcal{R} = \mathcal{R}_+ \cup \mathcal{R}_-$. The roots in $\mathcal{R}_+$ (resp. $\mathcal{R}_-$) are called *positive* (resp. *negative*) roots. This decomposition can be done in such a way that there exists a weight space V_β called a *highest weight space* such that

$$\varrho(E_\alpha)V_\beta = 0 \qquad \text{for all } \alpha \in \mathcal{R}_+. \qquad (4.3)$$

Using this notation the key result is:

THEOREM 4.4. (FULTON AND HARRIS, 1991, PROPOSITION 14.13) *For any semi-simple complex Lie algebra* $\mathbf{g}$ *the following holds.*

(i) *Every finite-dimensional representation on V of* $\mathbf{g}$ *possesses a highest weight space. Take one vector v in this space.*
(ii) *The subspace W of V generated by the images of the highest weight vector v under successive applications of generators* E_α *of root spaces* $\mathbf{g}_\alpha$ *for* $\alpha \in \mathcal{R}_-$ *is an irreducible subrepresentation.*
(iii) *An irreducible representation possesses a unique highest weight vector up to multiplication by scalar, i.e. the dimension of the highest weight space is one.*

The negative roots allow us to determine explicitly a basis of an irreducible representation once that a highest weight vector is determined. It is, however, possible to find a refinement of this method in order to obtain a more efficient way. Indeed, it can be shown that only a subset of $\mathcal{R}_-$ is necessary. More precisely, we call *primitive positive* (*resp. negative*) *roots* the subset of $\mathcal{R}_+$ (resp. $\mathcal{R}_-$) of roots that cannot be expressed by positive (resp. negative) roots. In the previous theorem, $\mathcal{R}_-$ can be replaced by the subset $\mathcal{R}_-^p$ of primitive negatives roots. More precisely,

PROPOSITION 4.5. (FULTON AND HARRIS, 1991, OBSERVATION 14.16) *Any irreducible representation V is generated by the images of its highest weight vector v under successive applications of roots spaces* $\mathbf{g}_\alpha$ *where* α *ranges over the primitive negative roots.*

Furthermore, the highest weight space V_{β_0} is uniquely characterized by the property

$$\varrho(E_\alpha)V_{\beta_0} = 0 \qquad \text{for all } \alpha \in \mathcal{R}_+^p. \qquad (4.4)$$

Two other results are also useful for our construction:

PROPOSITION 4.6. *(a) If a representation is irreducible, its highest weight is simple.*
  (b) Two irreducible representations are equivalent if their highest weights are equal.

The root systems are well known for the semi-simple complex Lie algebras. There are various equivalent ways to determine the sets of positive, negative and primitive roots (negative or positive) as well as classification of the corresponding highest weight space (see, for instance, Fulton and Harris, 1991). Nevertheless, this information can be found in the literature on Lie groups and Lie algebras.

Before closing this section, we need to introduce a bit more terminology. We assume that the representation space V is decomposed as in (4.2) and that V_{β_0} denotes the maximal weight space. Let $\mathcal{R}_-^p = \{\alpha_1, \ldots, \alpha_q\}$ be a set of negative primitive roots. For any weight space V_β, there is a word $P = E_{p_1} E_{p_2} \cdots E_{p_n}$ with $p_i, \ i = 1, \ldots, n$ in $\mathcal{R}_-^p$ such that

$$\varrho(E_{p_1} E_{p_2} \cdots E_{p_n}) V_{\beta_0} \subset V_\beta.$$

For a given weight vector β the length of words $P' = E_{p'_1} \cdot E_{p'_2} \cdots E_{p'_m}$ such that $\varrho(P')(V_{\beta_0}) \subset V_\beta$ is unique (this length is the sum of the coordinates of the point β in the lattice in $\mathbf{g}_0^*$ generated by $\alpha_1, \ldots, \alpha_q$ and with the origin in β_0). We collect all weight spaces of the same length n into a set, called the *nth layer* Δ_n. With this definition, $V_{\beta_0} \in \Delta_0$ as a corollary of proposition (4.5). The layer Δ_{n+1} can be generated by successive applications of elements E_α with α in $\mathcal{R}_-^p$ on the weight spaces of the layer Δ_n. Furthermore, since V is finite dimensional, the number of layers is finite.

4.3. COMPUTING INVARIANTS AND EQUIVARIANTS

We describe in this section an algorithm to determine a vector space basis of the equivariants $f : V \to W$, homogeneous of a certain degree of a connected semi-simple compact Lie group G, acting on finite-dimensional vector spaces V and W of dimensions n and m, respectively, This algorithm does not distinguish between primary and secondary invariants. Nevertheless, Molien series and Gröbner basis may be useful to recover some part of this information.

Let us choose a basis of V consisting of bases for each irreducible component which yields a decomposition of the variables into groups $x = (x^1, \ldots, x^r)$. So the action of G on V is given by $\vartheta : G \to (\mathbb{C}^n)$. Let Θ, ζ, θ be the associated actions as in Section 4.1. On W the choice of the basis respects the irreducible components as well yielding a block diagonal representation $\rho : G \to GL(\mathbb{C}^m), \ \rho(g) = \text{diag}(\rho^1(g), \ldots, \rho^s(g))$. The associated representation of the Lie algebra is denoted $\varrho : \mathbf{g} \to GL(\mathbb{C}^m)$ and is diagonal as well. Additionally we assume that the basis is chosen such that they form a basis of the weight spaces, i.e. in $\mathbb{C}^m$ unit vectors correspond to the elements of the weight spaces. Indexing by the weights β we have the basis $w_{\beta,j}^i, i = 1, \ldots, s, j = 1, \ldots, \dim V_\beta$ where β is a weight of ϱ^i and

$$E_\alpha : w_{\beta,j}^i \to \sum_{k=1}^{\dim V_\gamma} \varrho^i(E_\alpha)_{\beta,j,\alpha+\beta,k} \ w_{\alpha+\beta,k}^i,$$

for all generators E_α of root spaces $\mathbf{g}_\alpha$. Analogously for the generators H_l of the Cartan subalgebra $\varrho^i(H_l)$ is a diagonal matrix with entries $\beta(H_l)$. For both ρ and ϱ we use the

same coordinate system such that $\rho(\exp(g)) = \exp(\varrho(g))$. For ϑ and ζ the same is true. ϑ and ρ describe how in these coordinates $C[x]_\vartheta^\rho$ corresponds to the equivariant polynomial mappings $V \to W$. The following algorithm generalizes the description given in Sattinger (1979) for $SO(3)$.

ALGORITHM 4.7. (COMPUTATION OF GENERIC EQUIVARIANT)

INPUT:

connected semi-simple Lie group given by associated Lie algebra represented by generators H_l of the Cartan subalgebra and primitive positive roots $E_\alpha \in \mathcal{R}_+^p$ and primitive negative roots $E_\alpha \in \mathcal{R}_-^p$,
matrices $\zeta(E_\alpha), \zeta(H_l)$, matrices $\varrho(E_\alpha), \varrho(H_l)$,
degree $\underline{k} = (k_1, \ldots, k_r)$.
OUTPUT: *a vector space basis of $H_{\underline{k}}^N(\mathbb{C}[x]_\vartheta^\rho)$.*

Let $M \subset H_{\underline{k}}^N(\mathbb{C}[x])$ denote the set of monomials of multidegree $\underline{k}$. For $i = 1, \ldots, s$.
A generic homogeneous polynomial is of the form

$$P(x^1, \ldots, x^r) = \sum_{m \in M}^{(i)} a_m^i \cdot m(x)$$

where a_m^i are unknowns. This is an ansatz for the component corresponding to the highest weight space $f_{\beta_0}^i(x) = P(x)$. The other components $f_{\beta,k}^i(x)$ remain undetermined until step (iii).
(ii) The unknowns a_m^i are determined by the following conditions

$$\forall \text{ generators } H_l \qquad \theta(-H_l)(f^i(x)) = \varrho(H_l) \cdot f^i(x),$$

$$\forall \alpha \in \mathcal{R}_+^p \qquad\qquad \theta(E_\alpha)(f^i(x)) = 0.$$

By comparing coefficients in the component $f_{\beta_0}^i$ this gives linear equations in the unknowns a_m^i. Solve this system and substitute the solution into $f_{\beta_0}^i$ which then still depends on a subset of the a_m^i. This determines the layer $\triangle_0$.
(iii) Assume the components $f_{\beta,k}^i$ for all weights β in the layer $\triangle_n$ are known. Then the components $\alpha + \beta, j$ corresponding to the weight spaces in the following layer $\triangle_{n+1}$ are determined by $\alpha \in \mathcal{R}_-^p$ by

$$\theta(-E_\alpha)f^i(x) = \varrho^i(E_\alpha)f^i(x).$$

For $\alpha \in \mathcal{R}_-^p$ and components β, k this means

$$\frac{d}{dx} f_{\beta,k}^i(x) \cdot \zeta(E_\alpha) \cdot x = \sum_{\alpha+\beta,j} \varrho^i(E_\alpha)_{\beta,k,\alpha+\beta,j} f_{\alpha+\beta,j}^i,$$

where on the left-hand side $f_{\beta,k}^i(x)$ are polynomials and $f_{\alpha+\beta,j}^i$ on the right-hand side are unknown components. By linear manipulation this gives the components $f_{\alpha+\beta,j}^i$ of the layer $\triangle_{n+1}$.
Altogether $f = (f^1(x), \ldots, f^s(x))$ is a generic equivariant.

PROOF. This algorithm is a direct application of the results of the previous section. The determination of the component $f_{\beta_0}^i(x)$ is provided by the fact that the maximal weight is in the kernel of all primitive positive roots and is an eigenspace for the elements in the

Cartan subalgebra. Now, the successive applications of all primitive negative roots on the highest weight provides a set of basis of the full representation space W. Each iteration in the algorithm allows us to determine a basis for the $n + 1$-th layer from the knowledge of the n-th layer. As the number of layers is finite, the algorithm reaches necessarily a layer $\Delta_{n'} = \{0\}$ which is empty. As unit vectors correspond to weight spaces the result is an equivariant vector field in the orthonormal basis $\{w^i_{\beta_0}, w^i_{\beta_1,1}, \ldots, w^i_{\beta_q,t_q}, i = 1, \ldots, s\}$. $\square$

REMARK 4.8. (i) For real Lie groups such as $SO(3)$ the method is also applicable. The real associated Lie algebra can be embedded into a complex one by complexification $\mathbf{g}^c = \mathbf{g} \times_R \mathbb{C}$. Now if $\mathbf{g}$ is a simple Lie algebra (i.e. without proper nontrivial ideal) then its complexified $\mathbf{g}^c$ is also simple (see Fulton and Harris (1991)). Then the irreducible representations of $\mathbf{g}$ are just obtained by restriction to the real part of the irreducible representations of $\mathbf{g}^c$.

(ii) For compact Lie groups being generated by a semi-simple connected component G and a finite group H one computes generic G-invariants and G-equivariants. For the generators of H additional linear equations in the generic coefficients are derived and solved. This yields generic invariants and equivariants.

(iii) For groups $G \times H$ which are a direct product with a finite group H the application of the Reynolds projection of H onto a G-invariant yields an invariant. The $G \times H$-equivariants are obtained from the G-equivariants by use of the equivariant Reynolds projection analogously. Concerning the multi-grading observe that less blocks might exist in the diagonalized form of $\vartheta(G \times H)$ than of $\vartheta(G)$. Thus there may exist less grading of the invariant ring and the module of equivariants.

(iv) If G is normal in K, the fundamental K-invariants are obtained from fundamental G-invariants because $N_K(G)/G$ is operating on the vector space of G-invariants and its conjugates. The $N_K(G)/G$-invariants of this action yield the K-invariants, see Kempf (1987), or more readably in Rumberger (1995).

EXAMPLE 4.9. For the representations $l = 1$ and $l = 2$ of $SO(3)$ and degree $k = (2, 3)$ the computation of the generic invariant and generic equivariant takes 148 s and 298 s, respectively.

Algorithm 4.7, together with the algorithms for completeness in Section 3.2, yields an algorithmic determination of fundamental invariants and fundamental equivariants for special compact Lie groups. Details of these algorithms will appear elsewhere.

References

Atiyah, M., MacDonald, I. (1969). *Introduction to Commutative Algebra*. Reading, MA, Addison-Wesley.
Bayer, D., Morrison, I. (1988). Gröbner bases and geometric invariant theory I. *J. Symb. Comput.*, **6,** 209–217.
Bayer, D., Stillman, M. (1992). Computation of Hilbert functions. *J. Symb. Comput.*, **14,** 31–50.

Becker, T., Weispfenning, V. (1993). *Gröbner Bases, a Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics **141**. New York, Springer.

Bröcker, T., tom Dieck, T. (1985). *Representation of Compact Lie Groups.* New York, Springer.

Bruns, W., Herzog, J. (1993). *Cohen–Macaulay Rings.* Cambridge, U.K., Cambridge University Press.

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, (an algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal). Ph. D. Thesis, Mathematics Institute University of Innsbruck, Austria.

Buchberger, B. (1985). Gröbner bases, an algorithmic method in polynomial ideal theory. In Bose, N., ed., *Multidimensional Systems Theory*, Chapter 6, pp. 184–232. Dodrecht, Reidel Publishing Company.

Caboara, M., De Dominicis, G., Robbiano, L. (1996). Multigraded Hilbert functions and Buchberger algorithm. In Lakshman, Y., ed., *ISSAC 96, Proc. 1996 Int. Symp. on Symbolic and Algebraic Computation*, pp. 72–78. New York, ACM.

Campbell, S.A., Holmes, Ph. (1992). Heteroclinic cycles and modulated travelling waves in a system with D_4-symmetry. *Physica D*, **59**, 52–78.

Chossat, P. (1993). Forced reflectional symmetry breaking of an $O(2)$-symmetric homoclinic cycle. *Nonlinearity*, **6,** 723–731.

Chossat, P., Dias, F. (1995). The 1:2 resonance with $O(2)$ symmetry and its applications in hydrodynamics. *Nonlinear Sci.*, **5,** 105–129.

Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. New York, Springer.

Derksen, H. (1997). Computation of invariants for reductive groups. Preprint. Available at ftp://daisy.math.unibas.ch/pub/hderksen/preprints.html.

Eisenbud, D. (1995). *Commutative Algebra with a view Toward Algebraic Geometry*, Graduate Texts in Mathematics **150**. New York, Springer.

Eisenbud, D., Sturmfels, B. (1994). Finding sparse systems of parameters. *J. Pure Appl. Algebra*, **94,** 143–157.

Fulton, W., Harris, J. (1991). *Representation Theory. A first Course*, Graduate Texts in Mathematics **120**. New York, Springer.

Gatermann, K. (1996a). The moregroebner package version 2.0—an improvement of the Gröbner package. A Maple program. Available by www at the address http://www.zib.de/gatermann/moregroebner.html.

Gatermann, K. (1996b). Semi-invariants, equivariants and algorithms. *Appl. Algebra Eng. Commun. Comput.*, **7,** 105–124.

Gatermann, K., Guyard, F. (1997). The symmetry package in Maple. Available by www at the address http://www.zib.de/gatermann/symmetry.html.

Gatermann, K., Lauterbach, R. (1998). Automatic classification of normal forms. *Nonlinear Anal.*, **34,** 157–190.

Gatermann, K., Werner, B. (1996) Secondary Hopf bifurcation caused by steady-state mode interaction. In Chaddam, J., Golubitsky, M., Langford, W. and Wetton, B., eds, *Pattern Formations: Symmetry Methods and Applications*. Dordrecht, Reidel Publishing Company.

Gianni, P., Mora, T., Robbiano, L., Traverso, C. (1996). Multigraded Hilbert functions and Buchberger Algorithm. Preprint 1996.

Golubitsky, M., Stewart, I., Schaeffer, D. G. (1988). *Singularities and Groups in Bifurcation Theory II*, Applied Mathematical Sciences **69**. New York, Springer.

Heydtmann, A. (1997). Finvar.lib, a Singular library to compute invariant rings and more. Available at http://www.mathematik.uni-kl/ zca/Singular. *Demonstration at the workshop on Algorithmic Invariant Theory, Dagstuhl, May 1996.*

Hochster, M., Roberts, J. (1974). Rings of invariants of reductive groups acting on regular rings are Cohen–Macaulay. *Adv. Math.*, **13,** 115–175.

Humphreys, J. (1972, 1982). *Introduction to Lie Algebra and Representation Theory.* New York, Springer.

Humphreys, J. (1975, 1980). *Linear Algebraic Groups.* New York, Springer.

Jaric, M., Michel, L., Sharp, R. (1984). Zeros of covariant vector fields for the point groups: invariant formulation. *J. Physique*, **45,** 1–27.

Kemper, G. (1993). The *invar* package for calculating rings of invariants. Available by ftp from the electronic share library of Maple neptune@inf.ethz.ch, 1993.

Kemper, G. (1996). Calculating invariant rings of finite groups over arbitrary fields. *J. Symb. Comput.*, **21,** 351–366.

Kemper, G., Steel, A. (1997). Some algorithms in invariant theory of finite groups. In Dräxler, P., Michler, G. O., Ringle, C. U., eds, *Proc. Euroconference on Computational Methods for Representations of Groups and Algebra*, Progress in Mathematics. Birkhäuser, Basel. 1998.

Kempf, G. (1987). Computing invariants. In Koh, S. ed., *Invariant Theory*, LNM **1278**. Berlin, Heidelberg, Springer.

Koenig, M. (1997). Linearization of vector fields on the orbit space of the action of a compact Lie group. *Math. Proc. Camb. Phil. Soc.*, **121,** 401–424.

Lari-Lavassani, A., Langford, W., Huseyin, K., Gatermann, K. (1997). Steady-state mode interactions for D_3 and D_4-symmetric systems. Technical Report Preprint FI-NP 1997-009, The Fields Institute. Dynamics of Continuous, Discrete and Impulsive Systems (to appear).

Lauterbach, R., Sanders, J. (1997). Bifurcation analysis for spherically symmetric systems using invariant theory. *J. Dyn. Diff. Eqns* **9**, 535–560.

Leis, C. (1995). Hopf–Verzweigung in Systemen mit sphärischer Symmetrie: Invariante Tori und verbindende Orbits. Ph. D. Thesis, Freie Universität Berlin, Fachbereich Mathematik und Informatik. (In German.)

Macaulay, F. (1927). Some properties of enumeration in the theory of modular systems. *Proc. London Math. Soc.*, **26,** 531–555.

Matthies, K. (1996). The Bogdanov–Takens bifurcation implies chaos in dynamical systems with D_3-symmetry. M.Sc. Thesis (Diplomarbeit), Free University, Berlin.

Mishra, B. (1993). *Algorithmic Algebra*, Texts and Monographs in Computer Science **14**. New York, Springer.

Mora, T., Robbiano, L. (1988). The Gröbner fan of an ideal. *J. Symb. Comput.*, **6,** 183–208.

Robbiano, L. (1985). Term orderings on the polynomial ring. In *EUROCAL 85, European Conference on Computer Algebra Vol. II*, LNCS **204**, pp. 513–517. Springer.

Rumberger, M. (1995). Auffinden von Invarianten in speziellen Fällen. Manuscript (in German).

Rumberger, M., Scheurle, J. (1996). Invariant C^j-functions and center manifold reduction. In Broer, H., van Gils, S., Hoveijn, I. and Takens, F. eds., *Nonlinear Dynamical Systems*, Progress in Nonlinear Differential Equations and Their Applications **19**, pp. 145–153. Basel, Birkhäuser.

Sattinger, D. (1978). Bifurcations from rotationally invariant states. *J. Math. Phys.*, **19,** 1720–1731.

Sattinger, D. (1979). *Group Theoretic Methods in Bifurcation Theory*, LNM **762**. New York, Springer.

Sturmfels, B. (1993). *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation **1**. Wien, Springer.

Sturmfels, B. (1996). *Gröbner Bases and Convex Polytopes*, University Lecture Series **8**. Providence, RI, AMS.

Sturmfels, B., White, N. (1991). Computing combinatorial decompositions of rings. *Combinatorica*, **11,** 275–293.

Weispfenning, V. (1987). Admissible orders and linear forms. *ACM Sigsam Bull.*, **21,** 16–18.

Worfolk, P. (1994). Zeros of equivariant vector fields: algorithms for an invariant approach. *J. Symb. Comput.*, **17,** 487–511.