Using symmetries in the eigenvalue method for polynomial systems

Robert M. Corless\textsuperscript{a,1}, Karin Gatermann\textsuperscript{b}, Ilias S. Kotsireas\textsuperscript{c}

\textsuperscript{a} Department of Applied Mathematics, Ontario Research Centre for Computer Algebra, University of Western Ontario, London N6A 5B7, Ontario, Canada

\textsuperscript{b} December 18, 1961 – January 1, 2005, Formerly Canada Research Chair in Computer Algebra, Department of Computer Science, University of Western Ontario, London N6A 5B7, Ontario, Canada

\textsuperscript{c} Department of Physics and Computer Science, Wilfrid Laurier University, 75 University Avenue West, Waterloo N2L 3C5, Ontario, Canada

\textbf{A R T I C L E  I N F O}

Article history:
Received 28 February 2007
Accepted 30 November 2008
Available online 15 May 2009

This paper is dedicated to the memory of Karin Gatermann

\textbf{A B S T R A C T}

One way of solving polynomial systems of equations is by computing a Gröbner basis, setting up an eigenvalue problem and then computing the eigenvalues numerically. This so-called eigenvalue method is an excellent bridge between symbolic and numeric computation, enabling the solution of larger systems than with purely symbolic methods. We investigate the case that the system of polynomial equations has symmetries. For systems with symmetry, some matrices in the eigenvalue method turn out to have special structure. The exploitation of this special structure is the aim of this paper. For theoretical development we make use of SAGBI bases of invariant rings. Examples from applications illustrate our new approach.

© 2009 Published by Elsevier Ltd

\textbf{1. Introduction}

Many systems of polynomial equations arising in applications have symmetry. Typical examples appear in numerical mathematics, e.g. in the construction of quadrature formulas. The conformation of molecules in chemistry is another example which is explained in von zur Gathen and Gerhard (1999). A third example is the $N$-body problem in celestial mechanics (Kotsireas, 2001). The exploitation of symmetry in polynomial systems has been a research topic for many years. An overview of known methods using Gröbner bases and invariant theory is given in Chapter 4.1 in Gatermann (2000).

\textsuperscript{1} Tel.: +1 519 661 2111; fax: +1 519 661 3523.

E-mail addresses: Rob.Corless@uwo.ca (R.M. Corless), ikotsire@wlu.ca (I.S. Kotsireas).

0747-7171/$ – see front matter © 2009 Published by Elsevier Ltd
doi:10.1016/j.jsc.2008.11.009
In this paper we are using the eigenvalue method (Stetter, 1993) which is implemented in Maple V.7 (Char et al., 1991). A description is given in Cox et al. (1998) Chapter 2.4 and Sturmfels (2002) Chapter 2.3. The relation of eigenvalue problems and polynomial system solving was first observed in the context of resultants in Auzinger and Stetter (1988) which is explained in Cox et al. (1998) Chapter 3.6. The papers (Corless et al., 1995; Emiris, 1996; Mourrain, 1998) relate the resultant matrices to the multiplication matrices in the eigenvalue method.

We assume familiarity with Cox et al. (1998) and only briefly recall the notation. Given polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, where $k$ is a computable field, we assume that the ideal $I = \langle f_1, \ldots, f_m \rangle$ has finite codimension such that the quotient ring $k[x]/I$ is a $k$-vector space of finite dimension. This implies that the ideal is zero-dimensional. We choose a basis of this vector space and choose representatives $g_1, \ldots, g_d$ of the equivalence classes. Using a term order we choose the representatives as a linear combination of standard monomials such that each representative has a different leading term. One possible choice of representatives is the set of standard monomials itself. In this case it is common practice to call the basis the normal set.

Given any polynomial $f$, the matrix representing the linear mapping

$$A_f : k[x]/I \to k[x]/I, \quad [g] \mapsto [f \cdot g]$$

with respect to a basis is denoted by $A_f$. This is the so-called multiplication matrix or companion matrix in case the standard monomials are used as basis. We follow the convention that the image $A_f([g])$ corresponds to the $f$-th column of $A_f$. Then the eigenvalues of $A_f$ are the values of $f$ evaluated at the solutions of the polynomial system of equations. And the corresponding left eigenvectors $(\psi A_f = \psi v)$ are the polynomials $g_i$ evaluated at the solutions. If multiple solutions exist, $A_f$ may be transformed to Jordan form with associated vectors which are derivatives evaluated at the solutions (Möller and Stetter, 1995). Typically, one chooses $f(x) = x_i$ and thus the eigenvalues are coordinates of the solutions. Observe that there is some confusion in the literature by sometimes dealing with $A_f^l$ and left eigenvectors (in Möller and Stetter (1995); Char et al. (1991)) and sometimes using $A_f$ and right eigenvectors (in Cox et al. (1998); Sturmfels (2002)). Note in particular that the Maple implementation in the Groebner package uses the dual (i.e. transpose) of the matrices discussed here, and thus the right eigenvectors of those matrices give the left eigenvectors of this paper.

Once a Gröbner basis with respect to a term order is known it is easy to determine the matrix $A_f$ algorithmically by division. In this approach a Gröbner basis with respect to any term order is useful. This is a big advantage since Gröbner bases with respect to total degree order have much lower complexity than Gröbner bases with respect to lexicographic term orders. For details concerning the numerical computation and multiplicity of solutions we refer to Corless et al. (1997), Corless et al. (1995), Möller and Stetter (1995), Möller and Sauer (2000b) and Möller and Sauer (2000a).

We are interested in polynomial systems with symmetry. In that case the associated ideal $I$ is invariant with respect to a linear representation of a group $\Gamma$. The relation to invariant theory (Derksen and Kemper, 2002; Gatermann, 2000) is as follows. The invariant ring

$$k[x]^\Gamma = \{ f \in k[x] \mid f(\varphi \gamma x) = f(x), \forall \gamma \in \Gamma \}$$

gives rise to the ideal $I^\Gamma = k[x]^\Gamma \cap I$ having the same set of solutions as $I$. Unfortunately, in most cases it is very time-consuming to compute a basis of $I^\Gamma$. In this context we will need $I^\Gamma$ for theoretical purposes only. For an invariant polynomial $f$, the linear mapping

$$A_f^\Gamma : k[x]^\Gamma/I^\Gamma \to k[x]^\Gamma/I^\Gamma, \quad [g] \mapsto [f \cdot g]$$

is represented by a matrix $A_f^\Gamma$.

The paper is organized as follows. In Section 2 we start with typical examples of polynomial systems with symmetry, from dynamical systems, numerics and other applications. Section 3 contains our main results on the block diagonal structure of the multiplication matrix for invariant polynomials. In Algorithm 12 we show how to exploit this result in an efficient way.

Since the theoretical derivation requires SAGBI bases of invariant rings and intrinsic Gröbner–SAGBI bases, we briefly review SAGBI bases in Section 6. Although they have been introduced already
in 1989 (Robbiano and Sweedler, 1988; Kapur and Madlener, 1989) it is only recently that they have been used, see for example Gatermann (2003). Section 7 investigates the linear mapping $\mathcal{A}^f_\mu$, including multiplicities of orbits.

2. Examples of symmetric polynomial systems

In this paper we are interested in polynomial systems with symmetry and want to solve them with an eigenvalue method exploiting the symmetry. We start with typical examples from dynamics, chemistry and the theory of numerical algorithms.

We use linear representation theory as was nicely introduced in Fässler and Stiefel (1992). Given a finite group $\Gamma$ operating on $k^n$ by a linear representation $\vartheta : \Gamma \rightarrow GL(k^n)$ (the field $k$ usually being $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), an induced linear representation is $\rho : \Gamma \rightarrow Aut(k[x])$, $\gamma \mapsto \rho(\gamma)$ with $\rho(\gamma) : k[x] \rightarrow k[x]$, $p(x) \mapsto p(\vartheta(\gamma^{-1})x)$ for all $\gamma \in \Gamma$. We are interested in special invariant vector spaces with respect to $\rho$ which is the analog in the general theory. A vector space $V \subseteq k[x]$ is called invariant if for all $f \in V$ also $\rho(\gamma)(f) \in V$ for all $\gamma \in \Gamma$. Since ideals are vector spaces, the following definition is a special case.

**Definition 1.** The ideal $I \subset k[x_1, \ldots, x_n]$ is called invariant with respect to a linear representation $\vartheta : \Gamma \rightarrow GL(k^n)$ if with $f \in I$ we have $\vartheta(\gamma)x \in I$, $\forall \gamma \in \Gamma$.

If for a given system of polynomials $f_1, \ldots, f_m$ the ideal $I = \langle f_1, \ldots, f_m \rangle$ is invariant we call the system symmetric. In most cases this is observed in situations where the system is invariant as a vector space, i.e. $V = \text{span}(f_1, \ldots, f_m)$ is invariant with respect to $\rho$. This is equivalently expressed as equivariance of the given polynomials.

Given a second induced linear representation $\vartheta : \Gamma \rightarrow GL(k^n)$, a tuple $f \in (k[x])^m$ is called equivariant with respect to $\vartheta$ if

$$\vartheta(\gamma)(f(x)) = f(\vartheta(\gamma)x), \quad \forall \gamma \in \Gamma.$$  

We are concerned with equivariant tuples $f \in (k[x])^m$ or equivalently equivariant mappings $\Gamma \rightarrow k^m, \gamma \mapsto (f_1(\gamma), \ldots, f_m(\gamma))$.

Obviously, the solutions come in orbits, $\mathcal{O}_a = \{ p \in k^n \mid \exists \gamma \in \Gamma : \gamma a = p \}$.

2.1. Superstable orbits and bifurcation points of the logistic map

In this section we present examples of polynomial systems with symmetry, arising in the theory of discrete dynamical systems, which is the theory of iterations

$$y_i := f(y_{i-1}), \quad i = 1, \ldots,$$

for a given smooth function $f : \mathbb{R} \rightarrow \mathbb{R}$. A typical example which has been studied in great detail is the logistic map

$$f(\mu, y) = \mu y (1 - y),$$

depending on a parameter $\mu \in (0, 4]$. While the sequences $\{y_i, i = 1, \ldots\}$ are considered for fixed $\mu$ it is interesting to know how these orbits $\{y_i, i = 1, \ldots\}$ vary if the parameter $\mu$ varies.

In particular, one is interested in periodic orbits with period $N$, which means that $y_N = y_1$. For the logistic map the periodic orbit satisfies the following system of polynomial equations

$$0 = \mu y_1 (1 - y_1) - y_2,$$

$$0 = \mu y_2 (1 - y_2) - y_3,$$

$$\vdots$$

$$0 = \mu y_{N-1} (1 - y_{N-1}) - y_N,$$

$$0 = \mu y_N (1 - y_N) - y_1.$$

(1)
The stability of a periodic orbit is determined by the expression
\[ P = \prod_{i=1}^{N} f'(\mu, y_i) = \prod_{i=1}^{N} \mu (1 - 2y_i), \]
where the derivative means differentiation with respect to \( y \). In case \( P = 0 \) the orbit is called a superstable orbit while \( P = 1 \) gives rise to a bifurcation point. So for the logistic map a polynomial condition is satisfied for superstable orbits in addition to (1)
\[ 0 = \prod_{i=1}^{N} \mu (1 - 2y_i). \] (2)
For bifurcation points we have either
\[ 0 = \prod_{i=1}^{N} \mu (1 - 2y_i) - 1, \] (3)
or
\[ 0 = \prod_{i=1}^{N} \mu (1 - 2y_i) + 1. \] (4)
System (1) together with (2), (3) or (4) gives three polynomial systems of equations in \( n = N + 1 \) variables \( x = (\mu, y_1, \ldots, y_N) \). The polynomials \( f_1, \ldots, f_{n-1} \) are the right-hand sides of (1) while \( f_n \) is the right-hand side in (2), (3) or (4).

The symmetry of these systems is described by the cyclic group \( Z_N = \{id, r, r^2, \ldots, r^{N-1}\} \) operating as \( \vartheta(r)(\mu, y_1, \ldots, y_N) = (\mu, y_2, \ldots, y_N, y_1) \). The linear representation \( \vartheta : Z_N \rightarrow GL(\mathbb{R}^n) \) is given by \( \vartheta(r)(f_1, \ldots, f_n) = (f_2, \ldots, f_{n-1}, f_1, f_n) \). All three systems are equivariant with respect to \( \vartheta \) and \( \vartheta \).

The logistic map is the prototype of one-dimensional mappings because all possible types of orbits in one-dimensional mapping bifurcation diagrams appear already in the bifurcation diagram of the logistic map. The orbits of the logistic map exhibit a quite varied range of phenomena, such as periodicity, chaos, and boundedness. See Hao (1989) and Schroeder (1991) for a more detailed exposition on superstable orbits and the bifurcation points of the logistic map. The solutions of this example may be found at the end of Section 4.

2.2. Central configurations in the N-body problem of celestial mechanics

Another class of systems of polynomial equations exhibiting symmetries arises in the study of central configurations of the N-body problem of Celestial Mechanics which is a well-known Hamiltonian system. Central configurations are the only known solutions that can be computed analytically. The equations of central configurations can be written as a system of nonlinear polynomial equations using the mutual distances as unknowns. This formalism has been developed in Albouy and Chenciner (1998) in a very general context. A reformulation of this system using Linear Algebra has been developed in Kotsireas (1998).

Consider \( N \) particles of masses \( m_1, m_2, \ldots, m_N \) moving under their mutual gravitational attraction. Below, we restrict ourselves to the case of equal masses and, using homogeneity, we normalize the common value of the \( N \) masses to 1. We denote by \( s_{ij} \) the square of the mutual distance between the bodies \( i \) and \( j \). For reasons related with the fact that we are using the Newtonian potential energy function, we put \( S_{ij} = s_{ij}^{-3/2} \). Denote by \( \Delta_1, \Delta_2, \ldots, \Delta_N \) the oriented volumes of the \( N \) simplexes formed by the \( N \) bodies. The following mutual distances \( s_{ij} \) (and their corresponding \( S_{ij} \)) are denoted with distinct letters to agree with the standard notation:
\[ b = s_{13}, d = s_{23}, f = s_{34} \]
and
\[ B = S_{13}, D = S_{23}, F = S_{34}. \]
The following theorem is proved in Kotsireas (1998), see also Kotsireas (2001).

**Theorem 2.** The equations of central configurations of the Newtonian N-body problem with equal masses in a Euclidean space of dimension \( k = N - 2 \) in the case \( \Delta_1 \neq \Delta_2, \Delta_3 = \cdots = \Delta_N \) are given by:

\[
\begin{align*}
  k(b - d)(B - D) + (k - 2)(B + D) - 2kF + 4 &= 0 \\
  k(b - d)(B + D - 2F) + (k + 2)(B - D) &= 0 \\
  k(b - d)^2 - 2k(b + d) + 2(k - 1)f + k &= 0 \\
  B^2b^3 - 1 &= 0 \\
  D^2d^3 - 1 &= 0 \\
  F^2f^3 - 1 &= 0.
\end{align*}
\]

Taking \( N = 4 \) \( (k = 2) \) we obtain the corresponding system for the central configurations of the planar Newtonian 4-body problem with equal masses and it turns out that this analysis describes all possible planar central configurations of four equal masses.

System (5) is a system in 6 polynomials and 6 variables \( x = (b, d, f, B, D, F) \) and has the symmetry of \( \Gamma = Z_2 = \{id, s\} \). The first representation is given by \( \vartheta(s)(x) = (d, b, f, D, B, F) \) while \( \theta(s)(f_1, \ldots, f_6) = (f_1, f_2, f_3, f_4, f_5, f_6) \). System (5) is equivariant with respect to \( \vartheta \) and \( \theta \).

Another challenging system arises in the study of the spatial Newtonian 5-body problem with equal masses when we require the symmetry conditions \( \Delta_1 \neq 0, \Delta_2 = \Delta_3, \Delta_4 = \Delta_5 \). These conditions amount to the geometrical constraint that the central configuration will contain two symmetry planes. The following mutual distances \( s_{ij} \) (and their corresponding \( s_{ij} \)) are denoted with distinct letters to keep up with the standard notation.

\[
\begin{align*}
  a &= s_{12} & c &= s_{14} & d &= s_{23} & e &= s_{24} & \ell &= s_{45}
\end{align*}
\]

and

\[
\begin{align*}
  A &= S_{12} & C &= S_{14} & D &= S_{23} & E &= S_{24} & L &= S_{45}.
\end{align*}
\]

The following theorem is proved in Kotsireas (1998), see also Kotsireas (2001).

**Theorem 3.** The equations of central configurations in the spatial Newtonian 5-body problem with equal masses, with exactly two symmetry planes are given by the linear equation:

\[
A - C + 2D - 2L = 0
\]

and the fact that the matrix below must be of rank \( r \leq 2 \).

\[
\begin{pmatrix}
  -5A + 5C & -8A - 8C + 4L + 4D + 8E \\
  D + L - 2E & -A + C \\
  -8a - 8c + d + \ell + 4e & -2d + 2\ell + 8a - 8c \\
  -4c + 4a - d + \ell & -8e + 2d + 2\ell
\end{pmatrix}
\]

To write down the system describing the central configurations in this case, we have to supplement the equations of the theorem above with the equations

\[
A^2a^3 - 1 = 0, \quad C^2c^3 - 1 = 0, \quad D^2d^3 - 1 = 0, \quad l^2\ell^3 - 1 = 0, \quad E^2e^3 - 1 = 0.
\]

coming from the fact that we are using the Newtonian potential energy function.

2.3. Numerical quadrature

The following system of polynomial equations comes up in the construction of numerical quadrature formulas. A numerical quadrature formula is an approximation of an integral by a weighted sum

\[
\int_{-1}^{1} h(u) \, du \simeq \sum_{i=1}^{N} w_i \, h(y_i), \quad h \in C^\infty([-1, 1]),
\]

where \( N \) is a fixed integer number and \( w_i \) are given (positive) real numbers called weights and \( y_i \) are given real numbers (preferably in \([-1, 1]\)) called nodes.

The task is to find a ‘good’ formula. One meaning of ‘good’ is that the formula is exact for all polynomials up to degree \( d \). This is possible for \( d = 2N - 1 \). The monomials of degree \( \leq d \) form a
vector space basis of \( \mathbb{R}[x]_{\leq d} \). Thus the demand
\[
\int_{-1}^{1} u^j du = \sum_{i=1}^{N} w_i y_i^j, \quad j = 0, 1, \ldots, 2N - 1
\]
gives a system of \( n = 2N \) polynomial equations in \( x = (w, y) \in k^{2N} \):
\[
\begin{align*}
0 &= w_1 + \cdots + w_N - 2 \\
0 &= w_1 y_1 + \cdots + w_N y_N - 0 \\
0 &= w_1 y_1^2 + \cdots + w_N y_N^2 - \frac{2}{3} \\
&\vdots \\
0 &= w_1 y_1^{2N-1} + \cdots + w_N y_N^{2N-1} - 0.
\end{align*}
\]

The group \( \Gamma = \mathbb{Z}_2 \times S_N \) includes the symmetric group \( S_N \) operating with \( \vartheta|_{S_N} : S_N \to GL(\mathbb{R}^{2N}) \) where each permutation \( \pi \in S_N \) is operating like \( \vartheta(\pi) : \mathbb{R}^{2N} \to \mathbb{R}^{2N}, (w, y) \mapsto (w_{\pi(1)}), \ldots, w_{\pi(N)}, y_{\pi(1)}, \ldots, y_{\pi(N)} \) permuting both the weights and nodes simultaneously. Additionally, the reflection \( s \in \mathbb{Z}_2 \) is operating like \( (w, y) \mapsto (w, -y) \). The group \( S_N \) is not operating on the integrals. The reflection \( u \to -u \) operates so that \( \int_{-1}^{1} h(-u) du = \int_{-1}^{1} h(u) du \) for even \( h \) and \( \int_{-1}^{1} h(-u) du = -\int_{-1}^{1} h(u) du = 0 \) for odd \( h \). So the polynomials \( f_{2j-1}(w, y) \) corresponding to even monomials are invariant under \( Z_2 \times S_N \) while the polynomials \( f_{2j}(w, y) \) corresponding to even monomials are semi-invariant, i.e. \( f_{2j}(w, -y) = -f_{2j}(w, y) \). The linear representation \( \vartheta : \mathbb{Z}_2 \times S_N \to GL(\mathbb{R}^n) \) is given by \( \vartheta(s)(f_{2j}) = -f_{2j}, \vartheta(s)(f_{2j+1}) = f_{2j+1} \) for \( s \in \mathbb{Z}_2 \) and \( \vartheta(\pi) = id \) for all \( \pi \in S_N \). System (8) is equivariant with respect to \( \vartheta \) and \( \vartheta \).

3. Block diagonal structure in the eigenvalue method

In this section we present our main result on the block structure of the multiplication matrix \( A_f \) for an invariant ideal and an invariant polynomial \( f \) with respect to a symmetry adapted basis. We assume familiarity with linear representation theory and invariant theory as in Fässler and Stiefel (1992) and Gatermann (2000).

Assume that the group \( \Gamma \) has \( N \) irreducible representations. Then there are \( N \) isotypic components of the polynomial ring
\[
k[x] = \bigoplus_{i=1}^{N} V_i,
\]
where the first component \( V_1 = k[x]^\Gamma \) is the invariant ring itself. Given an invariant ideal \( I \), we will consider its associated isotypic decomposition
\[
I = \bigoplus_{i=1}^{N} I \cap V_i,
\]
and define \( I_i := I \cap V_i \), where \( I_1 = I^\Gamma = I \cap k[x]^\Gamma \) is the ideal in the invariant ring. The linear mapping
\[
A_f : k[x]/I \to k[x]/I, \quad [g] \mapsto [f \cdot g]
\]
is considered for an invariant polynomial \( f \). There are restrictions
\[
A_f|_{V_i} : V_i/I_i \to V_i/I_i, \quad [g] \mapsto [f \cdot g], \quad i = 1, \ldots, N.
\]
The first one is the mapping on the invariant part \( A_f^\Gamma : k[x]^\Gamma /I^\Gamma \to k[x]^\Gamma /I^\Gamma \).

Since \( k[x]/I = V_1/I_1 \oplus \cdots \oplus V_N/I_N \) and \( A_f \) is commutative and thus commuting with the group action the main theorem is obvious.

Theorem 4. Given a linear representation \( \vartheta \) of a group \( \Gamma \), a zero-dimensional, invariant ideal \( I \) and an invariant polynomial \( f \), then the mappings above satisfy
\[
A_f = A_f|_{V_1} + \cdots + A_f|_{V_N}.
\]
The following corollary is a version of Schur’s lemma.

**Corollary 5.** Assume $\Gamma$ and $\vartheta$ as well as ideal $I$ and $f$ as in the theorem above. Then it is possible to choose a basis of $k[x]/I$ such that the matrix $A_f$ representing $\mathcal{A}_f$ with respect to this basis is block diagonal. There is one block for each irreducible representation which may be decomposed further according to the dimension of the irreducible representation.

**Proof.** From the theorem above it is obvious that one may choose vector space bases of $V_i/I_i$, $i = 1, \ldots, N$. □

After proving the existence of the block diagonal structure we are interested in computing the blocks. There are several ways of determining the multiplication matrix with respect to the set of standard monomials. We use Gröbner bases here. If we denote the multiplication matrix with respect to the set of standard monomials (normal set) by $B_f$, a change of coordinates gives the multiplication matrix $A_f$ with respect to a set of polynomials $g_j, j = 1, \ldots, t = \dim(k[x]/I)$ which are linear combinations of standard monomials and form a vector space basis by

$$A_f = T^{-1}B_fT.$$  

The $j$-th column of $T$ contains the coefficients of standard monomials in $g_j$.

For invariant ideals $I$ it will not always be possible to choose $g_j$ such that they all are elements of some isotypic component $V_i$ and linear combinations of the standard monomials. However, for some group actions and some invariant ideals $I$ it is sufficient that the term order is grlex or some other order starting with comparing the degree. In general we use the following lemma.

**Lemma 6.** Suppose we are given a polynomial $f$ and a Gröbner basis of an ideal $I \subset k[x]$ with respect to $<$ with codimension $t$. Denote the multiplication matrix with respect to $f$ and the normal set by $B_f$. Assume $g_1, \ldots, g_t$ are polynomials which are linearly independent modulo $I$ and denote the corresponding multiplication matrix by $A_f$. There exists a matrix $T \in k^{t \times t}$ which can be computed by the division algorithm such that $A_f = T^{-1}B_fT$.

**Proof.** For each $g_j$ compute a normal form $\tilde{g}_j$ in the same equivalence class using the division algorithm. Then each $\tilde{g}_j$ is a linear combination of standard monomials. The coefficients define the entries of the matrix $T$ giving the change of coordinates. □

**Example 7.** We define $f_1 = (x - y)(25xy - 9), f_2 = x^2 + y^2 - 1$ and $I = \langle f_1, f_2 \rangle$. A Gröbner basis with respect to tdeg and $x > y$ is computed yielding the standard monomials $1, y, x, xy, y^2$. The solutions are shown in Fig. 1. The group $\Gamma = Z_2 \times Z_2$ is operating by $(x, y) \mapsto (y, x), (x, y) \mapsto (-y, -x), and (x, y) \mapsto (-x, -y)$. It has four irreducible representations. The invariant ring is polynomial and the isotypic components $V_2, V_3, V_4 \subset k[x, y]$ are free modules over the invariant ring $k[x, y]^{Z_2 \times Z_2}$. Two invariant polynomials $\pi_1 = xy, \pi_2 = x^2 + y^2$ generate the invariant ring. A module basis for $V_2$ is $b_{21} = x - y$, a basis for $V_3$ is $b_{31} = x + y$, and a basis for $V_4$ is $b_{41} = (x - y)(x + y)$. According to this we choose a vector space basis of $k[x, y]/I$ by $g_1 = 1, g_2 = xy$ for $k[x, y]^{Z_2 \times Z_2}$, $g_3 = x - y$ for $V_2/I_2, g_4 = x + y, g_5 = (x + y)xy$ for $V_3/I_3$, and $g_6 = x^2 - y^2$ for $V_4/I_4$.

As predicted by Corollary 5 the multiplication matrix of $\pi_1 = xy$ with respect to this basis has block diagonal structure

$$A_{\pi_1} = \begin{pmatrix}
0 & \frac{-9}{50} \\
1 & \frac{43}{50} \\
\frac{9}{25} & 0 \\
0 & \frac{-9}{50} \\
1 & \frac{43}{50} \\
\frac{9}{25} & 0
\end{pmatrix}.$$
But the system has even more structure. Two blocks are equal and $9/25$ is an eigenvalue of $A_{Z_2 \times Z_2}$. ☐

The block structure will be further investigated. For this we need more definitions.

The ideal $I^\Gamma = I \cap \mathbb{C}[x]^\Gamma$ generates an ideal in $\mathbb{C}[x]$, too. Since this ideal carries important information we look at its isotypic decomposition

$$\langle \{ f \in I^\Gamma \} \rangle = \bigoplus_{i=1}^N \langle \{ f \in I^\Gamma \} \rangle \cap V_i,$$

and define $I_i^\Gamma := \langle \{ f \in I^\Gamma \} \rangle \cap V_i$.

Recall from (Gatermann, 2000; Gatermann and Guyard, 1999; Stanley, 1979) that the isotypic components $V_i, i \geq 2$ are modules over the invariant ring and free modules over the ring in the primary invariants. This is even true for the subspaces $V_{ij}$.

**Proposition 8.** Given a group $\Gamma$ with a linear representation $\vartheta$ as above. Assume $I$ is a zero-dimensional ideal and $f$ is invariant. Denote the blocks by $A_i^\Gamma$ and $A_{ij}^\vartheta$, $i = 2, \ldots, N$, $j = 1, \ldots, n_i$. Then the subblock $A_{ij}^\vartheta$ has eigenvalues which are eigenvalues of $A_i^\Gamma$ with the same or smaller algebraic multiplicity.

**Proof.** We choose a basis $g_1, \ldots, g_s$ of $\mathbb{C}[x]^\Gamma / I^\Gamma$ such that $A_i^\Gamma$ is in Jordan form. Since $V_{ij}$ is a module over the invariant ring generated by $b_{ij}^1, \ldots, b_{ij}^l$, the elements $g_1b_{ij}^1, \ldots, g_1b_{ij}^l, \ldots, g sb_{ij}^1, \ldots, g sb_{ij}^l$ generate $V_{ij}/I_{ij}$. But some may be linearly dependent and therefore neglected. We can do this in a way that $A_{ij}^\vartheta$ is a substructure of $A_i^\Gamma$. ☐

For reflection groups the invariant ring is a polynomial ring and the isotypic components are thus free modules over the invariant ring. This enables further results on the block structure of the multiplication matrices.

**Lemma 9.** Assume $\vartheta (\Gamma)$ is a reflection group and $I_i = I_i^\vartheta$ for some $i$. Assume $f$ is an invariant polynomial. Then it is possible to choose a basis of $\mathbb{C}[x]/I$ such that the matrix $A_i$ is block diagonal and $A_{ij}^\vartheta = A_i^\Gamma$.

**Proof.** For reflection groups the invariant ring is polynomial and the isotypic components are free modules over the invariant ring. That means that $g_1b_{ij}^1, \ldots, g sb_{ij}^l$ in the proof above are linearly independent if considered in $V_{ij}$. Since $I_i = I_i^\vartheta$ is assumed, they are linearly independent as representatives of $V_{ij}/I_{ij}$. ☐

**Fig. 1.** The variety $V(I)$ in Example 7 as intersection of the two varieties $V(f_1), V(f_2)$. 
Example 7 (Continued). The linear representation considered above is a reflection group. Thus Lemma 9 applies. For the third component \( I_3 = I_3^{2 \times 2} \) and the block equals the block of the invariant ring. For the other components \( I_2 \neq I_2^{2 \times 2} \) and \( I_4 \neq I_4^{2 \times 2} \). Both blocks are \( 1 \times 1 \)-blocks with entry 9/25 being an eigenvalue of \( A_1^{2 \times 2} \).

These results agree perfectly with the group-theoretic result for the dimensions of irreducible representations \( \sum_{i=1}^{9} n_i^2 = |G| \). A solution orbit has at most \( |G| \) many elements.

4. Using the first block

The main result about the block diagonal structure suggests to use the first block associated to the invariant ring for solving a symmetric polynomial system.

If we are interested in the first block only, we do not want to compute the multiplication matrix with respect to the normal set and then change coordinates as in Lemma 6 since this is inefficient. In a particular situation we can avoid doing this.

Lemma 10. Assume \( I \subseteq k[x] \) is a zero-dimensional ideal of codimension \( t \) and that a Gröbner basis of \( I \) with respect to a given term order is known. Assume that we know linear combinations of standard monomials \( g_1, \ldots, g_r \in k[x] \) which have all distinct leading monomials. Given a polynomial \( f \in k[x] \) the multiplication matrix \( A_f \) with respect to the basis \( [g_1], \ldots, [g_r] \) may be computed directly with the division algorithm.

Proof. Since \( g_1, \ldots, g_r \) have different leading terms they form a vector space basis of \( k[x]/I \). First compute the normal form \( h \) off \( g_i \). While \( h \leftrightarrow 0 \) find \( g_i \) with \( \text{lm}(h) = \text{lm}(g_i) \), put \( a_{ij} = \text{lc}(h)/\text{lc}(g_i) \) and repeat with \( h = h - a_{ij} \text{lc}(h)\text{lm}(h) \). This determines \( h \) as a linear combination of the \( g_i \) whose coefficients are the entries in the \( j \)-th-column of \( A_f \).  

Remark 11. The situation in the lemma above corresponds to the situation of using a change of coordinates with the matrix \( T \) where \( T \) is lower triangular.

In the symmetric case we know that \( A_f \) for an invariant polynomial \( f \) is invariant on \( k[x]^r/I^T \). Thus the block \( A_f^{I^T} \) is computed by the division algorithm, if a basis \( g_1, \ldots, g_r \) of \( k[x]^r/I^T \) is known with different leading terms of their normal forms.

Algorithm 12. (Solving a symmetric system of polynomial equations)

**Input:** Gröbner basis \( G \) of invariant ideal \( I \) \((\dim 0)\) with respect to \(<\)

**algebra basis** \( \pi_1, \ldots, \pi_r \) of invariant ring

**Output:** complex solutions \( V(I) \)

1. Construct invariant polynomials \( g_1, \ldots, g_r \) whose normal forms have different leading terms
2. For \( j \) from 1 to \( r \) compute \( A^{I^T}_{g_j} \) by Lemma 10
3. Solve the eigenvalue problems \( \nu A^{I^T}_{g_j} = \lambda_\nu \) simultaneously giving \( s \) tuples \( \lambda \in \mathbb{C}^r \)
4. For each tuple of eigenvalues \( \lambda_1, \ldots, \lambda_r \) from (3) solve the polynomial system

\[
\pi_1(x) = \lambda_1, \quad \ldots, \quad \pi_r(x) = \lambda_r.
\]

The systems in step 4 can be solved either by the eigenvalue method again or by Newton’s method. Each system has one orbit of solutions. Thus it is sufficient to compute one solution only and derive the other from the group action. But for degenerate orbits (points in fixed point spaces of subgroups) the Newton method does not converge quadratically since the solutions have multiplicity. All points on a degenerate orbit have the same multiplicity.

Example 7 (Continued). Two invariant polynomials \( \pi_1 = xy, \pi_2 = x^2 + y^2 \) generate the invariant ring. \( g_1 = 1, g_2 = xy \) form a basis satisfying the conditions in step 1. So \( A_{g_1}^{I^T} \) might have as well been determined without the other blocks. The eigenvalues of \( A_{g_1}^{I^T} \) are \( 1/2 \) and \( 9/25 \). Since \( A_{g_1}^{I^T} \) is identity the eigenvalues are \( 1, 1 \). By Algorithm 12 we are left with solving the two small systems.
of equations
\[
\begin{align*}
xy &= \frac{1}{2} \quad \text{and} \quad xy = \frac{9}{25} \\
x^2 + y^2 &= 1
\end{align*}
\]
giving an orbit with two solutions \((\pm 0.707, \pm 0.707)\) and another orbit with four solutions \((\pm 0.92, 0.39), (\pm 0.39, 0.92)\), see Fig. 1. ♦

**Example 13.** Here we are solving the equations describing the bifurcation points of the logistic map for \(N = 4\). These are the equations (1) and (4) in 5 variables \(\mu, x_1, x_2, x_3, x_4\). The cyclic group with four elements operates on the variables \(x_1, x_2, x_3, x_4\) by permutation.

We computed a Gröbner basis with respect to the degree reverse lexicographical order in Singular. Thus we know that the dimension of the quotient ring is 64. But we do not need to construct matrices of this size. Instead we use the invariant-theoretic approach in Algorithm 12. The primary and secondary invariants of the action of the cyclic group are computed in Magma:

\[
P = [\mu, x_1 + x_2 + x_3 + x_4, x_1^2 + x_2^2 + x_3^2 + x_4^2, x_1 x_2 + x_1 x_4 + x_2 x_3 + x_3 x_4, x_1^4 + x_2^4 + x_3^4 + x_4^4]\]

\[
S = [1, x_1^3 + x_2^3 + x_3^3 + x_4^3, x_1 x_2 x_3, x_1^2 x_2^2 + x_2^2 x_3^2 + x_3^2 x_4^2, x_1^3 x_4 + x_2^3 x_1 + x_2 x_3^3 + x_3 x_4^3].
\]

Note that \(\mu\) is an invariant. By working incrementally on the degree of the invariants, we construct a normal set of 24 invariants which are linearly independent (they have different leading terms). Since we are interested only in the parameter value of \(\mu\) it is sufficient to compute the multiplication matrix \(M_\mu\) associated to the invariant polynomial \(\mu\). This is a \(24 \times 24\) matrix whose characteristic polynomial factorizes as follows:

\[
\begin{align*}
(\mu^4 + 1) & (\mu^4 - 8 \mu^3 + 24 \mu^2 - 32 \mu + 17) (\mu^4 - 4 \mu^3 - 4 \mu^2 + 16 \mu + 17) \\
(\mu^{12} - 12 \mu^{11} + 48 \mu^{10} - 40 \mu^9 - 193 \mu^8 + 392 \mu^7 + 44 \mu^6 + 8 \mu^5 - 977 \mu^4 \\
& - 604 \mu^3 + 2108 \mu^2 + 4913).
\end{align*}
\]

The third bifurcation point of the logistic map is given at a parameter value which is the real root in \([\frac{7}{2}, \frac{15}{4}]\) of the polynomial of degree 12 above. This polynomial of degree 12 has also been computed using integer relation finding techniques (Bailey and Broadhurst, 2001). The first two polynomials correspond to fixed points while the third polynomial corresponds to orbits of period two.

The full \(64 \times 64\)-multiplication matrix \(M_\mu\) has four blocks in the symmetry adapted coordinate system. Its characteristic polynomial is formed by the four polynomials above. But here the third polynomial appears with multiplicity two while the fourth polynomial appears with multiplicity four.

Exploiting the symmetry using Invariant Theory results in manipulating a much smaller multiplication matrix. ♦

5. Choosing a representative of an orbit

For large groups the number of primary and secondary invariants may be large and of high degree. Then the polynomial system in step 4 of Algorithm 12 may be a difficult problem itself. In this situation it might be better to compute a representative of a solution orbit directly.

**Lemma 14.** Given a group \(\Gamma\) and its linear representation \(\vartheta\) and a zero-dimensional invariant ideal \(I\) and symmetry adapted basis as in Corollary 5. Let \(A_f\) as before denote the matrix representing \(A_f : k[x]/I \to k[x]/I\) with respect to this basis for a given polynomial \(f\) (not necessarily invariant). Then there is a group operation on the eigenvectors. That means the eigenvectors form orbits. Moreover, for each orbit the normalized parts corresponding to the block associated to the invariant ring are equal.

**Proof.** The basis of representatives \([g_1], \ldots, [g_t]\) of \(k[x]/I\) is symmetry adapted. That means the group is operating on this basis by multiple irreducible representations. The vector space of eigenvectors is an invariant subspace. On the other hand the left eigenvectors (after normalization) are \([g_1(a), \ldots, g_t(a)]\), the symmetry adapted basis evaluated at the solutions \(a\). Since the solutions
form orbits, the tuple \( g_1, \ldots, g_r \) is evaluated at orbits, which defines the same group action on the eigenvectors. But invariant polynomials have the same value for each point in an orbit. Thus the first entries of the eigenvectors of an orbit corresponding to the invariants are equal.

**Algorithm 15.** (Solving a symmetric system of polynomial equations)

**Input:** Gröbner basis \( G \) of invariant ideal \( I (\dim 0) \) with respect to less algebra basis \( \pi_1, \ldots, \pi_r \) of invariant ring generators \( b^j_k \) of isotypic components as module over \( k[x]^r \)

**Output:** complex solutions \( V(I) \)

1. Determine a symmetry adapted basis \([g_1], \ldots, [g_r] \) of \( k[x]/I \)
2. For \( i = 1, \ldots, n \) compute the multiplication matrices \( A_{x_i} \)
3. Restricted computation of the eigenvalues and eigenvectors of a random linear combination of \( A_{x_i} \)
4. Compute the eigenvalues of \( A_x \) giving the coordinates of the solutions.

Since all multiplication matrices commute the eigenvectors are the same for each multiplication matrix. Thus step 4 is easily done. The computation of eigenvalues in step 3 may be done by Schur factorization, vector power iteration, or Rayleigh quotient iteration. Since the group action on the eigenvectors is known in the symmetry adapted coordinate system one may restrict to representatives of group orbits in the vector power iteration. Once the first eigenvector is approximated the group action will give us an orbit of eigenvectors. For the next iteration we try to stay transversal to the generalized eigenspace generated by the orbit of the first eigenvector and so on.

**Example 7 (Continued).** In this example the multiplication matrices are

\[
A_x = \begin{pmatrix}
0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{9}{50} & 0 \\
0 & 0 & -1 & 1 & \frac{34}{25} & 0 \\
\frac{1}{2} & \frac{9}{50} & 0 & 0 & 0 & \frac{43}{50} \\
\frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & \frac{1}{2} & 0 & 0 & 0 & -1 \\
0 & 0 & \frac{1}{2} & \frac{1}{2} & \frac{9}{50} & 0 \\
\end{pmatrix}, \quad A_y = \begin{pmatrix}
0 & 0 & -\frac{1}{2} & \frac{1}{2} & -\frac{9}{50} & 0 \\
0 & 0 & 1 & 1 & \frac{34}{25} & 0 \\
-\frac{1}{2} & -\frac{9}{50} & 0 & 0 & 0 & \frac{43}{50} \\
\frac{1}{2} & 0 & 0 & 0 & 0 & -\frac{1}{2} \\
0 & \frac{1}{2} & 0 & 0 & 0 & 1 \\
0 & 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{9}{50} & 0 \\
\end{pmatrix}.
\]

The left eigenvectors are the columns of

\[
\begin{pmatrix}
1.0 \\
0.5 \\
0.0 \\
1.41 \\
0.7 \\
0.0 \\
\end{pmatrix}
\begin{pmatrix}
1.0 \\
0.36 \\
-0.53 \\
-0.47 \\
0.69 \\
-0.69 \\
\end{pmatrix}
\begin{pmatrix}
1.0 \\
0.36 \\
0.53 \\
1.31 \\
0.47 \\
0.69 \\
\end{pmatrix}
\begin{pmatrix}
1.0 \\
0.36 \\
0.53 \\
1.31 \\
0.47 \\
-0.69 \\
\end{pmatrix}
\begin{pmatrix}
1.0 \\
0.36 \\
0.53 \\
1.31 \\
0.47 \\
-0.69 \\
\end{pmatrix}
\begin{pmatrix}
1.0 \\
0.36 \\
0.53 \\
1.31 \\
0.47 \\
-0.69 \\
\end{pmatrix}
\]

There are two orbits with two and four vectors respectively. The values equal the functions \( g_1, \ldots, g_6 \) evaluated at the 6 solutions.

6. SAGBI bases’ essentials

In Robbiano and Sweedler (1988); Kapur and Madlener (1989) SAGBI bases (or canonical bases) were first introduced while the textbooks (Sturmfels, 1996; Vasconcelos, 1998) give a nice tutorial on this topic. More special information is available in Adams et al. (1999), Miller (1996), Miller (1998) and Stillman and Tsai (1999).

As usual < denotes a term order on a polynomial ring \( k[x_1, \ldots, x_n] \) and \( lt(p) = lc(p) lm(p) \) denotes the leading term, leading coefficient and leading monomial, respectively. The field \( k \) is \( \mathbb{Q} \) or any other computable field of characteristic zero. \( in_< (I) \), \( in_< (S) \) denote the leading monomial ideal or leading monomial algebra, respectively.
Definition 16. A set $F \subseteq k[x]$ of polynomials is called a SAGBI basis of a subalgebra $S$ of $k[x]$ if

$$in_{\prec}(S) = \langle \lim(f), f \in F \rangle.$$  

Note that in general the set $F$ is not finite. For this reason, in Gatermann (2003) a variant is suggested where in the case of a graded subalgebra the subalgebra is truncated at some degree.

Analogous to the division algorithm in Gröbner bases theory there is a subduction algorithm. Given $p \in k[x]$ and a SAGBI basis of $S$ this provides an algorithmic test for algebra-membership of $p$ in $S$. For any $p$ it computes a representation $P(y) + r$ with $p(x) = P(f_1(x), \ldots, f_m(x)) + r(x)$ with $\lim(r) \not\in in_{\prec}(S)$ and $f_1, \ldots, f_m \in F$ and $P \in k[y_1, \ldots, y_n]$. Analogous to the Buchberger algorithm for Gröbner bases, there is an algorithm for converting an algebra basis of $S$ to a SAGBI basis of $S$. This algorithm has been implemented in Macaulay 2 (Grayson and Stillman, 1996) and in Singular (García Gómez, 2001; Greuel et al., 2001).

In this paper we are interested in the situation that the subalgebra $S$ is the invariant ring of a group $G^\ast$. Observe that for special group actions the SAGBI basis may not be finite, see Sturmfels (1996, p. 99). Given a set of generating invariant polynomials these are converted by the algorithm into a SAGBI basis, if a finite SAGBI basis exists. Otherwise a truncated SAGBI basis may be computed.

We are especially interested in ideals $I^G$ in the invariant ring. Typically, $I^G = I \cap k[x]^G$ for an invariant ideal $I \subset k[x]$. Also for this case the theory provides an algorithmic approach.

Definition 17 (Sturmfels (1996) p. 106). Assume an algebra $S \subset k[x]$ and an ideal $J$ in $S$. Then a set of polynomials $G$ is called an intrinsic Gröbner–SAGBI basis, if the leading monomial ideals

$$in_{\prec}(J) = \langle \lim(f), f \in \Gamma \rangle$$

are equal as ideals in the monomial subalgebra $in_{\prec}(S)$.

Analogous to the division algorithm and the Buchberger algorithm there exist algorithms which compute a representation and a Gröbner–SAGBI basis, respectively. Given a SAGBI basis $F$ of $S$ and a generating set $G$ of $J$ a reduction of a polynomial $p \in S$ consists of a representation $\lim(p) = \prod_{f \in F}(\lim(f))^{|f|} \lim(g)$ for a tuple $i$ and a $g \in G$. Choosing an appropriate constant $p - c \prod_{f \in F}(\lim(f))^{|f|} g(x)$ gives another polynomial in $S$ with smaller leading term. Repeating this step we find a representation

$$p(x) = \sum_{g \in G} a_g (f_1(x), \ldots, f_m(x)) g(x) + r(x),$$

where $a_g$ are polynomials in $k[y_1, \ldots, y_m]$ and $r$ is a polynomial in $S$ with $r = 0$ or $\lim(r) \not\in \langle \lim(g), g \in G \rangle$. In addition we have $\lim(a_g(f)) \leq \lim(p)$ for $g$ in $G$ with $a_g \neq 0$. We denote $r$ by $rem_{\prec}(p, F, G)$. Obviously, $\lim(r) \not\in in_{\prec}(J)$ is a finite SAGBI basis of $J$. This gives an ideal membership test and enables to compute a multiplication matrix as follows.

Assume that $J$ has finite codimension in $S$. Then $S/J$ is a vector space of finite dimension with the same dimension than $in_{\prec}(S)/in_{\prec}(J)$. For any $f \in S$ the mapping $L_f : S/J \rightarrow S/J$. $[g] \mapsto [f \cdot g]$ is a linear mapping between vector spaces.

Lemma 18. Given a SAGBI basis of $S$ and an intrinsic Gröbner–SAGBI basis of $J$ with respect to an order $\prec$. There exists a set of polynomials $h_1, \ldots, h_s \in S$ such that their leading terms are standard monomials of $J$ in $S$ and their leading terms are all different. Then the intrinsic division algorithm allows to compute a matrix $L = (l_{ij})$ representing the linear mapping $L_f$ with respect to the vector space basis $[h_1], \ldots, [h_s]$.

Proof. Since $J$ has finite codimension in $S$ there exist finitely many standard monomials $x^{e_1}, \ldots, x^{e_s}$ in $in_{\prec}(S) \setminus in_{\prec}(J)$. We assume that the monomials are ordered with respect to the term order as $x^{e_1} > \cdots > x^{e_s}$. Then there exist polynomials $h_i \in S \setminus J$ with $\lim(h_i) = x^{e_i}, i = 1, \ldots, s$. Choose $h = h_i$ such that it has a representation $h = f_1^{e_1} \cdots f_m^{e_m}$. This choice is not unique. Because of their different leading terms $[h_1], \ldots, [h_s]$ form a vector space basis of $S/J$. Using the intrinsic division algorithm we find $r = rem_{\prec}(f_1 h_i, F, G)$ with $\lim(r) = x_j^{e_j}$ for one monomial $x_j^{e_j}$. Then $l_{i0} = 0$ for $k = 1, \ldots, j-1$ and $l_{ij} = lc(r)/lc(h_i)$. Repeating this step for $r - l_{i0} h_i$ we receive a remainder $r_j$ with $\lim(r_j) = x_j^{e_j}$ for some $j > 0$. Then $l_{ij} = 0$ for $k = j + 1, \ldots, \nu - 1$ and $l_{ii} = lc(r_j)/lc(h_i)$. Repeating this process we receive a unique representation

$$\sum_{j=1}^{s} l_{ij}[h_j] \text{ of } [f \cdot h_i] \in S/J. \qed$$
For our case of an invariant ring the lemma provides a way of computing the representation matrix $A_f^\Gamma$ of the mapping $A_f^\Gamma: k[x]/I^\Gamma \to k[x]/I^\Gamma$, $[g] \mapsto [g \cdot f]$ where $f$ is another invariant polynomial. However one has to be careful with the relation between Gröbner–SAGBI bases and Gröbner–bases. As the following example shows the inclusions of monomial ideals in $k[x]$ for a solution $a \in V(I)$ may be generalized to the multiplicity of an orbit in the following way. We define

$$k[x]^{\Gamma}_{(x)} = \left\{ \frac{f}{h} \mid f, h \in k[x]^\Gamma, h(0) \neq 0 \right\}.$$

For a point $a \neq 0$ we define analogously

$$k[x]^{\Gamma}_{(x-a)} = \left\{ \frac{f}{h} \mid f, h \in k[x]^\Gamma, h(a) \neq 0 \right\}.$$

Observe that the local rings are equal for all members $a \in \mathbb{C}^n$ of the same orbit.

**Definition 20.** Assume a group $\Gamma$ is operating by a linear representation and $I$ is an invariant ideal. Let $I^\Gamma = I \cap k[x]^\Gamma$. For a solution $a \in V(I)$ the dimension

$$\dim_k(k[x]^{\Gamma}_{(x-a)}/I^\Gamma k[x]^{\Gamma}_{(x-a)})$$

called is the multiplicity of the orbit $\sigma_a$.

This definition seems to be natural and it might have been used before although we are not aware of any reference.

Analogous to Sturmfels (2002, p. 16) there is an alternative definition of multiplicity. Let

$$J := I^\Gamma : (I^\Gamma : (x - a) \cap k[x]^\Gamma)^\infty,$$

and $\dim(k[x]/J)$ be the multiplicity of $a$. Analogously to Proposition 2.5 in Sturmfels (2002) the rings $k[x]/J$ and $k[x]^{\Gamma}_{(x-a)}/I^\Gamma k[x]^{\Gamma}_{(x-a)}$ are isomorphic.

**Theorem 21.** If $k[x]^{\Gamma}/I^\Gamma$ has finite dimension then this dimension is the number of orbits in $V(I)$ counted with multiplicity. In other words: there is a ring isomorphism

$$k[x]^{\Gamma}/I^\Gamma \cong \bigotimes_{\sigma_a \subseteq V(I)} k[x]^{\Gamma}_{(x-a)}/I^\Gamma k[x]^{\Gamma}_{(x-a)}.$$

**Proof.** The proof is a generalization of the proof for the non-symmetric case in Cox et al. (1998, p. 141).
Corollary 22. Assume \( f \in k[x]^G \) and an invariant ideal \( I \) with \( I^F = I \cap k[x]^F \) Let \( A^r_I \) be the representation matrix of \( k[x]^F/I^F \to k[x]^F/I^r \), \([g] \mapsto [fg]\). Then the eigenvalues of \( A^r_I \) are the values of \( f \) at the solution orbits \( \Theta_a \in V(I) \). The algebraic multiplicity of an eigenvalue equals the multiplicity of the orbit.

Proof. The proof is identical with the proof in the non-symmetric case. \( \square \)

Example 7 (Continued). We consider the modified polynomials \( \tilde{f}_1 = (x - y)(25xy - 9)^2, f_2 = x^2 + y^2 - 1 \). A symmetry adapted basis of \( k[x, y]/I \) is \( 1, xy, x^2y^2, x - y, (x - y)xy, x + y, (x + y)xy, (x - y)x^2y^2, x^2 - y^2, (x^2 - y^2)xy \) giving the block diagonal structure of \( A_{xy} \) as

\[
\begin{pmatrix}
A_{xy}^1 & 0 \\
0 & A_{xy}^2
\end{pmatrix}
\]

with

\[
A_{xy}^1 = \begin{pmatrix} 0 & 0 & \frac{81}{1250} \\ 0 & 1 & -\frac{306}{625} \\ 0 & 1 & \frac{61}{50} \end{pmatrix},
A_{xy}^2 = \begin{pmatrix} 0 & -\frac{81}{625} \\ 1 & \frac{18}{25} \end{pmatrix}.
\]

The Jordan form of \( A_{xy} \) has the same structure. \( A_{xy}^1 \) has the eigenvalue 1/2 and the Jordan block

\[
J = \begin{pmatrix} \frac{9}{25} & 1 \\ 0 & \frac{9}{25} \end{pmatrix}.
\]

This is also the Jordan block for \( A_{xy}^2 \). The orbit has multiplicity two and so does every point in the orbit. \( \diamond \)

Given an ideal basis of an invariant ideal \( I \) it is easy to find some generators of \( I^F \subset k[x]^F \). But it is hard to determine a generating set. However, there is an ideal \( J \subset k[x]^F \) having the same real solutions as \( I \). This result due to Jarić, Michel and Sharp may be found in Gatermann (2000). So we may assume that we are given a set of invariant polynomials generating and ideal in the invariant ring. One way of handling this situation is to introduce slack variables for fundamental invariants, rewrite the given polynomials in these slack variables and consider the ideal in the ring in the slack variables with the known methods. Instead we suggest to use Gröbner–SAGBI bases.

Algorithm 23. (Symmetric eigenvalue method)

INPUT: SAGBI basis \( F \) of \( k[x]^F \) with respect to <
\(
\)Gröbner–SAGBI basis \( G \) of invariant ideal \( I^F \subset k[x]^F \) wrt < invariant polynomials \( \pi_1, \ldots, \pi_r \in k[x]^F \)

OUTPUT: values of \( \pi_1, \ldots, \pi_r \) at orbits \( \Theta \subset V(I^F) \)

(1) Choose basis \( h_1, \ldots, h_s \) as in Lemma 18
(2) Compute matrices \( A_{\pi_1}^r, \ldots, A_{\pi_r}^r \)
(3) Compute eigenvalues (and common eigenvectors) of \( A_{\pi_1}^r, \ldots, A_{\pi_r}^r \)

CONCLUSIONS: The exploitation of symmetry in the eigenvalue method enables to solve polynomial systems efficiently. But many polynomial systems with symmetry have infinitely many solutions. A typical example is that of the cyclohexane. Further research is needed in this direction. Another topic for future research is the careful exploration of multiplicities in the symmetric case with Jordan form and generalized eigenvectors as in Möller and Stetter (1995) specialized to the symmetric setting.

Acknowledgments

The authors like to thank Hans Stetter for asking how symmetry influences his eigenvalue method in the fall of 1998 at the MSRI in Berkeley. While starting this paper KG was a Ontario Research Chair of Computer Algebra at ORCCA, University of Western Ontario. KG also acknowledges the support of DFG by a Heisenberg scholarship. This work has been supported by a grant from the National Science and Engineering Research Council of Canada. While conducting this research, RMC was supported by
grants from the Natural Sciences and Engineering Research Council of Canada, and by a grant from the Ontario Research and Development Challenge Fund and Waterloo Maple, Inc. ISK was supported by an NSERC grant.

References


