

# Semi-invariants, equivariants and algorithms

Karin Gatermann

Konrad-Zuse-Zentrum für Informationstechnik Berlin,  
Heilbronner Str. 10  
D-10711 Berlin-Wilmersdorf  
Germany

**Abstract:** The results from invariant theory and the results for semi-invariants and equivariants are summarized in a way suitable for the combination with Gröbner basis computation. An algorithm for the determination of fundamental equivariants using projections and a Poincaré series is described. Secondly, an algorithm is given for the representation of an equivariant in terms of the fundamental equivariants. Several ways for the exact determination of zeros of equivariant systems are discussed.

## 1. Introduction

Symmetry is one of the main principles in nature. Many mathematicians have studied symmetry to explain phenomena and have exploited symmetry to simplify calculations. One distinguishes the abstract group  $G$  and their action on a vector space called linear representation

$$\vartheta : G \rightarrow Gl(\mathbb{C}^n), \quad t \mapsto \vartheta(t), \quad \vartheta(ts) = \vartheta(t)\vartheta(s), \quad \forall s, t \in G, \quad (1)$$

see FÄSSLER, STIEFEL [5] and SERRE [20] for the theory of linear representations. Here we concentrate on finite groups.

While polynomials  $p \in \mathbb{C}[x_1, \dots, x_n]$  with

$$p(\vartheta(t)x) = p(x) \quad \forall t \in G. \quad (2)$$

are called *invariant*, the mappings  $f : \mathbb{C}^n \rightarrow \mathbb{C}^N$  satisfying

$$f(\vartheta(t)x) = \rho(t)f(x) \quad \forall t \in G, \quad (3)$$

are called  $\vartheta$ - $\rho$ -equivariant, where  $\rho$  is a second linear representation. The functions (3) become very important in bifurcation theory and in the context of dynamical systems with symmetry because the dynamics of  $\vartheta$ - $\vartheta$ -equivariant vector fields show very interesting behavior. While the investigation of mode interaction and heteroclinic cycles depends on the structure of the equivariant mapping nowadays the attention is put on chaotic attractors. An  $\vartheta$ - $\rho$ -equivariant mapping with  $\rho \neq \vartheta$  having special properties is used as a detective for the observation of symmetry of chaotic attractors, see [1].

So the algebraic structure of the set of equivariants is interesting. Every equivariant is of the form

$$f(x) = \sum_{\lambda=1}^R A_{\lambda}(\sigma_1(x), \dots, \sigma_n(x)) b_{\lambda}(x), \quad A_{\lambda} \in \mathbb{C}[\sigma_1, \dots, \sigma_n], \quad (4)$$

where the  $\sigma_j$  are so-called *primary invariants* and  $b_i$  are *fundamental equivariants* generating the free module. This structure has e.g. been used in [8].

My starting interest in the algebraic structure of functions (3) was the singularity theory in [10]. This theory is demonstrated only for the easy groups  $Z_2 = \{id, s\}$ ,  $Z_2 \times Z_2$  and an irreducible action of  $D_3$ . Application of this theory to examples of moderate size necessitates support of Computer Algebra. The first part being the computation of the fundamental equivariants.

So the aim of this paper is threefold:

- computation of fundamental equivariants
- representing an equivariant in terms of fundamental equivariants and invariants as in (4)
- solve  $\vartheta$ - $\vartheta$ -equivariant systems  $f(x) = 0$ .

Before giving algorithms a section with theory is presented. Hopefully the summary is helpful for people working in the field of dynamical systems. Emphasis is put on those properties which are needed for computation. The theory of invariants has been well investigated in the end of last century (HILBERT, MOLIEN) and in the beginning of this century (NOETHER [17]). Since this old theory is still relevant and often applied, STURMFELS [23] recently combined invariant theory with the computation of Gröbner bases by the BUCHBERGER-Algorithm. Part of this material is also contained in [4]. For Gröbner bases see e.g. [2], [4].

For  $\vartheta$ - $\vartheta$ -equivariants various results are known: JARIC, MICHEL, SHARP [13], WORFOLK [25], SATTINGER [18]. In contrast to this I present the results on Hilbert series, projections and Cohen-Macaulayness more general for  $\vartheta$ - $\rho$ -equivariants. In this new viewpoint the proofs are based on the analogous results for the semi-invariants to be found in STANLEY [22].

In Section 3 various algorithms are given and their efficiency is discussed. While in [7] the theory of linear representations is used to solve systems of equations also invariants and equivariants can be used. The generators are used in JARIC, MICHEL, SHARP [13] to determine exactly the zeros of an  $\vartheta$ - $\vartheta$ -equivariant system of algebraic equations using invariants. WORFOLK [25] combined this approach with the Buchberger-Algorithm. The structure of the semi-invariants can be used to solve equivariant systems of equations as well. The algorithms are tested for examples and the inconsistent computing times are given.

## 2. The free module of equivariants

In this section we will give the theoretical facts preparing the section on algorithms. Projections, Poincaré series, dimensions of vector spaces, and free modules will be given. We start with summarizing the theory of invariants, see [4], [21], [22], [23].

### Invariants

Let  $\mathbb{C}[x_1, \dots, x_n]$  denote the ring of polynomials in variables  $x_1, \dots, x_n$ .

Let  $\vartheta : G \rightarrow \text{Aut}(\mathbb{C}^n)$  be a linear representation of the group  $G$ . We assume that  $\vartheta$  is faithful and restrict throughout this paper to *finite* groups.

**Definition 2.1** *A polynomial  $p \in \mathbb{C}[x]$  is called invariant, if*

$$p(\vartheta(t)x) = p(x), \quad \forall t \in G.$$

The invariant polynomials form a ring, denoted by  $\mathbb{C}[x]_{\vartheta}$ . From invariant theory [23] one knows that the ring of invariants is generated by some *fundamental invariants*  $\sigma_1, \dots, \sigma_l$ .

In the special case of reflection groups a Theorem by CHEVALLEY [3] states that  $l = n$  fundamental invariants are sufficient, see Theorem 2.8. In general the theory is more complicated. A Theorem by NOETHER gives

bounds for the number of fundamental invariants and their degrees, see [17]. This is important for the algorithmic construction of generators: one may restrict to a finite dimensional vector space.

For an algorithmic construction there are three further important facts. The invariant ring is the image of the *Reynold projector* :

$$P : \mathbb{C}[x] \rightarrow \mathbb{C}[x]_{\vartheta}, \quad P(p(x)) = \frac{1}{|G|} \sum_{t \in G} p(\vartheta(t^{-1})x), \quad p \in \mathbb{C}[x].$$

Since  $D(t)(p(x)) = p(\vartheta(t^{-1})x)$  describes a linear representation  $D$  on  $\mathbb{C}[x]$  the Reynold projector is the projection on the trivial isotypic component, well-known from the theory of linear representations.

The vector space  $M_k$  of homogeneous polynomials of degree  $k$  is an invariant space wrt  $D$ . Thus we have a restricted projection  $P|_{M_k}$ . The dimensions  $m_k = \dim(\mathbb{C}[x]_{\vartheta} \cap M_k)$  are known from the Molien series since the right hand side of (5) can be evaluated easily.

**Theorem 2.2** ([23]) *Let  $m_k = \dim(\mathbb{C}[x]_{\vartheta} \cap M_k)$ . Then the Molien series satisfies*

$$\psi(z) := \sum_{k=0}^{\infty} m_k z^k = \frac{1}{|G|} \sum_{t \in G} \frac{1}{\det(I - z\vartheta(t))}. \quad (5)$$

The most important fact from algorithmic point of view is that of Cohen-Macaulayness.

Let  $R$  be a graded algebra. If the ring  $R$  is finitely generated by  $\sigma_1, \dots, \sigma_n$  as a module, where  $\sigma_j$  are homogeneous and have positive degree, the  $\sigma_j$  are called a *homogeneous system of parameters*. The algebra is called to be *Cohen-Macaulay* if it is a *free* module over every system of homogeneous parameters.

**Theorem 2.3** ([23]) *The invariant ring  $\mathbb{C}[x]_{\vartheta}$  is Cohen-Macaulay.*

This theorem appeared first in [12]. A self-contained proof appeared in [14]. For each homogeneous system of parameters  $\sigma_1, \dots, \sigma_n$  of  $\mathbb{C}[x]_{\vartheta}$  there exists  $\eta_{\nu}, \nu = 1, \dots, r$  with

$$\mathbb{C}[x]_{\vartheta} \cong \bigoplus_{\nu=1}^r \eta_{\nu} \mathbb{C}[\sigma].$$

We choose the ordering in a way that  $\eta_1 = 1$ . The  $\sigma_j$  are called *primary* invariants and the  $\eta_{\nu}$  are called *secondary* invariants. This means that the

Molien series equals

$$\psi(z) = \frac{\sum_{\nu=1}^r z^{\deg(\eta_\nu)}}{\prod_{j=1}^n (1 - z^{\deg(\sigma_j)})}. \quad (6)$$

Once a homogeneous system of parameters is known, the number and degrees of the secondary invariants are given with formula (6). This is the main point of the algorithmic construction of secondary invariants in [23]. For the construction of primary invariants one has to show that the radical of  $(\sigma_1, \dots, \sigma_n)$  is  $(x_1, \dots, x_n)$ , see [23] and Section 3.

**Lemma 2.4** *Let  $\vartheta$  be a linear representation on  $\mathbb{C}^n$  and let  $\sigma_1, \dots, \sigma_n$  be homogeneous invariants. If  $\text{radical}(\sigma_1, \dots, \sigma_n) = (x_1, \dots, x_n)$  then  $\sigma_1, \dots, \sigma_n$  form a homogeneous system of parameters of the ring of invariants.*

**Proof:** The  $\sigma_1, \dots, \sigma_n$  are algebraically independent and thus we can consider  $\text{radical}(\sigma_1, \dots, \sigma_n)$  as a module over  $\mathbb{C}[\sigma_1, \dots, \sigma_n]$ . The radical is finitely generated. Since the radical equals  $(x_1, \dots, x_n)$  and the invariants of positive degree form a subspace of  $(x_1, \dots, x_n)$  the invariant ring is a finitely generated module over  $\mathbb{C}[\sigma_1, \dots, \sigma_n]$ . In other words the invariants form a homogeneous system of parameters. Since the invariant ring is Cohen-Macaulay the invariant ring is free as a module over its subring  $\mathbb{C}[\sigma_1, \dots, \sigma_n]$ . ■

### Isotypic components of $\mathbb{C}[x]$

In order to prepare the theory of equivariants the isotypic components are discussed. Let  $G$  have the irreducible representations  $\vartheta_i, i = 1, \dots, h$ , where  $\vartheta_1$  denotes the unit representation and  $n_i$  is the dimension of  $\vartheta_i$ . Let the character of  $\vartheta_i$  denote by  $\chi_i$ . The group action  $\vartheta$  on  $\mathbb{C}^n$  results in a linear representation  $D$  on  $\mathbb{C}[x]$  given by  $D(t)(p(x)) = p(\vartheta(t^{-1})x)$ . With respect to  $D$  the ring  $\mathbb{C}[x]$  as a vector space has a decomposition in isotypic components  $V_i$ . The invariant ring  $\mathbb{C}[x]_\vartheta$  is the component corresponding to the unit representation  $\vartheta_1$ . The elements of  $V_i, i \neq 1$  are called *semi-invariants* or  *$\vartheta_i$ -invariants*, [22]. Projections onto  $V_i$  are given by

$$P^i(p(x)) = \frac{n_i}{|G|} \sum_{t \in G} \bar{\chi}_i(t) D(t)p(x) = \frac{n_i}{|G|} \sum_{t \in G} \bar{\chi}_i(t) p(\vartheta(t^{-1})x) \quad (7)$$

or if one wants a symmetry adapted basis

$$P^{11}(p) = \frac{n_i}{|G|} \sum_{t \in G} (\vartheta_i(t^{-1}))_{11} D(t)p,$$

and

$$P^{1\mu}(p) = \frac{n_i}{|G|} \sum_{t \in G} (\vartheta_i(t^{-1}))_{1\mu} D(t)p, \quad \mu = 2, \dots, n_i.$$

This is explained in more detail in [5], [20]. The invariance of  $M_k$  wrt  $D$  implies a graded isotypic decomposition

$$M_k = \bigoplus_{i=1}^h (V_i \cap M_k) = \bigoplus_{i=1}^h V_i^k, \quad k = 0, \dots.$$

STANLEY [22] calls the  $\mathbb{C}[x]_{\vartheta}$ -module  $V_i$  a  $Z$ -graded  $\mathbb{C}[x]_{\vartheta}$ -module satisfying

$$M_l V_i^k \subset V_i^{k+l} \quad \forall i, l, k.$$

For the algorithmic treatment of semi-invariants we need the analogues results as for the invariants.

**Theorem 2.5** ([13] p. 3, [22] Thm. 2.1) *Let  $m_k^i$  denote the multiplicity of  $\vartheta_i$  in  $V_i \cap M_k$ . Then the Hilbert series or Poincaré series is*

$$\psi_i(z) := \sum_{k=0}^{\infty} m_k^i z^k = \frac{1}{|G|} \sum_{t \in G} \frac{\bar{\chi}_i(t)}{\det(I - z\vartheta(t))}, \quad (8)$$

where  $\chi_i(t) = \text{trace}(\vartheta_i(t))$  is the character corresponding to the irreducible representation  $\vartheta_i$ .

**Proof:** The proof uses an identification of the space  $M_k$  of homogeneous polynomials of degree  $k$  with a space of tensors. Let  $V := \mathbb{C}^n$  and let  $V^k$  denote the tensor product of  $V$  with itself  $k$  times. A  $k$ -linear mapping  $V^k \rightarrow \mathbb{C}$  is identified with a tensor  $B \in (V^*)^{\otimes k}$ .  $B$  is called *symmetric*, if it is invariant with respect to all permutations of arguments,

$$B(v_1, \dots, v_k) = B(v_{\pi(1)}, \dots, v_{\pi(k)}) \quad \forall \pi \in S_k, v_j \in V,$$

$S_k$  being the symmetric group. The space  $M_k$  is isomorphic to the subspace of symmetric tensors denoted by  $((V^*)^{\otimes k})_s$ .

The given linear representation  $\vartheta : G \rightarrow \text{Aut}(V)$  implies other linear representations. The first is the tensor product (Kronecker product)

$$\vartheta^{\otimes k} : G \rightarrow \text{Aut}(V^k),$$

$$\begin{aligned}\vartheta^{\otimes k}(t) &: V^k \rightarrow V^k, \\ \vartheta^{\otimes k}(t)(v_1 \otimes \cdots \otimes v_k) &= \vartheta(t)v_1 \otimes \cdots \otimes \vartheta(t)v_k.\end{aligned}$$

The representation on  $(V^*)^{\otimes k}$  is isomorphic and thus denoted with the same symbol.

$$\begin{aligned}\vartheta^{\otimes k} &: G \rightarrow \text{Aut}((V^*)^{\otimes k}), \\ \vartheta^{\otimes k}(t)(B(v_1, \dots, v_k)) &= B(\vartheta(t^{-1})v_1, \dots, \vartheta(t^{-1})v_k).\end{aligned}$$

If  $B$  is symmetric, then  $\vartheta^{\otimes k}(t)B$  is symmetric as well. Thus  $((V^*)^{\otimes k})_s$  is invariant wrt  $\vartheta^{\otimes k}$  and the subrepresentation

$$(\vartheta^{\otimes k})_s : G \rightarrow \text{Aut}(((V^*)^{\otimes k})_s)$$

is isomorphic to the group action on  $M_k$ . It has a character denoted by  $\gamma_k^s$ . By the formula for multiplicities

$$m_k^i = \frac{1}{|G|} \sum_{y \in G} \gamma_k^s(y) \bar{\chi}_i(y),$$

where  $\chi_i$  is the character of the irreducible representation  $\vartheta_i$ .

For a fixed  $t \in G$  let  $e_1, \dots, e_n$  be the eigenvectors of  $\vartheta(t)$  with eigenvalues  $\lambda_1, \dots, \lambda_n$ .  $(V^k)_s$  is spanned by the vectors

$$(e_{i_1} \otimes \cdots \otimes e_{i_k})_s = \sum_{\pi \in S_k} e_{i_{\pi(1)}} \otimes \cdots \otimes e_{i_{\pi(k)}}$$

A basis of  $(V^{\otimes k})_s$  is denoted by  $P_{l_1, \dots, l_n}$  with  $l_1 + \cdots + l_n = k$ .

The action of  $(\vartheta^{\otimes k})_s$  on  $P_{l_1, \dots, l_n}$  is

$$(\vartheta^{\otimes k})_s(P_{l_1, \dots, l_n}) = \lambda_1^{l_1} \cdots \lambda_n^{l_n} P_{l_1, \dots, l_n}.$$

Thus the character is

$$\gamma_k^s(t) = \text{trace}((\vartheta^{\otimes k})_s) = \sum_{l_1 + \cdots + l_n = k} \lambda_1^{l_1} \cdots \lambda_n^{l_n}.$$

This gives

$$\begin{aligned}\sum_{k=0}^{\infty} z^k \gamma_k^s(t) &= \sum_{k=0}^{\infty} \sum_{l_1 + \cdots + l_n = k} (z\lambda_1)^{l_1} \cdots (z\lambda_n)^{l_n} \\ &= \sum_{l_1, \dots, l_n=0} (z\lambda_1)^{l_1} \cdots (z\lambda_n)^{l_n} \\ &= \prod_{i=1}^n \frac{1}{1 - z\lambda_i} \\ &= \frac{1}{\det(I - z\vartheta(t))}\end{aligned}$$

$$\begin{aligned} \sum_{k=0}^{\infty} m_k^i z^k &= \frac{1}{|G|} \sum_{k=0}^{\infty} \left( \sum_{t \in G} \gamma_k^s(t) \bar{\chi}_i(t) \right) z^k \\ &= \frac{1}{|G|} \sum_{t \in G} \frac{\bar{\chi}_i(t)}{\det(I - z\vartheta(t))} \end{aligned}$$

■

**Remark:** This is essential the proof of the Molien series. Only the unit representation is replaced by another irreducible representation. A proof using the same ideas can also be found in [22].

$V_i^k = V_i \cap M_k$  has dimension  $m_k^i \cdot n_i$  where  $n_i$  is the dimension of  $\vartheta_i$ .

**Theorem 2.6** ([13], STANLEY [22]) *Assume  $\sigma_1, \dots, \sigma_n$  are primary invariants for  $\mathbb{C}[x]_{\vartheta}$ . Then the isotypic components  $V_i, i = 2, \dots, h$  are modules finitely-generated and free over  $\mathbb{C}[\sigma_1, \dots, \sigma_n]$ .*

**Proof:** We use that

$$\mathbb{C}[x] = \bigoplus_{i=1}^h V_i$$

is a direct sum of vector spaces of infinite dimension.

In [23], proof of Thm. 2.3.5, it is shown that  $\mathbb{C}[x]$  is Cohen-Macaulay. Especially this means that  $\mathbb{C}[x]$  is a free module over the ring in the primary invariants. Thus

$$\begin{aligned} \mathbb{C}[x]/(\sigma_1, \dots, \sigma_n) &= \bigoplus_{i=1}^h V_i/(\sigma_1, \dots, \sigma_n), \\ f + \sum_{j=1}^n h_j \sigma_j &= \sum_{i=1}^h \left( P^i(f) + \sum_{j=1}^n P^i(h_j) \sigma_j \right), \end{aligned}$$

is a direct sum of finite vector spaces. The projections  $P^i$  (7) are  $\mathbb{C}[x]_{\vartheta}$ -module homomorphism. Thus a basis can be chosen consisting of homogeneous polynomials which are elements of either one of the  $V_i$ . So

$$V_i = \bigoplus_{\nu=1}^{r_i} \bigoplus_{\mu=1}^{n_i} \eta_{\nu\mu} \mathbb{C}[\sigma_1, \dots, \sigma_n].$$

■



**Theorem 2.7** ([22], Proposition 4.9) *Let  $\vartheta$  be a linear representation of a finite group  $G$  and assume that  $\sigma_1, \dots, \sigma_n$  are the primary invariants. Then the group action on  $\mathbb{C}[x]/(\sigma_1, \dots, \sigma_n)$  is  $t$  times the regular representation.*

CHEVALLEY [3] proved much earlier a special case of Theorem 2.7 with  $t = 1$ .

**Theorem 2.8** ([3]) *Let  $\vartheta$  be a linear representation of a finite group  $G$  and assume that  $\sigma_1, \dots, \sigma_n$  are the primary invariants. Assume that  $\vartheta(G)$  is generated by reflections with respect to hyperplanes. Then the group action on  $\mathbb{C}[x]/(\sigma_1, \dots, \sigma_n)$  is isomorphic to the regular representation.*

Since the regular representation decomposes like  $\sum_{i=1}^h n_i \vartheta_i$ , it follows from Theorem 2.7 for the number of generators of  $V_i$  that

$$r_i \cdot n_i = t \cdot n_i \cdot n_i.$$

Of course  $t$  depends on the choice of the primary invariants. The degrees of  $\eta_{\nu\mu}$  can be read off from  $\psi_i(z) \cdot \prod_{j=1}^n (1 - z^{\deg(\sigma_j)})$ .

## Equivariants

Now we consider the module of equivariants. A lot of results are very similar to those for the invariant ring. They are deduced from the results for the isotypic components.

Let  $\mathbb{C}[x_1, \dots, x_n]^N$  denote the module of polynomial mappings with  $N$  components. Let  $\rho : G \rightarrow \text{Aut}(\mathbb{C}^N)$  be a linear representation.

**Definition 2.9** *A polynomial mapping is called  $\vartheta$ - $\rho$ -equivariant, if*

$$p(\vartheta(t)x) = \rho(t)p(x) \quad \forall t \in G.$$

For  $\rho = \vartheta$  we obtain what in bifurcation theory is normally called  $G$ -equivariant.

**Example 2.10** *The detectives ([1]) already mentioned in the introduction are examples for  $\vartheta$ - $\rho$ -equivariants.*

**Example 2.11** *A second example is given by the matrices which commutes, i.e.  $S(\vartheta(t)x) = \vartheta(t)S(x)\vartheta(t^{-1})$ ,  $S \in \mathbb{C}[x]^{n,n}$ . They are important in bifurcation theory because Jacobians of equivariant vector fields have this property*

and degeneracies of the Jacobian are conditions for singular points. Every commuting matrix is isomorphic to a  $\vartheta$ - $\rho$ -equivariant, where  $\rho : G \rightarrow \text{Aut}(\mathbb{C}[x]^{n^2})$  is given by the tensor product  $\rho = \vartheta \times \vartheta^*$  of two linear representations  $\vartheta$  and the contragradient representation  $\vartheta^* : G \rightarrow \text{Aut}(\mathbb{C}^n)$ ,  $\vartheta^*(t) = \vartheta(t^{-1})^t$ . Obviously,  $\vartheta^* = \vartheta$  for orthogonal representations  $\vartheta$ .

The equivariant mappings form a module  $\mathbb{C}[x]_\vartheta^\rho$  over the ring of invariants  $\mathbb{C}[x]_\vartheta$ . For finite groups the module of equivariants is finitely generated by some fundamental equivariants  $b_1, \dots, b_l$ .

It is well-known that for reflection groups the gradients  $\frac{d}{dx}\sigma_j(x)$ ,  $j = 1, \dots, n$  generate the module of  $\vartheta$ - $\vartheta$ -equivariants, which in [13] is derived with Theorem 2.8. This result is more general valid for connected compact Lie groups which was shown by SCHWARZ in [19] by using Theorem 2.8 as well. This result was used for example by FIELD and RICHARDSON [6].

For reflection groups also the other modules of  $\vartheta$ - $\rho$ -equivariants are free modules over the invariant ring.

In [25] for arbitrary finite groups the NOETHER degree bound is generalized to  $\vartheta$ - $\vartheta$ -equivariants. A similar bound is valid for  $\vartheta$ - $\rho$ -equivariants as well.

A projection on the  $\vartheta$ - $\rho$ -equivariants is given by  $P^{\vartheta, \rho} : \mathbb{C}[x]^N \rightarrow \mathbb{C}[x]_\vartheta^\rho$

$$P^{\vartheta, \rho}(p(x)) = \frac{1}{|G|} \sum_{t \in G} \rho(t)p(\vartheta(t^{-1})x), \quad p \in \mathbb{C}[x]^N. \quad (9)$$

Similar to the invariant case  $P^{\vartheta, \rho} = \frac{1}{|G|} \sum_{t \in G} D(t)$  is the projection on the trivial component of the linear representation

$$D : G \rightarrow \text{Aut}(\mathbb{C}[x]^N), \quad D(t) = \rho(t)p(\vartheta(t^{-1})x).$$

Let  $M_k^N$  denote the vector space of  $N$ -tuples where the components are homogeneous polynomials of degree  $k$  or are zero. We may write  $M_k^N = (M_k)^N$ . Since  $M_k^N$  is an invariant space wrt  $D$  we can compute with the restriction

$$P_{|M_k^N} : M_k^N \rightarrow M_k^N \cap \mathbb{C}[x]_\vartheta^\rho.$$

**Theorem 2.12** *Let  $m_k = \dim(M_k^N \cap \mathbb{C}[x]_\vartheta^\rho)$ . Then*

$$\psi^\rho(z) := \sum_{k=0}^{\infty} m_k z^k = \frac{1}{|G|} \sum_{t \in G} \frac{\bar{\chi}(t)}{\det(I - z\vartheta(t))}, \quad (10)$$

where  $\chi$  denotes the character of  $\rho$ .

In case  $\rho$  is the unit representation this is the Molien series for the ring of invariants, see [23]. In case  $\rho = \vartheta$  this series was given by SATTINGER [18] and more recently by WORFOLK [25].

**Proof of Theorem 2.12:** The group action  $\rho$  on  $\mathbb{C}^N$  decomposes like  $\sum_{i=1}^h m_i(\rho)\vartheta_i$  where  $m_i(\rho)$  denote the multiplicities. By a suitable change of coordinates in  $\mathbb{C}^N$  using symmetry adapted basis we may assume that a  $\vartheta$ - $\rho$  equivariant  $f$  consists of  $m_i(\rho)$   $\vartheta$ - $\vartheta_i$ -equivariants  $f^{ij} \in \mathbb{C}[x_1, \dots, x_n]_{\vartheta}^{i_j} \subset \mathbb{C}[x_1, \dots, x_n]^{n_i}, j = 1, \dots, m_i(\rho)$ :

$$f = (f^{11}, \dots, f^{1m_1}, f^{21}, \dots, f^{hm_h}).$$

Since we assume a symmetry adapted basis,  $f_1^{ij}, \dots, f_{n_i}^{ij}$  form the vector basis of an irreducible subspace of  $V_i \subset \mathbb{C}[x_1, \dots, x_n]$ . This implies an identification

$$\mathbb{C}[x]_{\vartheta}^{\rho} \simeq \bigoplus_{i=1}^h m_i(\rho)V_i$$

having the Poincaré series  $\sum_{i=1}^h m_i(\rho)\psi_i(z)$ . The character of  $\rho$  is  $\chi = \sum_{i=1}^h m_i(\rho)\chi_i$  which completes the proof. ■

**Theorem 2.13** *If  $\sigma_1, \dots, \sigma_n$  are primary invariants for  $\mathbb{C}[x]_{\vartheta}$  then the module of  $\vartheta$ - $\rho$ -equivariants is finitely-generated and free over  $\mathbb{C}[\sigma_1, \dots, \sigma_n]$ .*

**Proof:** By the proof of Theorem 2.12  $\mathbb{C}[x]_{\vartheta}^{\rho}$  is isomorphic to  $\bigoplus_{i=1}^h m_i(\rho)V_i$ . Application of Theorem 2.6 completes the proof. ■

The degrees of the homogeneous generators can be read off from

$$\psi^{\rho}(z) \cdot \prod_{j=1}^n (1 - z^{\deg(\sigma_j)}) = c_1 z^{d_1} + \dots + c_l z^{d_l}.$$

By Theorem 2.7 the number of generators is

$$\sum_{i=1}^h t n_i \cdot m_i(\rho).$$

### 3. Algorithms

The algorithms in this section consider the computation of fundamental equivariants and the representation of an equivariant in terms of fundamental invariants and equivariants. They make use of the Buchberger algorithm

available in a lot of Computer Algebra systems. For details on the Buchberger algorithm see [2] or [4].

### Primary invariants

We start with recalling the computation of primary invariants using Lemma 2.4.

**Algorithm 3.14** (*Computation of primary invariants*)

**Input:** linear representation  $\vartheta$  of dimension  $n$

**Output:** primary invariants  $\sigma_1, \dots, \sigma_n$

Compute  $n$  invariants  $\sigma_1, \dots, \sigma_n$  (e.g. with the Reynold projector)  
if  $\text{radical}(\sigma_1, \dots, \sigma_n) = (x_1, \dots, x_n)$  then  $\sigma_1, \dots, \sigma_n$  are primary invariants  
else try another set.

Algorithm 3.14 is a simplified version of an algorithm in [23]. The radical test can be done with the Buchberger algorithm (Algorithm 2.5.1 in [23]).

**Algorithm 3.15** (*Check whether  $f \in \text{radical}(h_1, \dots, h_l)$* )

**Input:** polynomials  $h_1, \dots, h_l$   
polynomial  $f$

Introduce a new variable  $z$  and compute the Gröbner basis  $\mathcal{G}$   
of  $(h_1, \dots, h_l, fz - 1)$ .  
If  $1 \in \mathcal{G}$  then  $f \in \text{radical}(h_1, \dots, h_l)$ .

Due to the use of the Buchberger algorithm this radical test may happen to be time consuming.

## Fundamental equivariants

**Algorithm 3.16** (*Computation of a free module basis of  $\vartheta$ - $\rho$ -equivariants*)

**Input:** primary invariants  $\sigma_1, \dots, \sigma_n$ ,  
linear representations  $\vartheta, \rho$  of dimension  $n, N$ , respectively.  
**Output:** free module basis  $b_1, \dots, b_r$  of  $\vartheta$ - $\rho$ -equivariants

$\psi(z) := \text{poincareseries}(\vartheta, \text{character}(\rho));$  Thm. 2.12  
 $\psi(z) := \psi(z) \cdot \prod_{j=1}^n (1 - z^{\deg(\sigma_j)})$   
 $\quad = c_1 z^{d_1} + \dots + c_l z^{d_l}$   
 $B := \emptyset$   
for  $j := 1 : l$  do  
     $M :=$  vector space basis of  $M_{d_j}^N$   
    while  $c_j > 0$  and  $M \neq \emptyset$   
         $p :=$  next\_p\_in  $M$ ;  $M := M \setminus \{p\}$ ;  
         $b :=$  projection( $p$ ); projection  $P^{\vartheta, \rho}$   
        if  $b \neq 0$  and  
             $b$  independent of  $B$  over  $\mathbb{C}[\sigma_1, \dots, \sigma_n]$  Algorithm 3.17  
            then  $B := B \cup \{b\}$ ;  
             $c_j := c_j - 1$ ;  
        endif  
    endwhile  
    if  $c_j \neq 0$  write 'something wrong';  
endfor

**Algorithm 3.17** (*Test whether  $b \in \bigoplus_{\lambda} b_{\lambda} \mathbb{C}[\sigma_1, \dots, \sigma_n]$* )

**Input:** primary invariants  $\sigma_1(x), \dots, \sigma_n(x)$   
free module basis  $b_{\lambda}(x), \lambda = 1, \dots, R$ , polynomial vector  $b(x)$   
**Output:** true or false

$B_{\lambda} = \sum_{j=1}^m (b_{\lambda}(x))_j z^j, \lambda = 1, \dots, R$   
 $B = \sum_{j=1}^m (b(x))_j z^j$   
Compute Gröbner basis  $\mathcal{G}_0$  of  $(\beta_{\lambda} - B_{\lambda}, \sigma_j - \sigma_j(x))$   
wrt  $x_1 > \dots > x_n > z > \beta_1 > \dots, \beta_R > \sigma_1 > \dots > \sigma_n$   
Reduce  $B$  modulo  $\mathcal{G}_0$  to  $g$ .  
if  $g \in \mathbb{C}[\beta, \sigma]$  then true else false.

Algorithm 3.16 describes the computation of fundamental  $\vartheta$ - $\rho$ -equivariants using the Poincaré series in order to get the degrees. In case  $\rho$  is the unit representation this algorithm equals the algorithm for the computation of secondary invariants (Algorithm 2.5.14 in [23]).

A variant is possible: First compute the fundamental  $\vartheta$ - $\vartheta_i$ -equivariants,  $i = 1, \dots, h$  where  $m_i(\rho) > 0$ . By change of coordinates they give all fundamental  $\vartheta$ - $\rho$ -equivariants. This makes clear that Algorithm 3.16 is better than the Algorithm in [25] which is restricted to  $\vartheta$ - $\vartheta$ -equivariants and uses linear algebra technique.

Algorithm 3.17 checks whether  $b$  is an element of a free module

$$\bigoplus_{\lambda} b_{\lambda} \mathbb{C}[\sigma_1, \dots, \sigma_n].$$

For the involved Gröbner computation a module version is helpful. Then the  $\beta_j$  are defined to be module variables. In [14] it is proposed to do this by means of linear algebra. A test whether  $b$  is an element of the vector space formed by  $b_{\lambda}(x)\sigma_1^{d_1}(x) \cdots \sigma_n^{d_n}(x)$  of degree equal to the degree of  $b$  is performed by solving a system of linear equations obtained by comparing coefficients.

### Representing a given equivariant

**Algorithm 3.18** (*representation of one  $\vartheta$ - $\rho$ -equivariant in fundamental invariants and fundamental equivariants*)

**Input:**  $p(x) \in \mathbb{C}[x]_p^{\rho}$ , primary invariants  $\sigma_1(x), \dots, \sigma_n(x)$ ,  
free module basis  $b_{\lambda}(x)$ ,  $\lambda = 1, \dots, R$

**Output:**  $A_{\lambda}(\sigma) \in \mathbb{C}[\sigma_1, \dots, \sigma_n]$  such that  
$$p(x) = \sum_{\lambda=1}^R A_{\lambda}(\sigma_1(x), \dots, \sigma_n(x)) b_{\lambda}(x)$$

use a help variable  $z$

$$B := \sum_{j=1}^N p_j(x) z^j$$

$$B_{\lambda} := \sum_{j=1}^m (b_{\lambda}(x))_j z^j, \lambda = 1, \dots, R$$

Compute a Gröbner basis of the ideal generated by

$$\beta - B(x, z), \beta_{\lambda} - B_{\lambda}(x, z), \lambda = 1, \dots, R, \sigma_j - \sigma_j(x), j = 1, \dots, n$$

with respect to the lexicographic ordering and

$$\sigma_1 < \cdots < \sigma_n < \beta_1 < \cdots < \beta_R < \beta < z < x_1 < \cdots < x_n$$

The polynomial in the Gröbner basis in  $\mathbb{C}[\beta, \beta_1, \dots, \beta_R, \sigma_1, \dots, \sigma_n]$  is

$$\beta - \sum_{\lambda=1}^R A_{\lambda}(\sigma) \beta_{\lambda}$$

**Algorithm 3.19** (*Representation of several  $\vartheta$ - $\rho$ -equivariants in fundamental invariants and fundamental equivariants*)

**Input:**  $p_1(x), \dots, p_l(x) \in \mathbb{C}[x]_{\vartheta}^{\rho}$ , primary invariants  $\sigma_1(x), \dots, \sigma_n(x)$ ,  
free module basis  $b_{\lambda}(x), \lambda = 1, \dots, R$

**Output:**  $p_j = \sum_{\lambda=1}^R A_{\lambda}^j(\sigma_1, \dots, \sigma_n) b_{\lambda}, j = 1, \dots, l$

use a help variable  $z$

$$B_{\lambda} := \sum_{j=1}^N (b_{\lambda}(x))_j z^j, \lambda = 1, \dots, R$$

Compute a Gröbner basis  $\mathcal{G}_0$  of the ideal generated by

$$\beta_{\lambda} - B_{\lambda}(x, z), \lambda = 1, \dots, R, \sigma_j - \sigma_j(x), j = 1, \dots, n$$

with respect to the lexicographic ordering and

$$\sigma_1 < \dots < \sigma_n < \beta_1 < \dots < \beta_R < z < x_1 < \dots < x_n$$

for each  $j = 1, \dots, l$

$$B := \sum_{i=1}^m (p_j(x))_i z^i$$

$$B(x, z) \rightarrow_{\mathcal{G}_0} P(\beta_1, \dots, \beta_R, \sigma_1, \dots, \sigma_n)$$

Algorithm 3.18 is more or less the inverse of Algorithm 3.16. If  $\rho$  is the unit representation the help variable  $z$  is not necessary. When several representations are needed, it seems to be appropriate to compute one Gröbner basis in advance (Algorithm 3.19). The difference is that a Gröbner basis of  $(\sigma_j - \sigma_j(x)), j = 1, \dots, n, \eta_{\nu}, \nu = 2, \dots, r$  is computed first and then used in the second Gröbner calculation. But computational experience shows that Algorithm 3.19 is not necessarily faster than Algorithm 3.18 although on a naive level one may have this impression. The point is that a Gröbner basis  $\mathcal{G}_0$  of  $(\sigma_j - \sigma_j(x), \beta_{\lambda}(x) - B_{\lambda}(x))$  is not appropriate to the symmetry of the problem. The reduction  $p(x) \rightarrow_{\mathcal{G}_0} P(\sigma, \beta)$  eventually needs more steps than a reduction which also uses the polynomials  $\sigma_j - \sigma_j(x), \beta_{\lambda}(x) - B_{\lambda}(x)$  itself.

In case of equivariants it might be helpful to use a module version of Gröbner, to define the variables  $\beta_j$  as module variables and to choose a weighted ordering.

An alternative to Algorithm 3.18 and 3.19 would be a method based on linear algebra techniques, but using the Buchberger algorithm is the elegant way.

**Algorithm 3.20** (*Computation of syzygies*)

**Input:** primary invariants  $\sigma_1(x), \dots, \sigma_n(x)$ ,

secondary invariants  $\eta_2, \dots, \eta_r$

**Output:**  $\eta_\mu \eta_\lambda = \sum_{\nu=1}^r \eta_\nu A_\nu(\sigma)$ ,  $\mu = 2, \dots, r$ ,  $\lambda = 2, \dots, r$

Apply Algorithm 3.18 or 3.19 to  $p(x) = \eta_\mu(x)\eta_\lambda(x)$  with  $\rho$  equal to the unit representation, without using the help variable  $z$ .

**Algorithm 3.21** (Representation of a polynomial in primary invariants and free module basis of the polynomial ring)

**Input:**  $p(x) \in \mathbb{C}[x]$ ,  
primary invariants  $\sigma_j(x)$ ,  $j = 1 \dots, n$

**Output:**  $p = A(x, \sigma)$

Compute a Gröbner basis of the ideal generated by  $\beta - p(x)$ ,  $\sigma_1 - \sigma_1(x)$ ,  $\dots$ ,  $\sigma_n - \sigma_n(x)$  wrt the lexicographical ordering and  $\sigma_1 < \dots < \sigma_n < \beta < x_1 < \dots < x_n$ . The polynomial which is linear in  $\beta$  describes a relation

$$\beta - \sum_{i=1}^h \sum_{\nu=1}^{r_i} \sum_{\mu=1}^{n_i} A_{\nu\mu}^i(\sigma) \eta_{\nu\mu}^i(x)$$

where  $\eta_{\nu\mu}^i(x)$  generate  $\mathbb{C}[x]$  over  $\mathbb{C}[\sigma_1, \dots, \sigma_n]$  as a module.

**Remark:** The algorithms of this section can be improved by choosing a problem adapted term ordering. The Gröbner package of REDUCE allows to define various orderings.

## 4. Solving symmetric algebraic systems

In this section we apply the results from the previous sections to the exact solution of a system of equations

$$f(x) = 0, \quad f \in \mathbb{R}[x_1, \dots, x_n]^n$$

where  $f$  is  $\vartheta$ - $\vartheta$ -equivariant. We restrict to real representations:  $\vartheta(t)$ ,  $t \in G$  are assumed to be orthogonal matrices. Then also the fundamental invariants and fundamental equivariants may be assumed to have real coefficients.

An interesting connection to common zeros of invariant polynomials is known:



**Theorem 4.22** ([13], see also [25]) *Let  $\vartheta$  be an orthogonal representation of a finite group  $G$  and let the fundamental  $\vartheta$ - $\vartheta$ -equivariants denote by  $b_1, \dots, b_R \in \mathbb{R}[x]_{\vartheta}^{\vartheta}$ . Let  $f$  be another  $\vartheta$ - $\vartheta$ -equivariant. The real zeros of  $f(x) = 0$  are exactly the common real zeros of the invariant polynomials*

$$b_{\lambda}^t(x)f(x) = 0, \quad \lambda = 1, \dots, R.$$

If one is also interested in the complex solutions one has to demand  $\bar{b}_{\lambda}^t f = 0, \lambda = 1, \dots, R$ . Based on Theorem 4.22 WORFOLK [25] proposed to proceed in several steps:

- express  $b_{\lambda}^t f$  in terms of invariants by means of linear algebra techniques:

$$b_{\lambda}^t(x)f(x) = F_{\lambda}(\sigma_1(x), \dots, \sigma_n(x), \eta_1(x), \dots, \eta_r(x)), \quad \lambda = 1, \dots, R.$$

- Find all real solutions  $(\tilde{\sigma}, \tilde{\eta})$  of  $F_1(\sigma, \eta) = 0, \dots, F_R(\sigma, \eta) = 0$  with Gröbner bases technique.
- Find all real solutions of  $\sigma(x) = \tilde{\sigma}, \eta(x) = \tilde{\eta}$  for each solution  $(\tilde{\sigma}, \tilde{\eta})$ .

A much simpler method doing the steps simultaneously is given in the following algorithm.

**Algorithm 4.23** (*Solution of an equivariant system*)

**Input:**  $\vartheta$ - $\vartheta$  equivariant mapping  $f$ ,  
primary invariants  $\sigma_j, j = 1, \dots, n$ ,  
secondary invariants  $\eta_{\nu}, \nu = 1, \dots, r$   
fundamental equivariants  $b_{\lambda}, \lambda = 1, \dots, R$ .

**Output:** Real solutions of  $f(x) = 0$ .

Compute a Gröbner basis  $\mathcal{G}$  of the ideal generated by  $b_{\lambda}^t(x)f(x), \lambda = 1, \dots, R, \sigma_j - \sigma_j(x), j = 1, \dots, n, \eta_{\nu} - \eta_{\nu}(x), \nu = 2, \dots, r$  with respect to the ordering  $\sigma_1 < \dots < \sigma_n < \eta_1 < \dots < \eta_r < x_1 \dots < x_n$ .

Compute the real solutions of  $\mathcal{G}$ .

Secondly, one can use the results in Section 2 on the isotypic components. Theorem 2.6 shows that each  $f_k(x), k = 1, \dots, n$  has a representation

$$f_k(x) = \sum_{i=1}^h \sum_{\mu=1}^{r_i} \sum_{\nu=1}^{n_i} \eta_{\nu\mu}(x) B_{\nu\mu}^i(\sigma(x)), \quad k = 1, \dots, n.$$

Let  $J = (\sigma_1 - \sigma_1(x), \dots, \sigma_n - \sigma_n(x))$ .

$$F_k(x, \sigma) = \sum_{i=1}^h \sum_{\mu=1}^{r_i} \sum_{\nu=1}^{n_i} \eta_{\nu\mu}(x) B_{\nu\mu}^i(\sigma) \in \mathbb{R}[x, \sigma], \quad k = 1, \dots, n, \quad (11)$$

are the representatives of  $f_k$  in  $\mathbb{R}[x, \sigma]/J$  with the lowest degree in  $x$ . Then the Gröbner bases of the ideal generated by

$$F_k(x, \sigma), \quad k = 1, \dots, n, \quad \sigma_j - \sigma_j(x), \quad j = 1, \dots, n,$$

wrt the lexicographical ordering  $x_1 < \dots < x_n < \sigma_1 < \dots < \sigma_n$  contains the information on the solutions. This suggests a two-step algorithm where the representation (11) is computed with Algorithm 3.21. A better way is a Gröbner computation in one step:

**Algorithm 4.24** (*Solution of equivariant system of algebraic equations*)

**Input:**  $\rho$ - $\vartheta$ -equivariant  $f \in \mathbb{R}[x]_{\vartheta}^{\rho}$ ,  
primary invariants  $\sigma_j(x), j = 1, \dots, n$   
**Output:** solutions of  $f(x) = 0$ .

Compute a Gröbner basis  $\mathcal{G}$  of the ideal generated by

$$f_k(x), k = 1, \dots, n, \quad \sigma_j - \sigma_j(x), j = 1, \dots, n$$

wrt the lexicographical ordering  $\sigma_1 < \dots < \sigma_n < x_1 < \dots < x_n$ .

Then solve  $\mathcal{G}$ .

The advantage of Algorithm 4.24 is that the fundamental equivariants are not needed. This allows to generalize to  $\vartheta$ - $\rho$ -equivariant mappings,  $\vartheta \neq \rho$ . In contrast to Algorithm 4.23 also the complex solutions are determined.

In both Algorithms 4.23 and 4.24 a Gröbner basis of  $(\sigma_j - \sigma_j(x))$  is included. By this fact it is important to choose primary invariants such that the Gröbner basis of  $(\sigma_j - \sigma_j(x))$  is computed easily. The choice influences the computing times of Algorithms 4.23 and 4.24 a lot.

**Example 4.25** (*Cyclohexane*) A. DRESS described the deformation of the cyclic hydrogen molecule with six nodes in three-space with three variables (essentially the distances) and four equations:

$$\begin{aligned} f_1(x_1, x_2, x_3) &:= f_3(x_2, x_3, x_1), \\ f_2(x_1, x_2, x_3) &:= f_1(x_2, x_3, x_1), \end{aligned}$$

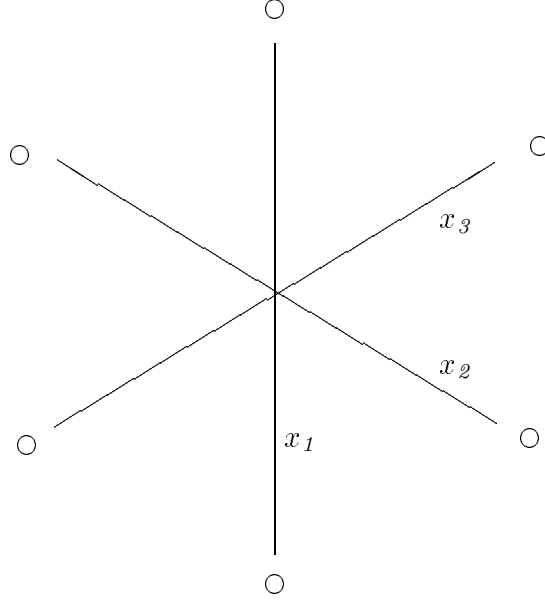


Figure 1: Geometry of the Cyclohexane. 3 distances describe the deformation in the three-dimensional Euclidean space.

$$\begin{aligned}
 f_3(x_1, x_2, x_3) &:= \det \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 8/3 & x_1 & 8/3 \\ 1 & 1 & 0 & 1 & 8/3 & x_2 \\ 1 & 8/3 & 1 & 0 & 1 & 8/3 \\ 1 & x_1 & 8/3 & 1 & 0 & 1 \\ 1 & 8/3 & x_2 & 8/3 & 1 & 0 \end{pmatrix}, \\
 f_4(x_1, x_2, x_3) &:= \det \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 8/3 & x_1 & 8/3 & 1 \\ 1 & 1 & 0 & 1 & 8/3 & x_2 & 8/3 \\ 1 & 8/3 & 1 & 0 & 1 & 8/3 & x_3 \\ 1 & x_1 & 8/3 & 1 & 0 & 1 & 8/3 \\ 1 & 8/3 & x_2 & 8/3 & 1 & 0 & 1 \\ 1 & 1 & 8/3 & x_3 & 8/3 & 1 & 0 \end{pmatrix}, \tag{12}
 \end{aligned}$$

In [16] this problem was solved without exploiting the symmetry. The symmetry is given by the dihedral group  $D_3 = \{id, r, r^2, s, sr, sr^2\}$  acting on the

problem with representations  $\vartheta$  and  $\rho$ ,

$$\vartheta(r) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \vartheta(s) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \rho(t) = \begin{pmatrix} \vartheta(t) & 0 \\ 0 & 1 \end{pmatrix}, \forall t \in D_3.$$

$F = (f_1, f_2, f_3, f_4)$  is  $\vartheta$ - $\rho$ -equivariant. Because  $f = (f_1, f_2, f_3)$  is  $\vartheta$ - $\vartheta$ -equivariant, a variant of Algorithm 4.23 applies. Because  $\vartheta(G)$  is generated by reflections there are three fundamental invariants. They are

$$\sigma_1(x) = x_1 + x_2 + x_3, \sigma_2(x) = x_1^2 + x_2^2 + x_3^2, \sigma_3(x) = x_1^3 + x_2^3 + x_3^3$$

and the fundamental equivariants are  $b_i = \frac{d\sigma_i}{dx}$ ,  $i = 1, 2, 3$ . By Theorem 4.22 the first way of solution is to compute the Gröbner basis of the ideal generated by

$$x_1^k f_1(x) + x_2^k f_2(x) + x_3^k f_3(x), \quad k = 0, 1, 2, \quad f_4(x), \quad \sigma_i - \sigma_i(x), \quad i = 1, 2, 3.$$

Table 1 compares this variant of Algorithm 4.23 with Algorithm 4.24 and the Gröbner computation without use of symmetry. In all three computations we have used the Gröbner package of REDUCE [15] with the factorizing possibilities and with restriction to positive solutions. The lexicographical ordering has been chosen. Although in Algorithm 4.24 the number of variables is extended, it is as fast as the Gröbner computation without use of symmetry. Another improvement could be made by choosing a sophisticated ordering which is supported by REDUCE. The second advantage of Algorithm 4.24 is that the solution structure shown in Figure 2 is much clearer than without use of symmetry, compare with [16]. The one-dimensional variety of solutions is parametrized by the first invariant  $\sigma_1$ .

For comparison, Table 2 shows the computing times for REDUCE (without factorizer), Maple, and Mathematica. Without factorization possibilities Algorithm 4.23 is better than Gröbner without use of symmetry. In the column for Algorithm 4.24 one recognizes that the implementation of the Gröbner package has been improved in REDUCE 3.5.

**Example 4.26** A class of problems is given by a Lotka-Volterra equation. The interior critical points satisfy

$$1 - cx_i + \sum_{j=1}^n \delta_{ij} x_i x_j^2 = 0, \quad 1 \leq i \leq n,$$

```

{{3*x1 - 11,
  3*x2 - 11,
  3*x3 - 11,
  9*sigma3 - 1331,
  3*sigma2 - 121,
  sigma1 - 11}},
{- sigma1 + x1 + x2 + x3,
 - 3*sigma1*x2 - 3*sigma1*x3 + 22*sigma1 + 3*x22 + 3*x2*x3 + 3*x32
 - 121,
 - 27*sigma1*x32 + 198*sigma1*x3 - 75*sigma1 + 27*x33 - 1089*x3
 - 250,
 - 9*sigma13 + 198*sigma12 - 1164*sigma1 + 9*sigma3 - 250,
 - 3*sigma12 + 44*sigma1 + 3*sigma2 - 242}}

```

Figure 2: Gröbner bases of the Cyclohexane problem.

	Gröbner	Algorithm 4.23	Algorithm 4.24
REDUCE develop. v. IBM RISC 6000	1.8 s	2.4 s	1.7 s
REDUCE develop. v. Sun 4	2.2 s	2.7 s	2.2 s
REDUCE 3.4.1 sparc4/70	1.9 s	2.4 s	1.8 s

Table 1: Computing times of Gröbner package for Cyclohexane with REDUCE. The factorizer and the restriction to positive solutions have been used.

	Gröbner	Algorithm 4.23	Algorithm 4.24
REDUCE develop. v. IBM RISC 6000	3.3 s	3.1 s	9.4 s
Maple HP 730	5.7 s	2.5 s	32 s
REDUCE 3.4.1 sparc4/70	1.3 s	0.8 s	—
Maple sparc4/70	8.6 s	3.7 s	47.2 s
Mathematica sparc4/70	3.8 s	2.9 s	—

Table 2: Computing times for Cyclohexane with REDUCE, Maple, Mathematica.

	Gröbner without sym.	Algorithm 4.23	Algorithm 4.24
without fact.	453 s	2.1s	6.0 s
with fact.	207 s	4.7 s	–

Table 3: Computing times for a Lotka-Volterra system with REDUCE on a IBM.

where the connection matrix is defined as

$$\delta_{ij} = \begin{cases} 0 & \text{if } i = j \\ 1 & \text{if } j \leq p, i \neq j, i \leq i \leq n, \\ -1 & \text{if } j > p, i \neq j, \end{cases}$$

For  $p = 3$  and  $n = 3$  the system has the symmetry of  $D_3$ . As in Example 4.25 the system is  $\vartheta$ - $\vartheta$ -equivariant with the same  $\vartheta$ . This means that the fundamental invariants and equivariants can be taken from Example 4.25. In Table 3 we give the computing times for the Gröbner computation without use of symmetry, with use of the equivariants and without equivariants, but with invariants. Because of the additional parameter  $c$  Algorithm 4.23 without factorization is faster than with. The Algorithm 4.23 is best in contrast to Example 4.25 with use of factorization where it is the worst.

## Conclusion

We showed how to compute the fundamental equivariants. These fundamental equivariants generate the module of equivariants over the ring in the primary invariants. Since these computations are usually done by hand, the computing times are not that relevant. The reliability of the computations and the fact that pencil and paper mathematics is automated is much more important than the performance.

The second topic of this paper is to find all solutions of a symmetric system of equations using invariants. An approach based on the theory of linear representations has already been given in [7]. The examples in this paper are overdetermined or depend on a parameter such that other methods than the Buchberger algorithm do not apply. If one is interested in all solutions of a system without parameters we also recommend mixed symbolic-numeric methods such as presented in [24]. In the examples presented here the use of invariants and equivariants are sometimes successful and sometimes not. The enlargement of the number of variables by using invariants means in

principle a dramatic enlargement of the complexity of the computation of Gröbner bases. Nevertheless the Example 4.26 shows that in the presence of parameters this means a huge simplification.

**Acknowledgment:** I thank Reiner Lauterbach for helpful discussions.

## References

- [1] E. Barany, M. Dellnitz, M. Golubitsky. *Detecting the Symmetry of Attractors*. Physica D 67, 66–87, 1993.
- [2] Th. Becker, V. Weispfenning. **Gröbner Bases**, A Computational Approach to Commutative Algebra. In Cooperation with H. Kredel, Springer, New York, 1993.
- [3] C. Chevalley. *Invariants of finite groups generated by reflections*. Amer. J. Math. 77, S. 778–782, 1955.
- [4] D. Cox, J. Little, D. O’Shea. **Ideals, Varieties, and Algorithms**, An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer, New York, 1992.
- [5] A. Fässler, E. Stiefel. **Group Theoretical Methods and Their Applications**. Birkhäuser, Boston, 1992.
- [6] M.J. Field, R.W. Richardson. *Symmetry Breaking and the Maximal Isotropy Subgroup Conjecture for Reflection Groups*. In C. Truesdell (Ed.) *Archive for Rational Mechanics and Analysis* Vol. 105, Springer, Berlin, 1989.
- [7] K. Gatermann. *Symbolic solution of polynomial equation systems with symmetry*. In Sh. Watanabe, M. Nagata (Eds.), Proceedings of ISSAC–90 (Tokyo, Japan, August 20–24, 1990), 112–119. ACM, New York, 1990.
- [8] K. Gatermann, B. Werner. *Secondary Hopf Bifurcation Caused by Steady-state Steady-state Mode interaction*. to appear in J. Chaddam, M. Golubitsky, W. Langford, B. Wetton (Eds.) *Pattern Formations: Symmetry Methods and Applications*, Fields Institute Com. Series, 1994.



- [9] K. Gatermann. A remark on the detection of symmetry of attractors. To appear in P. Chossat (Ed.), *Dynamics, Bifurcation and Symmetry*, Kluwer Academic Publishers, Dordrecht, 1994.
- [10] M. Golubitsky, I. Stewart, D.G. Schaeffer. **Singularities and Groups in Bifurcation Theory**. Vol. **II**, Springer, New York, 1988.
- [11] A.C. Hearn. *REDUCE User's Manual, Version 3.5*. The RAND Corp., Santa Monica, U.S.A. 1993.
- [12] M. Hochster, J.A. Eagon. *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. 93, 1020-1058, 1971.
- [13] M.V. Jaric, L. Michel, R.T. Sharp. *Zeros of covariant vector fields for the point groups: invariant formulation*. J. Physique 45, 1-27, 1984.
- [14] J.M. McShane, L.C. Grove, *Polynomial Invariants of Finite Groups*. to appear in *Algebras, Groups and Geometries*, 1993.
- [15] H. Melenk, H.M. Möller, W. Neun. *GROEBNER A Package for Calculating Groebner Bases*. available with REDUCE 1992.
- [16] H. Melenk, H.M. Möller, W. Neun. *Symbolic solution of large stationary chemical kinetics problems*. Konrad-Zuse-Zentrum, preprint SC 88-7, 1988.
- [17] E. Noether. *Der Endlichkeitssatz der Invarianten endlicher Gruppen*. Math. Ann. 77, 89-92, 1916.
- [18] D.H. Sattinger. *Group Theoretic Methods in Bifurcation Theory*. Lecture Notes in Mathematics 762, Springer, Berlin, Heidelberg, New York, 1979.
- [19] G.W. Schwarz. *Lifting Smooth Homotopies of Orbit Spaces*. In Institut des Hautes Études Scientifiques, Publications Mathématiques 51, 1980.
- [20] J.P. Serre. **Linear Representations of Finite Groups**. Springer, New York, 1977.
- [21] N.J.A. Sloane. *Error-correcting codes and invariant theory: new applications of a nineteenth-century technique*. Amer. Math. Monthly 84, 82-107, 1977.

- [22] R.P. Stanley. *Invariants of finite groups and their applications to combinatorics*. Bulletin Am. Math. Soc. 1, 475-511, 1979.
- [23] B. Sturmfels. **Algorithms in Invariant Theory**. Springer, Wien, 1993.
- [24] J. Verschelde, K. Gatermann. *Symmetric Newton Polytopes for Solving Sparse Polynomial Systems*. Konrad-Zuse-Zentrum, Preprint SC 94-3, 1994. accepted for publication by Advances in Applied Mathematics.
- [25] P.A. Worfolk. *Zeros of equivariant vector fields: Algorithms for an invariant approach*. submitted to J. Symbolic Computation, 1994.