Advances in Mathematics **141**, 366–384 (1999)
Article ID aima.1998.1787, available online at http://www.idealibrary.com on IDEAL®

Computation of Invariants for Reductive Groups

Harm Derksen*

Department of Mathematics, Northeastern University,
567 Lake Hall, Boston, Massachusetts 02155
E-mail: hderksen@math.unibas.ch

Received April 28, 1998; accepted September 19, 1998

We will give an algorithm for computing generators of the invariant ring for a given representation of a linearly reductive group. The algorithm basically consists of a single Gröbner basis computation. We will also show a connection between some open conjectures in commutative algebra and finding good degree bounds for generating invariants.

1. INTRODUCTION

Let G be a linear algebraic group defined over the field k. Let $\rho: G \to \mathrm{GL}(V)$ be a representation of G on a k-vector space V of dimension $n < \infty$. The group G acts linearly on the k-algebra $\mathcal{O}(V) \cong k[X_1, X_2, ..., X_n]$ of polynomial functions on V, the *coordinate ring* of V. The *invariant ring* $\mathcal{O}(V)^G$ is the subalgebra of invariant functions. Hilbert proved in 1890 that $\mathcal{O}(V)^G$ is always finitely generated when G is *linearly reductive* (see [14]). A group is called *linearly reductive* when every finite dimensional G-module is the direct sum of irreducible modules (see for example [38]).

In this paper we will present an algorithm for computing generators of the invariant ring for arbitrary linearly reductive groups G. The algorithm is based on Hilbert's proof of 1890 which was considered not constructive at all at that time. Hilbert gave a more constructive proof of his finiteness result in 1893 (see [15]) by constructing a homogeneous system of parameters. This method leads to algorithms as described in Sturmfels' book (see [40]). There are several implementations for computing invariant rings of finite groups. Kemper wrote the INVAR package for the computer algebra system MAPLE (cf. [22, 23]) and his algorithms have been implemented in MAGMA too. Heydtmann wrote the FINVAR.LIB library

* Partially supported by SNF (Schweizerischer Nationalfonds) and Freiwillige Akademische Gesellschaft.

0001-8708/99 $30.00

in SINGULAR (cf. [13]). There are also implementations by Gatermann in REDUCE and MAPLE (see [10]).

Suppose now that G is a linearly reductive group. We define the following constant:

$$\beta_G(V) = \min\{d \mid \mathcal{O}(V)^G \text{ is generated by invariants of degree} \leqslant d\}.$$

For some special cases, a good upper bound is known. Jordan gave a good bound in the case $G = \mathrm{SL}_2$ and $\mathrm{char}(k) = 0$, using the methods of Gordan (see [19] and [20]). We have Noether's bound for finite groups. Wehlau proved in [41] a good bound for tori. The first general bound for semisimple groups was found by Popov (see [31] and [32]). He combined the second constructive proof of Hilbert with the results of Hochster and Roberts stating that the invariant ring is Cohen–Macaulay (see [18]). In her thesis, Hiss was able to improve this bound and generalize it to arbitrary connected reductive groups, using some ideas of Knop's (see [6, 17]). Let $\sigma(V)$ be the smallest integer d such that for every $v \in V$ with 0 not in the closure of the orbit Gv, there exists a homogeneous invariant $h \in \mathcal{O}(V)^G$ with degree $\leqslant d$ such that $h(v) \neq 0$. Popov proved

$$\beta_G(V) \leqslant n \cdot \mathrm{lcm}\{1, 2, 3, ..., \sigma(V)\}$$

where "lcm" is the least common multiple. Let m be the dimension of G and let $T \subseteq G$ be a maximal torus of rank r. Let $X(T) \cong \mathbb{Z}^r$ be the group of characters of T and choose some norm $\|\cdot\|$ on the vector space $X(T) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^r$. Define

$$L_V = \max\{\|\chi_1\|, \|\chi_2\|, ..., \|\chi_n\|\}$$

where $\chi_1, ..., \chi_n$ are the weights of T appearing in V. It follows from Hiss' bound that

$$\sigma(V) \leqslant DL_V^m$$

where $D > 0$ is some fixed constant depending on the group only. Note that this bound doesn't depend on the dimension of V.

Popov's bound seems far from sharp. For example if $G = \mathrm{SL}_2$ and $V = V_d$, the binary forms of degree d, then $\sigma(V) \leqslant 96d^3$ and $\beta_G(V) \leqslant (d+1) \cdot \mathrm{lcm}\{1, 2, ..., 96d^3\}$. This bound is much worse than the bound $\beta_G(V) \leqslant d^6$ of Jordan (see [19] and [20]).

We will show that if the Eisenbud–Goto Conjecture is true (*Conjecture* 4.1), *then for any connected linearly reductive group there exist constants* $C, C' > 0$ *depending only on* G *and* $\|\cdot\|$ *such that*

$$\beta_G(V) \leqslant \min\{C(nL_V)^m, C'L_V^{m^2+m}\}.$$

In fact, the author has recently shown (see [5]) that one even has

$$\beta_G(V) \leqslant \max\left\{\sigma(V), \frac{3}{8} n\sigma^2(V)\right\}$$

which is a drastical improvement of the bound of Popov and Hiss. It follows that $\beta_G(V) \leqslant CnL_V^{2m}$ for some constant $C > 0$, and using Weyl's theorem (in the way we will do in Section 4) one can deduce $\beta_G(V) \leqslant C' L_V^{3m}$ from that. This can be seen as some empirical evidence for the Eisenbud–Goto Conjecture.

For finite groups we have the bound of Noether (see [29]): If G is a finite group and $\mathrm{char}(k) > |G|$ or $\mathrm{char}(k) = 0$, then

$$\beta_G(V) \leqslant |G|.$$

It is not known whether this bound holds for all finite reductive groups. Smith proved that one still has Noether's bound in this case if G is solvable (cf. [36]).

We will show that if the Subspace Conjecture (*Conjecture* 4.2) *is true, then Noether's bound holds whenever G is finite and linearly reductive, i.e., if* $\mathrm{char}(k)$ *does not divide the group order.*

For a more detailed overview about constructive invariant theory, see [6].

2. THE NULLCONE

Let k be a field, and G be a linearly reductive group over k. Suppose that V is an n-dimensional representation of G. The inclusion $\mathcal{O}(V)^G \hookrightarrow \mathcal{O}(V)$ corresponds to a morphism $\pi\colon V \to V/\!/G$, where $V/\!/G := \mathrm{Spec}\, \mathcal{O}(V)^G$ is the categorical quotient. The ring $\mathcal{O}(V) \cong k[X_1, X_2, ..., X_n]$ is graded $\mathcal{O}(V) = \bigoplus_{i \geqslant 0} \mathcal{O}(V)^i$, and this induces a grading on $\mathcal{O}(V)^G$. Let us write $\mathfrak{m}$ for the maximal homogeneous ideal $(X_1, X_2, ..., X_n)$ of $\mathcal{O}(V)$. We define $I_{\mathcal{N}}$ to be the ideal of $\mathcal{O}(V)$ generated by all homogeneous invariants of positive degree, which we will call the *zero-fiber ideal*. The space $\mathrm{Spec}(\mathcal{O}(V)/I_{\mathcal{N}})$ is equal to $\pi^{-1}\pi(0)$ in the schematic sense. The zero set of $I_{\mathcal{N}}$ is the so-called *nullcone* $\mathcal{N}$. The well-known Finiteness Theorem of Hilbert states that

THEOREM 2.1. *If G is a linearly reductive group, and V is a representation of G, then* $\mathcal{O}(V)^G$ *is finitely generated.*

Proof. The proof of this theorem is based on the following two facts:

1. The polynomial ring over a field is noetherian: every ideal in the polynomial ring $\mathcal{O}(V)$ is finitely generated (Hilbert's Basissatz).

2. There exists a unique G-invariant linear projection $\mathscr{R}: \mathscr{O}(V) \to \mathscr{O}(V)^G$ (i.e., $\mathscr{R}(g \cdot f) = \mathscr{R}(f)$ for all $g \in G$, $f \in \mathscr{O}(V)$ and $\mathscr{R}(f) = f$ for all $f \in \mathscr{O}(V)^G$), which is called the *Reynolds operator* (see [38]). It has the following properties:

(a) $\mathscr{R}$ is a $\mathscr{O}(V)^G$-module homomorphism;

(b) if $W \subseteq \mathscr{O}(V)$ is a G-invariant linear subspace, then $\mathscr{R}(W) = W^G$.

The ideal $I_{\mathscr{N}}$ is generated by invariants, and by the noetherian property we only need finitely many of them to generate $I_{\mathscr{N}}$, say $I_{\mathscr{N}} = (f_1, f_2, ..., f_r)$. Suppose that h is a homogeneous invariant of degree d. Using induction on d, we proof that $h \in k[f_1, f_2, ..., f_r]$. If $d = 0$, then $h \in k$ and the statement is clear. Otherwise we can write

$$h = \sum_{i=1}^{r} a_i f_i$$

with $a_1, a_2, ..., a_r \in \mathscr{O}(V)$. Without loss of generality we may assume that a_i is homogeneous of degree $d - \deg f_i < d$ for all i. Applying the Reynolds operator yields

$$h = \mathscr{R}h = \mathscr{R}\left(\sum_{i=1}^{r} a_i f_i\right) = \sum_{i=1}^{r} \mathscr{R}(a_i)\, f_i$$

By induction hypothesis, $\mathscr{R}(a_1), ..., \mathscr{R}(a_r) \in k[f_1, f_2, ..., f_r]$, so $h \in k[f_1, ..., f_r]$. ∎

The proof of Hilbert was criticized at the end of the nineteenth century because choosing the invariant generators $f_1, f_2, ..., f_r$ of $I_{\mathscr{N}}$ is a non-constructive step. However, we will show that there is a constructive way to obtain these $f_1, f_2, ..., f_r$.

LEMMA 2.2. *Suppose $h_1, h_2, ..., h_s \in \mathscr{O}(V)$ are homogeneous and generate $I_{\mathscr{N}}$. Then $\mathscr{R}(h_1), \mathscr{R}(h_2), ..., \mathscr{R}(h_s)$ generate $\mathscr{O}(V)^G$ as a k-algebra.*

Proof. If $f_1, f_2, ..., f_r \in \mathscr{O}(V)^G$ are generators of $I_{\mathscr{N}}$, then the images of $f_1, ..., f_r$ span the vector space $I_{\mathscr{N}}/\mathfrak{m}I_{\mathscr{N}}$. Therefore, the action of G on $I_{\mathscr{N}}/\mathfrak{m}I_{\mathscr{N}}$ is trivial, so the Reynolds operator is equal to the identity on $I_{\mathscr{N}}/\mathfrak{m}I_{\mathscr{N}}$. The image of h_i and $\mathscr{R}(h_i)$ in $I_{\mathscr{N}}/\mathfrak{m}I_{\mathscr{N}}$ are the same for all i. So the images of the $\mathscr{R}(h_i)$ span $I_{\mathscr{N}}/\mathfrak{m}I_{\mathscr{N}}$ and $\mathscr{R}(h_1), \mathscr{R}(h_2), ..., \mathscr{R}(h_s)$ generate $I_{\mathscr{N}}$ by the homogeneous Nakayama Lemma. Now we follow the proof of Hilbert's Finiteness Theorem to conclude $\mathscr{O}(V)^G = k[\mathscr{R}(h_1), \mathscr{R}(h_2), ..., \mathscr{R}(h_s)]$. ∎

3. FINDING GENERATORS OF THE ZERO-FIBER IDEAL

If generators of the $I_{\mathcal{N}}$ are known, then generators of the ring of invariants are found by applying the Reynolds operator by Lemma 2.2. In this section we deal with the problem of finding generators of $I_{\mathcal{N}}$. Consider the map

$$\psi: G \times V \to V \times V$$

given by $\psi(g, v) = (v, g \cdot v)$. Let $B \subseteq V \times V$ be the image of ψ. The ideal $\mathfrak{b}$ of the Zariski-closure $\bar{B}$ of B is given by

$$\mathfrak{b} = \{h \in \mathcal{O}(V \times V) \mid h(v, g \cdot v) = 0 \ \forall g \in G, v \in V\}.$$

We will identify $\mathcal{O}(V \times V) \cong \mathcal{O}(V) \otimes \mathcal{O}(V)$ with the polynomial ring $k[X, Y]$, where X and Y are abbreviations of $X_1, X_2, ..., X_n$ and $Y_1, Y_2, ..., Y_n$.

THEOREM 3.1. *We have an equality*:

$$((Y_1, Y_2, ..., Y_n) + \mathfrak{b}) \cap k[X] = I_{\mathcal{N}}.$$

Proof. "$\supseteq$": If $f(X) = f(X_1, ..., X_n)$ is an invariant of positive degree, then we get $f(X) = (f(X) - f(Y)) + f(Y)$. Now $f(Y) \in (Y_1, ..., Y_n)$ and $f(X) - f(Y) \in \mathfrak{b}$ because $(f(X) - f(Y))(v, g \cdot v) = f(v) - f(g \cdot v) = 0$ for all $g \in G$, $v \in V$.

"$\supseteq$": Conversely, if $f(X) \in (Y_1, ..., Y_n) + \mathfrak{b}$, then we can write

$$f(X) = \sum_i c_i(X) f_i(Y) + b(X, Y) \tag{3.1}$$

where $c_i(X) \in k[X]$, $f_i(Y) \in (Y_1, ..., Y_n)$ for all i and $b(X, Y) \in \mathfrak{b}$. We will view $V \times V$ as a G-variety, where G acts only on the second factor. The corresponding Reynolds operator:

$$\mathcal{R}_Y: k[X, Y] \to k[X, Y]^G = k[Y]^G[X]$$

is a $k[X]$-module homomorphism and its restriction to $k[Y]$ is equal to the Reynolds operator $k[Y] \to k[Y]^G$ because of its uniqueness. We apply $\mathcal{R}_Y$ on (3.1):

$$f(X) = \sum_i c_i(X) \mathcal{R}_Y(f_i(Y)) + \mathcal{R}_Y(b(X, Y)). \tag{3.2}$$

Now $\mathscr{R}_Y(b(X, Y)) \in \mathfrak{b}$ because $\mathfrak{b}$ is G-stable (we use property (b) of the Reynolds operator). Let $\Delta: V \hookrightarrow V \times V$ be the diagonal morphism. The corresponding algebra homomorphism is $\Delta^*: k[X, Y] \to k[X]$, $p(X, Y) \mapsto p(X, X)$. Applying Δ^* to Eq. (3.2) yields

$$f(X) = \sum_i c_i(X)\, \mathscr{R}(f_i(X)).$$

In fact, we have $\Delta^*(\mathscr{R}_Y(b(X, Y))) = 0$, because $\mathscr{R}_Y(b(X, Y)) \in \mathfrak{b} \subseteq \ker(\Delta^*)$. Now the $\mathscr{R}(f_i(X))$ are homogeneous invariants of positive degree, and we conclude that $f(X)$ lies in $I_{\mathscr{N}}$. ∎

We can reformulate Theorem 3.1 as:

COROLLARY 3.2. *If the ideal* $\mathfrak{b}$ *of* $\bar{B}$ *is generated by the* $f_1(X, Y)$, $f_2(X, Y)$, ..., $f_r(X, Y)$, *then* $f_1(X, 0)$, $f_2(X, 0)$, ..., $f_r(X, 0)$ *generate* $I_{\mathscr{N}}$.

The geometric interpretation of Theorem 3.1 is

$$\bar{B} \cap (V \times \{0\}) = \mathscr{N} \times \{0\}.$$

It is important to notice that this equality holds in the schematic sense.

Remark 3.3. Theorem 3.1 can be generalized. If $(h_1(X), ..., h_r(X)) \subseteq k[X]$ is a G-invariant ideal, then

$$((h_1(Y), ..., h_r(Y)) + \mathfrak{b}) \cap k[X]$$

is the ideal of $k[X]$ generated by $(h_1(X), ..., h_r(X)) \cap k[X]^G$. Let $W \subseteq V$ is the zero set of $h_1, ..., h_r$, $\pi: V \to : V//G$ is the categorical quotient and $p_1 : V \times V \to V$ is the projection onto the first factor. Then the geometric interpretation of this generalization is

$$\overline{p_1((V \times W) \cap \bar{B})} = \pi^{-1}\pi(W).$$

A similar statement is true if V is an arbitrary affine G-variety.

4. DEGREE BOUNDS FOR GENERATING INVARIANTS

Let $\beta_G(V)$ be as in the introduction. Our aim is to give a good upper bound for $\beta_G(V)$. We first state two conjectures.

Conjecture 4.1 (Eisenbud–Goto). If $\mathfrak{p}$ is a homogeneous prime ideal in the polynomial ring $k[X_1, ..., X_n]$ of degree d, then the module of ith syzygies can be generated by homogeneous polynomials of degree

$$\leqslant d + i + \dim_k \mathfrak{p}_1 - \text{height } \mathfrak{p} + 1$$

where $\mathfrak{p}_1$ is the vector space of linear functions in $\mathfrak{p}$ (see [8]).

Conjecture 4.2 (Subspaces Conjecture). Suppose that W is a k-vector space and $W_1, W_2, ..., W_d \subset W$ are subspaces. If I is the ideal of $W_1 \cup W_2 \cup \cdots \cup W_d$, then I is generated by homogeneous polynomials of degree $\leqslant d$.

If G is a finite group then G is linearly reductive if and only if $\text{char}(k)$ does not divide $|G|$. Noeher's bound $\beta_G(V) \leqslant |G|$ is known only in the cases $\text{char}(k) = 0$ and $\text{char}(k) > |G|$.

PROPOSITION 4.3. *Suppose that the Subspaces Conjecture is true, and G is a linearly reductive finite group, i.e.,* $\text{char}(k)$ *doesn't divide* $|G|$. *Then we have* $\beta_G(V) \leqslant |G|$.

Proof. The image B of $\psi: G \times V \to V \times V$ is the union of at most $|G|$ subspaces of dimension n. The ideal $\mathfrak{b}$ of $B = \bar{B}$ is generated by polynomials of degree $\leqslant |G|$. Using the lemma below we conclude $\beta_G(V) \leqslant d$. ∎

LEMMA 4.4. *If* $\mathfrak{b}$ *is generated by homogeneous polynomials of degree* $\leqslant d$ *then we have* $\beta_G(V) \leqslant d$.

Proof. If $\mathfrak{b}$ is generated by $f_1(X, Y), ..., f_r(X, Y) \in k[X, Y]$, then $I_{\mathcal{N}}$ is generated by $f_1(X, 0), ..., f_r(X, 0)$ by Corollary 3.2 and the ring $\mathcal{O}(V)^G$ is generated by the invariants $\mathcal{R}(f_1(X, 0)), ..., \mathcal{R}(f_r(X, 0))$ by Lemma 2.2. If $\mathfrak{b}$ is generated by homogeneous polynomials of degree $\leqslant d$, then so is the invariant ring. ∎

Suppose that G is a linearly reductive m-dimensional group, and V is an n-dimensional G-module. Choose a maximal torus $T \subseteq G$. Now $X^*(T) = \hom(T, k^*) \cong \mathbb{Z}^r$ be the group of characters. Choose some norm $\|\cdot\|$ on $E := X(T) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^r$. The action of T on V can be assumed to be diagonal, and it acts with n weights, $\chi_1, \chi_2, ..., \chi_n \in X(T)$. Let

$$L_V = \max\{\|\chi_1\|, \|\chi_2\|, ..., \|\chi_n\|\}.$$

THEOREM 4.5. *If the Eisenbud–Goto Conjecture is true, G is a linearly reductive m-dimensional group and* $\mathrm{char}(k)=0$ *then there exist constants $C, C'>0$, depending only on the group G and the choice of $\|\cdot\|$, such that*

$$\beta_G(V)\leqslant \min\{C(nL_V)^m,\ C'L_V^{m^2+m}\}.$$

From now on we suppose $\mathrm{char}(k)=0$ and k algebraically closed. The variety $\bar{B}\subset V\times V$ is a cone. Therefore we can view $\bar{B}$ as a projective variety in $\mathbb{P}(V\times V)$ with some degree d. If G is connected, then $\bar{B}$ is irreducible and $\mathfrak{b}$ is a prime ideal. If the Eisenbud–Goto Conjecture is true, then $\beta_G(V)\leqslant d$ by Lemma 4.4. So we need a bound for d. For this we will use the formula of Kazarnoviskii.

We need some more notation. We fix a Borel subgroup B containing T. We denote by $\alpha_1, \alpha_2, \ldots, \alpha_{(m-r)/2}$, the positive roots. Let $\mathscr{W}$ be the Weyl group and let $e_1, e_2, \ldots, e_r$ be the Coxeter exponents, i.e., $e_1+1, e_2+1, \ldots, e_r+1$ are the degrees of the generating invariants of $\mathscr{W}$. We denote by $\mathscr{C}_V\subset E:=X^*(T)\otimes_{\mathbb{Z}}\mathbb{R}$ the convex hull of the weights appearing in V, $\chi_1, \chi_2, \ldots, \chi_n$. On E we use the volume form dV given by any isomorphism $E\cong\mathbb{R}^r$ which identifies $X^*(T)$ with $\mathbb{Z}^r$. Finally we fix a $\mathscr{W}$-invariant scalar product $(\cdot,\cdot)$ on E and denote, for any $\gamma\in E$, by $\hat{\gamma}\in E^*$ the dual element defined by $\hat{\gamma}(\alpha)=2(\alpha,\gamma)/(\gamma,\gamma)$.

For a representation $\rho: G\to \mathrm{GL}(V)$, let $\delta_G(V)$ be the number of solutions $g\in G$ of

$$S_1(\rho(g))=S_2(\rho(g))=\cdots=S_m(\rho(g))=0 \tag{4.1}$$

for general $S_1, S_2, \ldots, S_m\in \mathrm{End}(V)^*$.

THEOREM 4.6 (Kazarnovskii, [21]). *The number $\delta_G(V)$ is equal to*

$$\frac{m!}{|\mathscr{W}|\,(e_1!\,e_2!\cdots e_r!)^2}\int_{\mathscr{C}_V}(\hat{\theta}_1\hat{\theta}_2\cdots\hat{\theta}_{(m-r)/2})^2. \tag{4.2}$$

where $\theta_1, \theta_2, \ldots, \theta_{(m-r)/2}$ are the positive roots.

See [6] for a more algebraic proof and [2] for a generalization of this result.

COROLLARY 4.7. *There exists a constant $C>0$ such that*

$$\delta_G(V)\leqslant CL_V^m.$$

Proof. The homogeneous polynomial

$$f:=(\hat{\theta}_1\hat{\theta}_2\cdots\hat{\theta}_{(m-r)/2})^2$$

has degree $m-r$. So $|f(z)| \leqslant C'\|z\|^{m-r}$ for some $C'>0$. If we integrate f over a ball of radius L_V, then the result will be $\leqslant (2L_V)^r \cdot C' L_V^{m-r}$, so

$$\delta_G(V) \leqslant \frac{m!\, 2^r}{|\mathscr{W}|\,(e_1!\, e_2! \cdots e_r!)^2}\, C' L_V^m = C L_V^m. \quad \blacksquare$$

LEMMA 4.8. *If $S_1, S_2, ..., S_m$ are not in general position, $|\rho^{-1}(k^* \cdot \mathrm{id})| < \infty$ and the number of solutions of* (4.1) *is finite, then this number is still bounded from above by* (4.2).

Proof. Let $\hat{G} \subset \mathbb{P}(\mathrm{End}(V))$ be the projective variety given by the cone $k^* \cdot \rho(G)$. The number of solutions of (4.1) equals the number of solutions of $p \in \hat{G}$ of

$$S_1(p) = S_2(p) = \cdots = S_m(p) = 0$$

multiplied by $|\rho^{-1}(k^* \cdot \mathrm{id})|$. By a generalization of the Bézout Theorem by Fulton and McPherson (see 12.3 of [9] and II.2.2 of [35]) this number of solutions is maximal when $S_1, S_2, ..., S_m$ are in general position. $\blacksquare$

We return to the computation of an upper bound for d, the degree of $\bar{B} \subset V \times V$ viewed as a projective variety in $\mathbb{P}(V \times V)$. Observe that $B = G\Delta(V)$ where $\Delta(V)$ is the diagonal of $V \times V$ and G acts only on the second factor of $V \times V$. Now $\Delta(V)$ is the zero set of n linear functions $f_i = X_i - Y_i$ with $1 \leqslant i \leqslant n$. Define for $i = 1, 2, ..., m$ functions on $G \times (V^* \times V^*)^{n+m-1}$ by

$$P_i(g, h_1, h_2, ..., h_{n+m-1}) = \det(g \cdot f_1,\ g \cdot f_2, ...,\ g \cdot f_n, h_i, h_{i+1}, ..., h_{n+i-1})$$

LEMMA 4.9. *Suppose that the generic stabilizer of the G-action on V is finite. For $h_i \in V^* \times V^*$ general enough, fixed, the number of common solutions of the P_i is finite and $\geqslant d$.*

Proof. The dimension of B is equal to $n+m$ because the generic stabilizer is finite. The number of intersection points of B and $h_1 = h_2 = \cdots = h_{n+m-1} = 0$ in $\mathbb{P}(V \times V)$ is exactly d if the h_i are general linear functions on $V \times V$. So d is equal to the number of $g \in G$ for which

$$f_1(g \cdot p) = f_2(g \cdot p) = \cdots = f_n(g \cdot p) = h_1(p) = h_2(p) = \cdots = h_{n+m-1}(p) = 0 \tag{4.3}$$

has a solution $p \in \mathbb{P}(V \times V)$, divided by the order of the generic stabilizer. For every such g and $1 \leqslant i \leqslant m$ we have $P_i(g, h_1, h_2, ..., h_{n+m-1}) = 0$. So the P_i have at least d common solutions for general $h_1, ..., h_{n+m-1}$.

We now prove finiteness. Let $Z \subset G \times (V^* \times V^*)^{n+m-1}$ be the zero set of $P_1, P_2, ..., P_m$. The projection of Z onto G is surjective. For fixed $g \in G$ we will compute its fiber dimension. Set $\bar{h}_i = h_i + W \in (V^* \oplus V^*)/W$, where W is the span of all $g \cdot f_i$. Then

$$\det(g \cdot f_1,\ g \cdot f_2, ...,\ g \cdot f_n, h_i, h_{i+1}, ..., h_{n+i-1}) = \det(\bar{h}_i, \bar{h}_{i+1}, ..., \bar{h}_{n+i-1})$$

The solution space for $(\bar{h}_1, ..., \bar{h}_{n+m-1})$ for these equations has dimension $(n+m)(n-1)$ by Lemma 4.10 below. For every $\bar{h}_i$ we have an n-dimensional space of representatives h_i, so the fiber dimension is $(n+m-1)\,n + (n+m)(n-1) = 2n^2 + 2nm - 2n - m$. The dimension of Z is $m + (2n^2 + 2nm - 2n - m) = 2n^2 + 2nm - 2n$. The generic fiber of the projection to $(V^* \times V^*)^{n+m-1}$ must have dimension $(n+m-1)\,2n - (2n^2 + 2nm - 2n) = 0$, so the general fiber is finite. ∎

LEMMA 4.10. *The variety*

$$Y := \{(v_1, v_2, ..., v_t) \in k^{u \times t} \mid \det(v_i, v_{i+1}, ..., v_{i+u-1}) = 0 (1 \leqslant i \leqslant t-u+1)\}$$

has dimension $(t+1)(u-1)$.

Proof. The variety Y is given by $t-u+1$ equations, so the codimension of Y is $\leqslant t-u+1$. Let W be the $(t-u+1)$-dimensional subspace of $k^{u \times t}$ of all matrices

$$\begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_{t-u+1} & 0 & \cdots & 0 & 0 \\ 0 & \lambda_1 & \cdots & \lambda_{t-u} & \lambda_{t-u+1} & \cdots & 0 & 0 \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & 0 & \cdots & \lambda_1 & \lambda_2 & \cdots & \lambda_{t-u+1} & 0 \\ 0 & 0 & \cdots & 0 & \lambda_1 & \cdots & \lambda_{t-u} & \lambda_{t-u+1} \end{pmatrix}$$

Now $\det(v_1, v_2, ..., v_u) = 0$ gives us $\lambda_1^n = 0$, so $\lambda_1 = 0$. From the second equation $\det(v_2, ..., v_{u+1}) = 0$ follows $\lambda_2 = 0$, etc., so $W \cap Y = \{0\}$. So Y is a complete intersection and its dimension is $tu - (t-u+1) = (t+1)(u-1)$. ∎

Proof of Theorem 4.5. Let

$$\pi: G \to \mathrm{GL}\left(\bigwedge^n (V \times V)\right) \subset \mathrm{End}\left(\bigwedge^n (V \times V)\right)$$

be the representation of G on $\bigwedge^n (V \times V)$. Now $P_i(g)$ is equal to $Q_i(\pi(g))$ where $Q_i \in \mathrm{End}(\bigwedge^n (V \times V))^*$ is defined by

$$A \in \mathrm{End}\left(\bigwedge^n (V \times V)\right)$$

$$\mapsto (A(f_1 \wedge \cdots \wedge f_n)) \wedge h_i \wedge \cdots \wedge h_{n+i-1} \in \bigwedge^{2n} (V \times V) \cong k$$

We apply Corollary 4.7 for $\bigwedge^n (V \times V)$. The weights appearing in $\bigwedge^n (V \times V)$ are all $\sum_{j=1}^u \lambda_j$ with $u \leqslant n$ and $\lambda_1, ..., \lambda_u$ weights of linear independent T-eigenvectors $v_1, v_2, ..., v_u$ in V. It follows that $L_{\bigwedge^n (V \times V)} \leqslant nL_V$. The number of

$$Q_1(\pi(g)) = Q_2(\pi(g)) = \cdots = Q_{m+n-1}(\pi(g))$$

is finite by Lemma 4.9. So this number is at most $\delta_G(\bigwedge^n (V \times V))$ by Lemma 4.8. On the other hand, from Lemma 4.9 follows that the number of solutions is at least d. So we get $\beta_G(V) \leqslant d \leqslant C(nL_V)^m$.

If the generic stabilizer is not finite, take some fixed representation V' with trivial generic stabilizer. Then

$$\beta_G(V) \leqslant \beta_G(V \oplus V') \leqslant C_2((n+n')(\max\{L_V, L_{V'}\}))^m \leqslant C_3(nL_V)^m$$

where $n' = \dim V'$ and $C_3 > 0$ is a large enough constant.

If G is not connected, then let G° be the connected component of $\mathrm{id} \in G$, which is a normal subgroup. Now $\mathcal{O}(V)^{G^\circ}$ is generated by homogeneous invariants of degree $\leqslant C_3(nL_V)^m$. From Noether's bound follows that $\mathcal{O}(V)^G = (\mathcal{O}(V)^{G^\circ})^{G/G^\circ}$ is generated by homogeneous invariants of degree $\leqslant |G/G^\circ| C_3(nL_V)^m \leqslant C_4(nL_V)^m$.

Suppose we have a decomposition

$$V = V_1^{a_1} \oplus V_2^{a_2} \oplus \cdots \oplus V_t^{a_t}$$

where the V_i are irreducible and different. By Weyl's theorem (see [42]) the generators of invariants of $\mathcal{O}(V)$ can found by polarizing invariants of $\mathcal{O}(V')$ where

$$V' = V_1^{\dim(V_1)} \oplus V_2^{\dim(V_2)} \oplus \cdots \oplus V_t^{\dim(V_t)}$$

In this situation we have $\beta_G(V) \leqslant \beta_G(V') \leqslant C_4(n'L_V)^m$ where $n' = \dim V'$. The number of different irreducible representations of highest weight λ

where λ has length $\leqslant L_V$ is $\leqslant C_5 L_V^r$. These representations all have dimension $\leqslant C_6 L^{(m-r)/2}$ because of the *Weyl formula* (see 3.2.6 of [30]):

$$\dim V_\lambda = \prod_{i=1}^{1/2(m-r)} \frac{\hat{\theta}_i(\lambda+\rho)}{\hat{\theta}_i(\rho)} \qquad \text{where} \quad \rho = \frac{1}{2} \sum_{i=1}^{1/2(m-r)} \theta_i \in E$$

This implies $n' \leqslant (C_5 L_V^r)(C_6 L_V^{(m-r)/2})^2 \leqslant C_7 L_V^m$, and so we finally deduce

$$\beta_G(V) \leqslant C_4(n' L_V)^m \leqslant C_4(C_7 L_V^{m+1})^m = C_8 L_V^{m(m+1)}. \quad \blacksquare$$

EXAMPLE 4.11. *Binary forms.* Let $G = \mathrm{SL}_2(k)$. The set of weights can be identified with $\mathbb{Z}$. Let V_d is the vector space of binary forms of degree d. The highest weight of this SL_2-module is d, so we have $L = d$, $m = \dim G = 3$ and $n = \dim V_d = d+1$. Suppose that the Eisenbud–Goto Conjecture is true. Because of Theorem 4.5 we get

$$\beta_G(V_d) \leqslant C((d+1)\,d)^3 < C_2 d^6$$

for some constant $C_2 > 0$. If $V = V_{d_1} \oplus V_{d_2} \oplus \ldots \oplus V_{d_t}$ with $d_i \leqslant d$ for all i, then by Theorem 4.5 we have

$$\beta_G(V) \leqslant C' d^{3^2+3} = C' d^{12}.$$

Indeed, Jordan proved that in this case we even have

$$\beta_G(V) \leqslant d^6$$

for $d \geqslant 2$ (see [19] and [20]).

5. THE ALGORITHM

Suppose that $\mathcal{O}(G)$ is isomorphic to $k[Z_1, Z_2, \ldots, Z_s]/I_G$, where I_G is an ideal of $k[Z_1, Z_2, \ldots, Z_s]$ generated by $h_1, h_2, \ldots, h_r$. The linear action on k^n is given by

$$\begin{pmatrix} X_1^g \\ X_2^g \\ \vdots \\ X_n^g \end{pmatrix} = \begin{pmatrix} a_{1,1}(g) & a_{1,2}(g) & \cdots & a_{1,n}(g) \\ a_{2,1}(g) & a_{2,2}(g) & \cdots & a_{2,n}(g) \\ \vdots & \vdots & & \vdots \\ a_{n,1}(g) & a_{n,2}(g) & \cdots & a_{n,n}(g) \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}$$

for all $g \in G$, where $a_{i,j} \in k[Z_1, Z_2, ..., Z_s]$ ($a_{i,j}$ is determined up to elements of I_G). Let $\Gamma \subseteq G \times V \times V$ be the Zariski-closed subset $\{(g, x, gx) \mid g \in G, x \in V\}$. The coordinate ring of Γ is

$$k[Z_1, Z_2, ..., Z_s, X_1, X_2, ..., X_n, Y_1, Y_2, ..., Y_n]/I_\Gamma$$

where the ideal I_Γ is generated by I_G and all $Y_i - \sum_{j=1}^n a_{i,j} X_j$ with $i = 1, 2, ..., n$. Now $\bar{B}$ is the closure of the projection of $\Gamma \subseteq G \times V \times V$ onto $V \times V$. The ideal $\mathfrak{b}$ of $\bar{B}$ is equal to $I_\Gamma \cap k[X, Y]$. This intersection can be computed using Gröbner basis (see [1], [3], or [7] for an introduction to Gröbner Basis). Choose an admissible ordering on the monomials of $k[Z, X, Y]$ such that Z_i is bigger than any monomial in X and Y. Compute a Gröbner basis S of I_Γ with respect to this ordering. The set $S \cap k[X, Y]$ is a Gröbner bases of $\mathfrak{b} = I_\Gamma \cap k[X, Y]$ (with respect to the induced ordering on $k[X, Y]$). If this Gröbner basis is $\{f_1, f_2, ..., f_l\} \subset k[X, Y]$, then $\{f_1(X, 0), f_2(X, 0), ..., f_l(X, 0)\}$ generate $I_\mathcal{N}$ (by Corollary 3.2). And finally $\mathcal{R}(f_1(X, 0)), \mathcal{R}(f_2(X, 0)), ..., \mathcal{R}(f_l(X, 0))$ generate $k[X]^G$ (by Lemma 2.2).

Application of $\mathcal{R}$ is not a trivial computation. It depends on the group G. For example if G is finite then $\mathcal{R}: k[X] \to k[X]^G$ is given by

$$\mathcal{R}(f) = \frac{1}{|G|} \sum_{g \in G} f^g.$$

For a semi-simple group the map $\mathcal{R}$ can be computed using the action of the Lie-algebra on $k[X]$. We will not discuss this here.

The algorithm is as follows:

input: $s, n \in \mathbb{N}$, $h_1, h_2, ..., h_r$, $a_{i,j} \in k[Z_1, Z_2, ..., Z_s]$ $(1 \leqslant i, j \leqslant n)$
$I_\Gamma := \{Y_1 - \sum_{j=1}^n a_{1,j} X_j, ..., Y_n - \sum_{j=1}^n a_{n,j} X_j, h_1, ..., h_r\}$
$S := \mathtt{Gröbner}(I_\Gamma, Z_1 > Z_2 > \cdots > Z_s > X_1 > \cdots X_n > Y_1 > \cdots > Y_n)$
$\mathfrak{b} := S \cap k[X_1, X_2, ..., X_n, Y_1, Y_2, ..., Y_n]$
$I_\mathcal{N} := \{\mathtt{substitute}(\{Y_1 = 0, Y_2 = 0, ..., Y_n = 0\}, f) \mid f \in \mathfrak{b}\}$
output: $\{\mathcal{R}(g) \mid g \in I_\mathcal{N}\}$

6. EXAMPLES

In this section we will look at some concrete examples.

EXAMPLE 6.1. *$\mathcal{G}_m$-action with weights $-5, -3, 2, 4$.* We take the multiplicative group $\mathcal{G}_m$ with coordinate ring $k[Z_1, Z_2]/(Z_1 Z_2 - 1)$. The group

acts on the four-dimensional vector-space with weights -5, -3, 2, 4. The matrix of this representation is

$$\begin{pmatrix} Z_2^5 & 0 & 0 & 0 \\ 0 & Z_2^3 & 0 & 0 \\ 0 & 0 & Z_1^2 & 0 \\ 0 & 0 & 0 & Z_1^4 \end{pmatrix}$$

We use the algorithm of the previous section to compute $k[X_1, X_2, X_3, X_4]^{\mathscr{G}_m}$. Let $I_\Gamma \subseteq k[Z, X, Y]$ be the ideal of the graph Γ. It is given by

$$I_\Gamma = (Z_1 Z_2 - 1,\ Y_1 - Z_2^5 X_1,\ Y_2 - Z_2^3 X_2,\ Y_3 - Z_1^2 X_3,\ Y_4 - Z_1^4 X_4)$$

Using Gröbner basis we can compute $\mathfrak{b} = I_\Gamma \cap k[X, Y]$ which is equal to

$$\begin{aligned} \mathfrak{b} = (&X_4 Y_3^2 - X_3^2 Y_4,\ X_1 X_3 Y_2 - X_2 Y_1 Y_3,\ X_1 X_4 Y_2 Y_3 - X_2 X_3 Y_1 Y_4 \\ &X_1 X_2 X_4^2 - Y_1 Y_2 Y_4^2,\ X_2^2 X_3 X_4 - Y_2^2 Y_3 Y_4,\ X_2^2 X_4^2 Y_3 - X_3 Y_2^2 Y_4^2, \\ &X_1^2 X_4 Y_2^2 - X_2^2 Y_1^2 Y_4,\ X_2^3 X_4 Y_1 - X_1 Y_2^3 Y_4,\ X_1^2 X_3 X_4^2 - Y_1^2 Y_3 Y_4^2, \\ &X_1 X_2 X_3^2 X_4 - Y_1 Y_2 Y_3^2 Y_4,\ X_2^2 X_3^3 - Y_2^2 Y_3^3,\ X_1^2 X_4^3 Y_3 - X_3 Y_1^2 Y_4^3, \\ &X_2^3 X_3^2 Y_1 - X_1 Y_2^3 Y_3^2,\ X_1^2 X_3^3 X_4 - Y_1^2 Y_3^3 Y_4,\ X_1 X_2 X_3^4 - Y_1 Y_2 Y_3^4, \\ &X_1^3 X_4^3 Y_2 - X_2 Y_1^3 Y_4^3,\ X_2^4 X_3 Y_1^2 - X_1^2 Y_2^4 Y_3,\ X_2^4 X_4^3 - Y_2^4 Y_4^3, \\ &X_1^2 X_3^5 - Y_1^2 Y_3^5,\ X_2^5 Y_1^3 - X_1^3 Y_2^5,\ X_1^4 X_4^5 - Y_1^4 Y_4^5) \end{aligned}$$

We find generators of $I_{\mathscr{N}}$ by substituting $Y = 0$. The null-cone ideal is generated by the elements

$$\begin{gathered} X_1^4 X_4^5,\ X_1^2 X_3^5,\ X_2^4 X_3^4,\ X_1 X_2 X_3^4,\ X_1^2 X_3^3 X_4, \\ X_2^2 X_3^3,\ X_1 X_2 X_3^2 X_4,\ X_1^2 X_3 X_4^2,\ X_2^2 X_3 X_4,\ X_1 X_2 X_4^2 \end{gathered}$$

We don't have to apply the Reynolds operator here, because these generators are already $\mathscr{G}_m$-invariant. In the torus case the algorithm presented here does the same as Algorithm 1.4.5. in [40].

EXAMPLE 6.2. *The finite group S_3 acting on a direct sum of the irreducible 2-dimensional and the signum representation.* Let ζ be the third root of unity. As an algebraic set (but not as a group), S_3 is isomorphic to the set $\{1, \zeta, \zeta^2\} \times \{-1, 1\}$ because they have the same cardinality. A bijection is given by $(12)^j (123)^i \mapsto (\zeta^i, (-1)^j)$. So the coordinate ring of

S_3 can be identified with $k[Z_1, Z_2]/(Z_1^3-1, Z_2^2-1)$. The representation is given by the matrix

$$\begin{pmatrix} (1+Z_2)/2 & (1-Z_2)/2 & 0 \\ (1-Z_2)/2 & (1+Z_2)/2 & 0 \\ 0 & 0 & Z_2 \end{pmatrix} \begin{pmatrix} Z_1 & 0 & 0 \\ 0 & Z_1^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} Z_1(1+Z_2)/2 & Z_1^2(1-Z_2)/2 & 0 \\ Z_1(1-Z_2)/2 & Z_1^2(1+Z_2)/2 & 0 \\ 0 & 0 & Z_2 \end{pmatrix}$$

The ideal I_Γ defining Γ is given by

$$I_\Gamma = (Z_1^3-1, Z_2^2-1, Y_1 - X_1 Z_1(1+Z_2)/2 - X_2 Z_1^2(1-Z_2)/2,$$
$$Y_2 - X_1 Z_1(1-Z_2)/2 - X_2 Z_1^2(1+Z_2)/2, Y_3 - X_3 Z_2)$$

Eliminating Z_1 and Z_2 with Buchbergers Algorithm yields

$$\begin{aligned} \mathfrak{b} = (&X_3^2 - Y_3^2, X_1 X_2 - Y_1 Y_2, X_1^3 + X_2^3 - Y_1^3 - Y_2^3, \\ &X_3 Y_1^3 - X_3 Y_2^3 + 2X_2^3 Y_3 - Y_1^3 Y_3 - Y_2^3 Y_3, \\ &X_2 X_3 Y_1^2 - X_1^2 X_3 Y_2 + X_2 Y_1^2 Y_3 - X_1^2 Y_2 Y_3, \\ &X_1 X_3 Y_1^2 - X_2^2 X_3 Y_2 - X_1 Y_1^2 Y_3 + X_2^2 Y_2 Y_3, \\ &X_2^2 X_3 Y_1 - X_1 X_3 Y_2^2 + X_2^2 Y_1 Y_3 - X_1 Y_2^2 Y_3, \\ &X_1^2 X_3 Y_1 - X_2 X_3 Y_2^2 - X_1^2 Y_1 Y_3 + X_2 Y_2^2 Y_3, \\ &X_2^3 X_3 - X_3 Y_2^3 + X_2^3 Y_3 - Y_2^3 Y_3, \\ &X_2^4 - X_2 Y_1^3 + X_1^2 Y_1 Y_2 - X_2 Y_2^3) \end{aligned}$$

We obtain the zero-cone ideal by substituting $Y=0$:

$$I_{\mathcal{N}} = (X_3^2, X_1 X_2, X_1^3 + X_2^3, X_2^3 X_3, X_2^4)$$

Note that we don't need X_2^4 because $X_2^4 = X_2(X_1^3 + X_2^3) - X_1^2(X_1 X_2)$. The first three generators are already invariant and $\mathscr{R}(X_2^3 X_3) = \frac{1}{2}(X_2^3 X_3 - X_1^3 X_3)$. So we finally get

$$k[X_1, X_2, , X_3]^{S_3} = k[X_3^2, X_1, X_2, X_1^3 + X_2^3, X_2^3 X_3 - X_1^3 X_3]$$

Remark 6.3. See [22] and [10] for other methods to compute invariants of finite group actions. Kemper implemented his method in the INVAR package in MAPLE. In [23] he deals with the case where the ground field has positive characteristic.

EXAMPLE 6.4. *The group* SL_2 *acting on* $W \oplus W \oplus S^2W$ *where* W *is the standard* 2*-dimensional representation.* We take the group SL_2 whose coordinate ring is $k[Z_1, Z_2, Z_3, Z_4]/(Z_1Z_4 - Z_2Z_3 - 1)$. The standard representation on the 2-dimensional space W is given by the matrix

$$\begin{pmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{pmatrix}$$

The representation on S^2W is given by the matrix

$$\begin{pmatrix} Z_1^2 & 2Z_2Z_1 & Z_2^2 \\ Z_3Z_1 & Z_4Z_1 + Z_3Z_2 & Z_4Z_2 \\ Z_3^2 & 2Z_4Z_3 & Z_4^2 \end{pmatrix}$$

Now we will take the 7-dimensional vector space $V := W \oplus W \oplus S^2W$ and compute the invariants $k[X_1, X_2, ..., X_7]^{\mathrm{SL}_2}$. Let $I_\Gamma \subseteq k[Z, X, Y]$ be the ideal which describes the graph $\Gamma \subseteq G \times V \times V$. We have

$$\begin{aligned} I_\Gamma = (&Z_1X_1 + Z_2X_2 - Y_1, Z_3X_1 + Z_4X_2 - Y_2, Z_1X_3 + Z_2X_4 - Y_3, \\ &Z_3X_3 + Z_4X_4 - Y_4, Z_1^2X_5 + 2Z_1Z_2X^6 + Z_2^2X_7 - Y_5, \\ &Z_1Z_3X_5 + Z_2Z_3X_6 + Z_1Z_4X_6 + Z_2Z_4X_7 - Y_6, \\ &Z_3^2X_5 + 2Z_3Z_4X_6 + Z_4^2X_7 - Y_7, -Z_2Z_3 + Z_1Z_4 - 1) \end{aligned}$$

We choose an ordering on the monomials in $Z_1, ..., Z_4, X_1, ..., X_7, Y_1, ..., Y_7$ such that $Z_i >$ every monomial in X and Y and we compute the reduced Gröbner basis. In a computation in SINGULAR this basis had 66 elements of which 18 lie in the ring $k[X, Y]$. These 18 polynomials generate the ideal $\mathfrak{b}$. The ideal $\mathfrak{b}$ has 9 minimal generators, namely

$$\begin{aligned} \mathfrak{b} = (&X_1^2X_7 - 2X_1X_2X_6 + X_2^2X_5 - Y_1^2Y_7 + 2Y_1Y_2Y_6 - Y_2^2Y_5, \\ &X_1X_3X_7 - 2X_2X_3X_6 + X_2X_4X_5 + X_6Y_2Y_3 - X_6Y_1Y_4 - Y_1Y_3Y_7 \\ &\quad + Y_2Y_3Y_6 + Y_1Y_4Y_6 - Y_2Y_4Y_5, \\ &X_3^2X_7 - 2X_3X_4X_6 + X_4^2X_5 - Y_3^2Y_7 + 2Y_3Y_4Y_6 - Y_4^2Y_5, \\ &X_3X_7Y_1 - X_4X_6Y_1 - X_1X_7Y_3 + X_2X_6Y_3 + X_4Y_1Y_6 - X_2Y_3Y_6 \\ &\quad - X_4Y_2Y_5 + X_2Y_4Y_5, \\ &X_3X_6Y_1 - X_4X_5Y_1 - X_1X_6Y_3 + X_2X_5Y_3 + X_3Y_1Y_6 - X_1Y_3Y_6 \\ &\quad - X_3Y_2Y_5 + X_1Y_4Y_5, \end{aligned}$$

$$X_3X_7Y_2 - X_4X_6Y_2 - X_1X_7Y_4 + X_2X_6Y_4 + X_4Y_1Y_7 - X_2Y_3Y_7 - X_4Y_2Y_6 + X_2Y_4Y_6,$$
$$X_3X_6Y_2 - X_4X_5Y_2 - X_1X_6Y_4 + X_2X_5Y_4 + X_3Y_1Y_7 - X_1Y_3Y_7 - X_3Y_2Y_6 + X_1Y_4Y_6,$$
$$X_2X_3 - X_1X_4 - Y_2Y_3 + Y_1Y_4, X_6^2 - X_5X_7 - Y_6^2 + Y_5Y_7)$$

Substituting $Y - 0$ yields

$$I_{\mathcal{N}} = (X_1^2X_7 - 2X_1X_2X_6 + X_2^2X_5, X_1X_3X_7 - 2X_2X_3X_6 + X_2X_4X_5, X_3^2X_7 - 2X_3X_4X_6 + X_4^2X_5, X_2X_3 - X_1X_4, X_6^2 - X_5X_7)$$

These are all invariants except $X_1X_3X_7 - 2X_2X_3X_6 + X_2X_4X_5$. If we apply the Reynolds-operator then we obtain

$$\mathcal{R}(X_1X_3X_7 - 2X_2X_3X_6 + X_2X_4X_5) = X_1X_3X_7 - X_2X_3X_6 - X_1X_4X_6 + X_2X_4X_5$$

The ring of invariants is therefore generated by

$$X_1^2X_7 - 2X_1X_2X_6 + X_2^2X_5, X_1X_3X_7 - X_2X_3X_6 - X_1X_4X_6 + X_2x_4X_5, X_3^2X_7 - 2X_3X_4X_6 + X_4^2X_5, X_2X_3 - X_1X_4, X_6^2 - X_5X_7$$

Remark 6.5. The algorithm presented here is short and easy to implement. The computation of the Gröbner basis of I_Γ takes a lot of time, so it is recommended to use a fast computer algebra system. The algorithm is implemented in the computer algebra system SINGULAR. The computation of each example took less than a second on a Sparcstation 20.

REFERENCES

1. W. W. Adams and P. Loustaunau, "An Introduction to Gröbner Bases," Graduate Studies in Math. III, Am. Math. Soc., Providence, 1994.
2. M. Brion, Groupe de Picard et nombres charactéristiques des variétés sphériques, *Duke Math. J.* **58** (1989), 397–424.
3. D. Cox, J. Little, and D. O'Shea, "Ideals, Varieties and Algorithms," Springer-Verlag, New York, 1992.
4. H. Derksen, "Constructive Invariant Theory and the Linearization Problem," Thesis, University of Basel, 1997.
5. H. Derksen, Polynomial bounds for invariant rings, preprint, 1997.
6. H. Derksen and H. Kraft, Constructive invariant theory, *Colloq. Séminaires* (*S.M.F.*), in press.
7. D. Eisenbud, "Introduction to Commutative Algebra with a View Towards Algebraic Geometry," Graduate Texts in Mathematics, Springer-Verlag, New York, 1995.

8. D. Eisenbud and S. Goto, Linear free resolutions and minimal multiplicity, *J. Algebra* **88** (1984), 89–133.
9. W. Fulton, "Intersection Theory," Springer-Verlag, Berlin, 1984.
10. K. Gatermann, Semi-invariants, equivariants and algorithms, *Appl. Algebra Eng. Commun. Comput.* **7** (1996), 105–124.
11. P. Gordan, Beweis dass jede Covariante und Invariante einer binären Form eine ganze Funktion mit numerischen Coefficienten solcher Formen ist, *J. reine angew. Math.* **69** (1868), 323–354.
12. M. Göbel, Computing bases for rings of permutation-invariant polynomials, *J. Symbolic Comput.* **19**, No. 4 (1995), 285–291.
13. A. E. Heydtmann, "Generating Invariant Rings of Finite Groups," Diploma Thesis, Saarbrücken, 1996.
14. D. Hilbert, Über die Theorie der algebraischen Formen, *Math. Ann.* **36** (1890), 473–534.
15. D. Hilbert, Über die vollen Invariantensysteme, *Math. Ann.* **42** (1893), 313–373.
16. D. Hilbert, Mathematische Probleme, *Arch. Math. Phys.* **1** (1901), 44–63 213–237; In "Gesammelte Abhandlungen Band III," pp. 290-329, Springer-Verlag, Berlin/Heidelberg/New York, 1970.
17. K. Hiss, "Constructive Invariant Theory for Reductive Algebraic Groups," Thesis, Brandeis University, 1997.
18. M. Hochster and J. Roberts, Rings of invariants of reductive groups acting on regular rings are Cohen–Macaulay, *Adv. Math.* **13** (1974), 115–175.
19. C. Jordan, Mémoire sur les covariants des formes binaires, *J. Math.* **2**, No. 3 (1876), 177–232.
20. C. Jordan, Sur les covariants des formes binaires, *J. Math.* **5**, No. 3 (1879), 345–378.
21. B. Kazarnovskii, Newton polyhedra and the Bezout formula for matrix-valued functions of finite-dimensional representations, *Funct. Anal. Appl.* **21** (1987), 73–74.
22. G. Kemper, The Invar package for calculating rings of invariants, IWR preprint **93–94** (1993), University of Heidelberg.
23. G. Kemper, Calculating invariant rings of finite groups over arbitrary fields, *J. Symbolic Comput.* **21** (1996), 351–366.
24. H. Kraft, "Geometrische Methoden in der Invariantentheorie," Vieweg-Verlag, 1984.
25. F. Meyer, Invariantentheorie, *Encyklopädie math. Wissenschaften* **IB2** (1899), 345–378.
26. D. Mumford, J. Forgarty, and F. Kirwan, "Geometric Invariant Theory," Springer-Verlag, Berlin, 1994.
27. M. Nagata, On the 14th problem of Hilbert, *Amer. J. Math.* **81** (1959), 766–772.
28. M. Nagata, Invariants of a group in an affine ring, *J. Math. Kyoto Univ.* **3** (1963/64), 369–377.
29. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, *Math. Ann.* **77** (1916), 89–92.
30. A. L. Onishchik and E. B. Vinberg, (Eds.), "Lie Groups and Lie Algebras III" Encyclopaedia of Mathematical Sciences, Vol. 41, Springer-Verlag, Berlin, 1994.
31. V. Popov, Constructive invariant theory, *Astérique* **87-88** (1981), 303–334.
32. V. Popov, The constructive theory of invariants, *Math. USSR Izvest.* **10** (1982), 359–376.
33. B. Schmid, Generating invariants of finite groups, *C.R. Acad. Sci. Paris Série I* **308** (1989), 1–6.
34. B. Schmid, Finite groups and invariant theory, *in* "Séminaire d'Algèbre" (P. Dubreil and M.-P. Malliavin, Eds.), Lecture Notes in Math., Vol. 1478, Springer-Verlag, Berlin/Heidelberg/New York, 1991.
35. I. R. Shafarevich, (Ed.), "Algebraic Geometry I," Encyclopaedia of Mathematical Sciences, Vol. 23, Springer-Verlag, Berlin, 1994.

36. L. Smith, E. Noether's bound in the invariant theory of finite groups, *Arch. Math.* (*Basel*) **66**, No. 2 (1996), 89–91.
37. D. Snow, Reductive group actions on Stein spaces, *Math. Ann.* **259** (1982), 79–97.
38. T. A. Springer, Aktionen Reduktiver Gruppen auf Varietäten, *in* "Algebraische Transformationsgruppen und Invariantentheorie" (H. Kraft, P. Slodowy, and T. A. Springer, Eds.), Birkhäuser Verlag, 1989.
39. T. A. Springer, "Linear Algebraic Groups," Birkhäuser Verlag, 1991.
40. B. Sturmfels, "Algorithms in Invariant Theory," Springer-Verlag, Wien/New York, 1993.
41. D. Wehlau, Constructive invariant theory for tori, *Ann. Inst. Fourier* **43**, No. 4 (1993), 1055–1066.
42. H. Weyl, "The Classical Groups, their Invariants and Representations," Princeton Mathematical Series, Vol. 1, Univ. Press, Princeton, NJ, 1946.