PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 129, Number 4, Pages 955–963
S 0002-9939(00)05698-7
Article electronically published on October 20, 2000

POLYNOMIAL BOUNDS FOR RINGS OF INVARIANTS

HARM DERKSEN

(Communicated by Michael Stillman)

ABSTRACT. HILBERT proved that invariant rings are finitely generated for linearly reductive groups acting rationally on a finite dimensional vector space. POPOV gave an explicit upper bound for the smallest integer d such that the invariants of degree $\leq d$ generate the invariant ring. This bound has factorial growth. In this paper we will give a bound which depends only polynomially on the input data.

1. INTRODUCTION

Suppose that G is a linearly reductive algebraic group over an algebraically closed base field k of characteristic 0 and that G acts rationally on an n-dimensional vector space V. The coordinate ring $\mathcal{O}(V)$ of V can be identified with the polynomial ring $k[X_1, \ldots, X_n]$. The group G acts on $\mathcal{O}(V)$ and we will denote the ring of invariants by $\mathcal{O}(V)^G$. HILBERT proved in 1890 that $\mathcal{O}(V)^G$ is generated by finitely many invariants as a k-algebra (see [10]). This proof was criticized for not being constructive. In 1893 HILBERT gave another more constructive proof of his finiteness result (see [11]), but he did not give a degree bound for the generators of the invariant ring.

About a century later, POPOV did obtain an explicit degree bound (cf. [22], [23]) by combining HILBERT's second proof with some results which were not known in HILBERT's time. Let us define

$$\beta(V) := \min\{\, d \mid \mathcal{O}(V)^G \text{ can be generated by polynomials of degree} \leq d \,\}.$$

Then POPOV's bound is given by

$$\beta(V) \leq n \operatorname{LCM}(1, 2, \ldots, \sigma(V))$$

where LCM is the least common multiple. The constant $\sigma(V)$ is the smallest integer d with the following property: if $v \in V$ and and any non-constant homogeneous invariant vanishes on v, then there exists a non-constant homogeneous invariant f of degree $\leq d$ such that $f(v) \neq 0$. This bound seems far from sharp, but so far it was open whether a polynomial bound exists (see page 189 of [24]). In this paper we will improve POPOV's bound drastically to

Received by the editors July 8, 1999.
2000 *Mathematics Subject Classification.* Primary 13A50.
The author was partially supported by the Swiss National Science Foundation (SNF) and the Freiwillige Akademische Gesellschaft.

Theorem 1.1.

$$\beta(V) \leq \max\{2, \tfrac{3}{8} s\, \sigma^2(V)\} \tag{1.1}$$

where $s := \dim \mathcal{O}(V)^G \leq n$.

Upper bounds for $\sigma(V)$ were given by Popov (see [22], [23]) and Hiss (see [12]). As remarked in [5] a good upper bound can be found using a formula of Kazarnovskii (see [16]). We will give an explicit upper bound for $\sigma(V)$ expressed in the degrees of polynomials defining the group G and the representation V.

Since G is affine, it is given as the zero set of polynomials $h_1, h_2, \ldots, h_l \in k[Z_1, \ldots, Z_t]$ for some positive integers l and t. Because the representation is rational, there are polynomials $a_{i,j} \in k[Z_1, \ldots, Z_t]$ $(1 \leq i, j \leq n)$ such that the representation $\rho : G \to \mathrm{GL}(V)$ is given by

$$g \mapsto \begin{pmatrix} a_{1,1}(g) & a_{1,2}(g) & \cdots & a_{1,n}(g) \\ a_{2,1}(g) & a_{2,2}(g) & & a_{2,n}(g) \\ \vdots & & \ddots & \vdots \\ a_{n,1}(g) & a_{n,2}(g) & \cdots & a_{n,n}(g) \end{pmatrix}, \qquad g \in G.$$

In Section 5 we will show that

Proposition 1.2. *If ρ has finite kernel, then*

$$\sigma(V) \leq H^{t-m} A^m \tag{1.2}$$

where $H := \max\{\deg(h_1), \ldots, \deg(h_l)\}$, $A := \max_{i,j}\{\deg(a_{i,j})\}$ *and* $m := \dim(G)$.

2. An example

Example 2.1. We take $G = \mathrm{SL}(W)$ where W is a q-dimensional vector space. Let $V_d = S^d(W)$ be the d-th symmetric power. If we choose a basis of W, we get an embedding of G into the $q \times q$ matrices, which is a q^2-dimensional space. The coordinate ring of G is given by

$$\mathcal{O}(G) = k[\{Z_{i,j} \mid 1 \leq i, j \leq q\}]/(\det((Z_{i,j})) - 1).$$

So we have $t = q^2$, $m = q^2 - 1$ and $H = q$. The action of G on V is given by a matrix $(a_{i,j})$ where all $a_{i,j}$ have degree $\leq d$. So we can take $A = d$. By Proposition 1.2 we now have

$$\sigma(V_d) \leq q d^{q^2-1}.$$

Note that $s = \dim \mathcal{O}(V)^G \leq \dim V = n = \binom{q+d-1}{q-1}$. From Theorem 1.1 it now follows that

$$\beta(V_d) \leq \tfrac{3}{8}\tbinom{q+d-1}{q-1} q^2 d^{2q^2-2}.$$

Note that this upper bound depends only polynomially on d. If $q = 2$, then we have binary forms of degree d and $\beta(V_d) \leq \frac{3}{2}(d+1)d^6$. For ternary forms $(q = 3)$ we get $\beta(V_d) \leq \frac{27}{8}(d+2)(d+1)d^{18}$.

In some special cases, sharper estimates than Popov's bound were already known. Gordan proved finite generation of the invariant rings for $G = \mathrm{SL}_2$ in 1868 (see [9]), before Hilbert. Jordan used these techniques to obtain $\beta(V_d) \leq d^6$ (cf. [14], [15]), which is just slightly better than our estimate for $q = 2$. For a finite group G, Noether gave the estimate $\beta(V) \leq |G|$ where $|G|$ is the group order. If

G is not cyclic, then one even has better bounds (see [25] and [26]). WEHLAU gave a good degree bound for tori in [27].

In [11], HILBERT actually describes an algorithm for computing invariants. This has been worked out in [24]. For finite groups, algorithms are described in [8], [17] and [18]. In [3] and [4], the author describes an algorithm for computing generators of the invariant ring for linearly reductive groups. This algorithm is based on the finiteness proof in HILBERT's earlier paper (cf. [10]). If the EISENBUD-GOTO Conjecture (cf. [6]) is true, then polynomial bounds for generators of the invariant rings can be deduced from that algorithm. Theorem 1.1 gives a similar upper bound for $\beta(V)$ without relying on the EISENBUD-GOTO conjecture. This can be seen as empirical evidence for this conjecture.

3. Some basic results

We first recall some results of HILBERT's constructive proof (see [11]). The nullcone is defined as

$$\mathcal{N}_V := \{\, v \in V \mid f(v) = 0 \text{ for all } f \in \mathcal{O}(V)^G \text{ homogeneous of degree} > 0 \,\}.$$

If $f_1, \dots, f_r$ are polynomials in a coordinate ring $\mathcal{O}(X)$ of an affine variety X, then we will denote their common zero set in X by $\mathcal{Z}(f_1, \dots, f_r)$. We define $\sigma(V)$ as the smallest integer d such that homogeneous invariants $f_1, \dots, f_r$ exist of degree $\leq d$ with $\mathcal{Z}(f_1, \dots, f_r) = \mathcal{N}_V$. HILBERT gave an upper bound for $\sigma(V)$ ([11], §14). Using his *Nullstellensatz* HILBERT proved:

Proposition 3.1 ([11], §4)**.** *If $f_1, f_2, \dots, f_r \in \mathcal{O}(V)^G$ are homogeneous invariants such that their common zero set $\mathcal{Z}(f_1, \dots, f_r)$ is equal to $\mathcal{N}_V$, then the invariant ring $\mathcal{O}(V)^G$ is a finitely generated module over $k[f_1, f_2, \dots, f_r]$.*

Suppose that R is a graded algebra over k. A set $\{p_1, \dots, p_s\} \in R$ of homogeneous polynomials is called a *homogeneous system of parameters* of R if

(1) $p_1, p_2, \dots, p_s$ are algebraically independent,
(2) R is a finitely generated $k[p_1, \dots, p_s]$-module.

One can actually find a homogeneous system of parameters for $\mathcal{O}(V)^G$. Given homogeneous invariants $f_1, \dots, f_r \in \mathcal{O}(V)^G$, one can find a homogeneous system of parameters as follows: Put $f_i' = f_i^{d/d_i}$ where $d_i := \deg(f_i)$ for all i and d is the least common multiple of $d_1, d_2, \dots, d_r$. Then $f_1', \dots, f_r'$ are homogenous of degree d and we can apply the Noether Normalization Lemma (see §1 of [11] or [28], Chapter VII, §7, Theorem 25):

Lemma 3.2. *Suppose that X is an affine variety and $R = \mathcal{O}(X)$ is a graded domain, $R = \bigoplus_{i=0}^{\infty} R_i$ with $R_0 = k$ (i.e., X is an irreducible cone). Assume that $f_1, \dots, f_r \in R$ are homogeneous. Let s be the Krull dimension of $k[f_1, \dots, f_r]$. If $p_1, p_2, \dots, p_s$ are generic k-linear combinations of $f_1, \dots, f_r$, then $k[f_1, \dots, f_r]$ is a finite $k[p_1, \dots, p_s]$-module, and*

$$\mathcal{Z}(p_1, \dots, p_s) = \mathcal{Z}(f_1, \dots, f_r).$$

Let $s = \dim(\mathcal{O}(V)^G)$ and take $p_1, \dots, p_s$ generic combinations of $f_1', f_2', \dots, f_r'$ as above. It follows that $\mathcal{O}(V)^G$ is a finite $k[p_1, \dots, p_s]$-module and that $p_1, \dots, p_s$ are algebraically independent. So $p_1, \dots, p_s$ is a homogeneous system of parameters. We have a degree bound

$$\deg(p_i) := d = \mathrm{LCM}(d_1, \dots, d_s) \leq \mathrm{LCM}(1, 2, \dots, \sigma(V)). \tag{3.1}$$

There exists a polynomial q such that $k(p_1,\dots,p_s,q)$ is the quotient field of $\mathcal{O}(V)^G$. The invariant ring $\mathcal{O}(V)^G$ is the integral closure of $k[p_1,\dots,p_s]$ in the finite field extension $k(p_1,\dots,p_s,q)$. At this point HILBERT refers to KRONECKER who had a theory for computing such integral closures. HILBERT does not give an explicit bound for the degrees of generators.

In [22] and [23] POPOV showed that by combining HILBERT's construction of invariants with more recent results in commutative algebra one actually obtains an upper bound for the degree of generators for a connected semisimple group G. First of all, HOCHSTER and ROBERTS proved the following theorem.

Theorem 3.3. *If G is a linearly reductive group acting rationally on V, then the invariant ring $\mathcal{O}(V)^G$ is Cohen-Macaulay (cf.* [13]*).*

For a graded Cohen-Macaulay ring $R=\bigoplus_{i=0}^{\infty} R_i$ finitely generated over $R_0=k$, let $a(R)$ be the degree of the Hilbert series as a rational function (see [2], Definition 4.3.6). The number $-a(R)$ is the smallest i such that the i-graded piece $(\omega_R)_i\neq 0$ where ω_R is the canonical module (see [2], Definition 3.6.13 and the remark before Definition 4.3.6). KEMPF proved that always $a(\mathcal{O}(V)^G)\leq 0$ (see [19]). KNOP improved the result of KEMPF:

Theorem 3.4. *For an arbitrary linearly reductive G we have*

$$a(\mathcal{O}(V)^G)\leq -\dim(\mathcal{O}(V)^G)$$

(see [20]*).*

We obtain POPOV's bound by applying the following lemma.

Lemma 3.5. *Suppose that $R=\bigoplus_{i=0}^{\infty} R_i$ is a graded Cohen-Macaulay domain over $R_0=k$ and $p_1,\dots,p_s$ is a homogeneous system of parameters of R. Then there exist homogeneous $h_1,\dots,h_l\in R$ such that*

$$R=Ph_1\oplus Ph_2\oplus\cdots\oplus Ph_l$$

with $P:=k[p_1,\dots,p_s]$ and $\deg(h_j)\leq\sum_{i=1}^{s}\deg(p_i)+a(R)$ for all j.

Proof. It is equivalent with the Cohen-Macaulay property that R can be written as

$$R=Ph_1\oplus Ph_2\oplus\cdots\oplus Ph_l$$

with $h_1,\dots,h_l\in R$ homogeneous. Consider the Hilbert series

$$F(R,t):=\sum_{i=0}^{\infty}\dim(R_i)\,t^i=\frac{\sum_{j=1}^{l}t^{e_j}}{\prod_{i=1}^{s}(1-t^{d_i})}$$

where $e_j:=\deg(h_j)$ and $d_i:=\deg(p_i)$. It follows that

$$e_j\leq\sum_{i=1}^{s}d_i+a(R).$$

□

As in HILBERT's proof, one gets a homogenous system of parameters $p_1,\dots,p_s$ with $\deg(p_i)\leq \mathrm{LCM}(1,2,\dots,\sigma(V))$ (see (3.1)). From Theorem 3.4 and Lemma 3.5 we obtain homogeneous $h_1,\dots,h_l$ such that

$$\deg(h_j)\leq\sum_{i=1}^{s}\deg(p_i)\leq s\mathrm{LCM}(1,2,\dots,\sigma(V)),$$

so it follows that

$$\beta(V) \leq s\mathrm{LCM}(1, 2, \ldots, \sigma(V)).$$

This is the bound given by Popov. The bound is huge because of taking the least common multiple, which was necessary for applying the Noether Normalization Lemma. In the next section we will improve the bound by using a generalization of Lemma 3.5 to avoid the Noether Normalization Lemma.

4. Proof of the main theorem

Lemma 4.1. *Suppose Y is an affine variety over k and assume that Let $R := \mathcal{O}(Y)$ is graded such that $R = \bigoplus_{i=0}^{\infty} R_i$ and $R_0 = k$. Suppose that $f_1, f_2, \ldots, f_r \in R$ are homogeneous of positive degree and $l \leq r - s$ where $s := \dim k[f_1, \ldots, f_r]$. Then there exist homogeneous*

$$p_1, \ldots, p_r \in k[f_1, \ldots, f_r, X_1, \ldots, X_l] \subset R[X_1, X_2, \ldots, X_l]$$

such that

(1) $\mathcal{Z}(f_1, \ldots, f_r, X_1, \ldots, X_l) = \mathcal{Z}(p_1, \ldots, p_r) \subset Y \times k^l$,
(2) $p_i(0, \ldots, 0) = f_i$ *for all* i.

Proof. We will prove the lemma using induction with respect to l. Suppose that $l = 1$ and $\dim k[f_1, \ldots, f_r] < r$. The map

$$F = (f_1, \ldots, f_r) : Y \to k^r$$

is not dominant. One can find an $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_r) \in k^r$ which is not in the image of F. Define $p_i \in R[X_1]$ as $p_i := f_i - \alpha_i X_1^{d_i}$ where d_i is the degree of f_i. We claim that $\mathcal{Z}(f_1, \ldots, f_r, X_1) = \mathcal{Z}(p_1, \ldots, p_r) \subset Y \times k$. The inclusion "$\subseteq$" is clear and we will now prove "$\supseteq$". Suppose that $(y, x) \in \mathcal{Z}(p_1, \ldots, p_r) \subseteq Y \times k$. Assume that $x \neq 0$. Since R is graded, Y has a natural action of the multiplicative group $k \setminus \{0\}$ such that every element of degree d is a semi-invariant with weight d. Now we have

$$f_i(x^{-1}y) - \alpha_i = x^{-d_i} f_i(y) - \alpha_i = x^{-d_i} p_i(y, x) = 0$$

for all i. This contradicts the choice of $\alpha \in k^r$. So $x = 0$ and

$$f_i(y) = p_i(y, 0) = 0$$

for all i.

Suppose now that $l > 1$. From the induction hypothesis we get

$$h_1, \ldots, h_r \in k[f_1, \ldots, f_r, X_1, \ldots, X_{l-1}]$$

such that

(1) $\mathcal{Z}(f_1, \ldots, f_r, X_1, \ldots, X_{l-1}) = \mathcal{Z}(h_1, \ldots, h_r) \subset Y \times k^{l-1}$,
(2) $h_i(0, \ldots, 0) = f_i$ for all i.

Because

$$\dim k[h_1, \ldots, h_r] \leq \dim k[f_1, \ldots, f_r, X_1, \ldots, X_{l-1}] = s + l - 1 \leq r - 1$$

we can apply the $l = 1$ case to $k[h_1, \ldots, h_r]$. We get $p_1, \ldots, p_r \in k[h_1, \ldots, h_r, X_l]$ such that

(1) $\mathcal{Z}(h_1, \ldots, h_r, X_l) = \mathcal{Z}(p_1, \ldots, p_r) \subset Y \times k^l$,
(2) $p_i(X_1, \ldots, X_{l-1}, 0) = h_i(X_1, \ldots, X_{l-1})$ for all i.

Therefore it follows that

(1) $\mathcal{Z}(f_1,\dots,f_r,X_1,\dots,X_l)=\mathcal{Z}(h_1,\dots,h_r,X_l)=\mathcal{Z}(p_1,\dots,p_r)$,
(2) $p_i(0,\dots,0)=h_i(0,\dots,0)=f_i$ for all i. □

Proposition 4.2. *Suppose that $R=\bigoplus_{i=0}^{\infty}R_i$ is a graded Cohen-Macaulay domain over $R_0=k$. Assume that $f_1,f_2,\dots,f_r\in R$ are homogeneous of positive degree such that R is a finite $k[f_1,\dots,f_r]$-module. Then there exist homogeneous $h_1,\dots,h_l\in R$ such that*

(1) *R is generated by $h_1,\dots,h_l$ as a $k[f_1,\dots,f_r]$-module,*
(2) $\deg(h_i)\le\sum_{i=1}^{r}\deg(f_i)-r+a(R)+\dim(R)$.

Proof. Let $s:=\dim R=\dim k[f_1,\dots,f_r]$. By Lemma 4.1 there exist homogeneous

$$p_1,\dots,p_r\in k[f_1,\dots,f_r,X_1,\dots,X_{r-s}]$$

such that

(1) $\mathcal{Z}(p_1,\dots,p_r)=\mathcal{Z}(f_1,\dots,f_r,X_1,\dots,X_{r-s})=\{(0,0)\}\subset Y\times k^{r-s}$,
(2) $p_i(0,\dots,0)=f_i$ for all i.

We have that $R[X_1,\dots,X_{r-s}]$ is finite over the ring $k[p_1,\dots,p_r]$ by [28], Chapter VII §7, page 198. We have

$$\begin{aligned}\dim k[p_1,\dots,p_r]&=\dim R[X_1,\dots,X_{r-s}]\\&=s+(r-s)=r.\end{aligned}$$

It follows that $p_1,\dots,p_r$ are algebraically independent, so $p_1,\dots,p_r$ is a homogeneous system of parameters. Note that the Hilbert series $F(R[X_1,\dots,X_{r-s}],t)$ is equal to $F(R,t)/(1-t)^{r-s}$, so $a(R[X_1,\dots,X_{r-s}])=a(R)+s-r$. By Lemma 3.5 we get $k[p_1,\dots,p_r]$-module generators $u_1,\dots,u_l$ of $R[X_1,\dots,X_{r-s}]$ such that

$$\begin{aligned}\deg(u_j)&\le\sum_{i=1}^{r}\deg(p_i)+a(R[X_1,\dots,X_{r-s}])\\&=\sum_{i=1}^{r}\deg(f_i)+a(R)+\dim(R)-r.\end{aligned}$$

Define $h_j:=u_j(0,\dots,0)$ for all j. Then $h_1,\dots,h_l$ generate R as a $k[f_1,\dots,f_r]$-module. □

Proof of Theorem 1.1. We will now apply the proposition to invariant rings. Let $R=\mathcal{O}(V)^G$ and $s:=\dim\mathcal{O}(V)^G$. By the definition of $\sigma(V)$ there exist $f_1,\dots,f_r\in\mathcal{O}(V)^G$ such that $\mathcal{Z}(f_1,\dots,f_r)=\mathcal{N}_V\subset V$ and $d_i:=\deg(f_i)\le\sigma(V)$ for all i. By replacing f_i by some power, we may assume that $\frac{1}{2}\sigma(V)<d_i\le\sigma(V)$ for all i. If now for example $f_1,\dots,f_{s+1}$ have the same degree, then by the Noether Normalization Lemma (Lemma 3.2) we can choose generic linear combinations $h_1,\dots,h_s$ of $f_1,\dots,f_{s+1}$ such that

$$\mathcal{Z}(f_1,\dots,f_{s+1})=\mathcal{Z}(h_1,\dots,h_s)$$

and we can replace $f_1,\dots,f_{s+1}$ by $h_1,\dots,h_s$. So without loss of generality we may assume that $\{f_1,\dots,f_r\}$ contains at most s polynomials of each degree. By Proposition 3.1, $\mathcal{O}(V)^G$ is finitely generated as a $k[f_1,\dots,f_r]$-module. By Proposition 4.2

and Theorem 3.4 there exist homogeneous invariants $h_1, h_2, \dots, h_l$ which generate $\mathcal{O}(V)^G$ as a $k[f_1, \dots, f_r]$-module and

$$\deg(h_i) \le \sum_{i=1}^{r} \deg(f_i) - r + \dim(\mathcal{O}(V)^G) + a(\mathcal{O}(V)^G) \le \sum_{i=1}^{r} \deg(f_i) - r$$
$$= \sum_{i=1}^{r} (\deg(f_i) - 1) \le s.\left\lceil \tfrac{\sigma(V)-1}{2} \right\rceil + s.\left\lceil \tfrac{\sigma(V)+1}{2} \right\rceil + \cdots + s.(\sigma(V) - 1)$$

and this is equal to

$$\begin{cases} s(\frac{3}{8}\sigma^2(V) - \frac{1}{4}\sigma(V)), & \text{if } \sigma(V) \text{ is even,} \\ \\ s(\frac{3}{8}\sigma^2(V) - \frac{3}{8}), & \text{if } \sigma(V) \text{ is odd.} \end{cases}$$

Clearly $f_1, \dots, f_r, h_1, \dots, h_l$ generate $\mathcal{O}(V)^G$ as a k-algebra. Now $\deg(f_i) \le \sigma(V)$ and $\deg(h_j) \le \frac{3}{8}s\sigma^2(V)$ for all i and j. This proves that

$$\beta(V) \le \max\{\sigma(V), \frac{3}{8}s\sigma^2(V)\}.$$

In fact we claim that

$$\beta(V) \le \max\{2, \frac{3}{8}s\sigma^2(V)\}.$$

Clearly, if $s = 0$, then there are only constant invariants, so $\beta(V) = 0$. If $s > 0$ and $\sigma(V) \ge 3$, then $\frac{3}{8}s\sigma^2(V) \ge \frac{9}{8}\sigma(V) \ge \sigma(V)$. □

5. Upper bounds for $\sigma(V)$

Popov completed his degree bound by giving an explicit bound for $\sigma(V)$ following the ideas of Hilbert. Hiss found a sharper bound for $\sigma(V)$, which doesn't depend on the dimension n of V, following ideas of Knop (see [12] and [5]). In [5] it was shown that one can find an even better bound using the formula of Kazarnovskii (see [16] and [1] for a generalization).

Proof of Proposition 1.2. Suppose that $\rho : G \to \mathrm{End}(V)$ is a representation with finite kernel and define $\delta_{\mathrm{gen}}(V)$ as the degree of $\rho(G)$, i.e., the number of intersection points of $\rho(G)$ with m generic affine hyperplanes, where $m := \dim G$. In [5] it was shown that

$$\sigma(V) \le \delta_{\mathrm{gen}}(V).$$

Suppose now that $\mathcal{O}(G) \cong k[Z_1, \dots, Z_t]/(h_1, \dots, h_l)$, and that the representation ρ is given by

$$g \mapsto \begin{pmatrix} a_{1,1}(g) & a_{1,2}(g) & \cdots & a_{1,n}(g) \\ a_{2,1}(g) & a_{2,2}(g) & & a_{2,n}(g) \\ \vdots & & \ddots & \vdots \\ a_{n,1}(g) & a_{n,2}(g) & \cdots & a_{n,n}(g) \end{pmatrix}, \qquad g \in G,$$

with $a_{i,j} \in k[Z_1, \dots, Z_s]$ for all i, j. Put $H = \max\{\deg(h_1), \dots, \deg(h_l)\}$ and $A = \max_{i,j}\{\deg(a_{i,j})\}$. Let $h'_1, \dots, h'_{t-m}$ be generic linear combinations of $h_1, \dots, h_l$. The zero set of $h'_1, \dots, h'_{t-m}$ is a union of m-dimensional varieties. One of these components is G. Choose m generic hyperplanes, given by generic linear combinations $a'_1, \dots, a'_m$ of all $a_{i,j}$ and 1. The set $S = \{g \in G \mid a'_1(g) = \cdots = a'_m(g) = 0\}$

has $\geq \delta_{\mathrm{gen}}(V)$ elements (equality holds, when ρ is injective). We now have $\#S \leq Q$, where Q is the number of solutions $v \in k^t$ with

$$a'_1(v) = a'_2(v) = \cdots = a'_m(v) = h'_1(v) = \cdots = h'_{t-m}(v) = 0. \tag{5.1}$$

Note that Q is finite. Let $\overline{a}'_1, \ldots, \overline{a}'_m, \overline{h}'_1, \ldots, \overline{h}'_{t-m}$ be the homogenized polynomials on the projective space $\mathbb{P}^s$. Now $\deg(\overline{a}'_i) \leq A$ and $\deg(\overline{h}'_j) \leq H$ for all i, j. Their intersection may not be transversal, but by a generalized version (see [7], §12.3) of BÉZOUT's theorem, the intersection

$$\overline{a}'_1 = \cdots = \overline{a}'_m = \overline{h}'_1 = \cdots = \overline{h}'_{t-m} = 0$$

has at most $A^m H^{t-m}$ irreducible components. Therefore (5.1) has at most $H^{t-m}A^m$ solutions and we conclude that $\sigma(V) \leq \delta_{\mathrm{gen}}(V) \leq Q \leq H^{t-m}A^m$. This proves Proposition 1.2. □

References

[1] M. Brion, *Groupe de Picard et nombres charactéristiques des variétés spériques*, Duke Math. J. **58** (1989), 397–424. MR **90i:**14048

[2] W. Bruns, J. Herzog, *Cohen-Macaulay Rings*, Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press. MR **95h:**13020

[3] H. Derksen, *Constructive Invariant Theory and the Linearization Problem*, Ph.D. thesis, Basel, 1997.

[4] H. Derksen, *Computation of reductive group invariants*, Adv. in Math. **141** (1999), 366–384.

[5] H. Derksen, H. Kraft, *Constructive invariant theory*, Algèbre non commutative, groupes quantiques et invariants (Reims, 1995), Smin. Congr. **2**, Soc. Math. France, Paris, 1997, 221–244. CMP 99:08

[6] D. Eisenbud, S. Goto, *Linear Free Resolutions and Minimal Multiplicity*, J. of Algebra **88** (1984), 89–133. MR **85f:**13023

[7] W. Fulton, *Intersection Theory*, Ergebn. Math. und Grenzgebiete, 3. Folge, vol. 2, Springer–Verlag, Berlin–Heidelberg–New York, 1984. MR **85k:**14004

[8] K. Gatermann, *Semi-invariants, equivariants and algorithms*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), 105–124. MR **99b:**20010

[9] P. Gordan, *Beweis dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten solcher Formen ist*, J. für reine u. angew. Math. **69** (1868), 323–354.

[10] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.

[11] D. Hilbert, *Über die vollen Invariantensysteme* Math. Ann. **42** (1893), 313–373.

[12] K. Hiss, *Constructive invariant theory for reductive algebraic groups*, Preprint, 1993.

[13] M. Hochster, J. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Adv. Math. **13** (1974), 115–175. MR **50:**311

[14] C. Jordan, *Mémoire sur les covariants des formes binaires*, J. de Math. **(3) 2** (1876), 177–232.

[15] C. Jordan, *Sur les covariants des formes binaires*, J. de Math. **(3) 5** (1879), 345–378.

[16] B. Kazarnovskii, *Newton polyhedra and the Bezout formula for matrix-valued functions of finite-dimensional representations*, Functional Analysis and its Applications **21(4)** (1987), 73–74. MR **90e:**22023

[17] G. Kemper, *The* INVAR *package for calculating rings of invariants*, IWR Preprint **93-94** (1993), University of Heidelberg.

[18] G. Kemper, *Calculating invariant rings of finite groups over arbitrary fields*, J. Symbolic Computation **21** (1996), 351–366. MR **98f:**13005

[19] G. Kempf, *The Hochster-Roberts theorem of invariant theory*, Michigan Math. J. **26** (1979), 19–32. MR **80g:**14040

[20] F. Knop, *Der kanonische Modul eines Invariantenringes*, J. Algebra **127** (1989), 40–54. MR **90k:**14053

[21] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916), 89–92.

[22] V. Popov, *Constructive invariant theory*, Astérique **87–88** (1981), 303–334. MR **83i:**14040
[23] V. Popov, *The constructive theory of invariants*, Math. USSR Izvest. **10** (1982), 359–376.
[24] B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Vienna, 1993. MR **94m:**13004
[25] B. Schmid, *Generating invariants of finite groups*, C. R. Acad. Sci. Paris **308 Série I** (1989), 1–6. MR **90d:**20014
[26] B. Schmid, *Finite groups and invariant theory*, In: P. Dubreil, M.-P. Malliavin, editors, *Séminaire d'Algèbre*, Lecture Notes in Math. **1478**, Springer-Verlag, Berlin–Heidelberg–New York, 1991. MR **94c:**13002
[27] D. Wehlau, *Constructive invariant theory for tori*, Ann. Inst. Fourier **43, 4**, 1993. MR **95c:**14068
[28] O. Zariski, P. Samuel, *Commutative Algebra*, vol. II, D. van Nostrand Co., Inc., 1960. MR **22:**11006

Department of Mathematics, Massachusetts Institute of Technology 77, Massachusetts Avenue, Cambridge, Massachusetts 02139
E-mail address: hderksen@math.mit.edu