Constructive Invariant Theory

Harm DERKSEN & Hanspeter KRAFT*
Universität Basel

Abstract

Invariant theory has been a major subject of research in the 19th century. One of the highlights was Gordan's famous theorem from 1868 showing that the invariants and covariants of binary forms have a finite basis. His method was constructive and led to explicit degree bounds for a system of generators (Jordan 1876/79).

In 1890, Hilbert presented a very general finiteness result using completely different methods such as his famous "Basissatz." He was heavily attacked because his proof didn't give any tools to construct a system of generators. In his second paper from 1893 he again introduced new techniques in order to make his approach more constructive. This paper contains the "Nullstellensatz," "Noether's Normalization Lemma," and the "Hilbert-Mumford Criterion!"

We shortly overview this development, discuss in detail the degree bounds given by Popov, Wehlau and Hiss and describe some exciting new development relating these bounds with the (geometric) degree of projective varieties and with the Eisenbud-Goto conjecture. The challenge is still the fact that the degree bounds for binary forms given by Jordan are much better than those obtained from the work of Popov and Hiss.

Résumé

La théorie des invariants a été un sujet de recherche majeur au 19ème siècle. Un des résultats marquants a été le fameux théorème de Gordan en 1868 qui établissait que les invariants et les covariants des formes binaires ont une base finie ; sa méthode était constructive et a conduit à des bornes explicites des degrés d'un système de générateurs (Jordan 1876/79).

En 1890, Hilbert a présenté un résultat de finitude très général utilisant des méthodes complètement différentes comme le fameux "Basissatz." Il a été vivement attaqué parce que sa preuve ne construisait pas un système de générateurs explicite. Dans son deuxième papier datant de 1893, il a introduit de nouvelles techniques pour rendre son approche plus constructive. Ce dernier

AMS 1980 *Mathematics Subject Classification* (1985 *Revision*): 13A50, 13P99, 14L30, (14D25, 14Q15)

*Both authors were partially supported by SNF (Schweizerischer Nationalfonds). The second author likes to thank the Department of Mathematics at UCSD for hospitality during the preparation of this manuscript.

papier contient le “Nullstellensatz,” le « Lemme de Normalization de Noether » et le « Critère de Hilbert-Mumford »!

Nous présentons brièvement ces développements, discutons en détail les bornes pour les degrés donnés par Popov, Wehlau et Hiss et décrivons certains nouveaux résultats reliant ces bornes avec le degré (géométrique) de certaines variétés projectives et avec la conjecture de Eisenbud-Goto. Encore maintenant, le défi est que les bornes des degrés données par Jordan pour les formes binaires sont meilleures que celles obtenues dans le travail de Popov et Hiss.

1 Introduction

Let $\rho\colon G \to \mathrm{GL}(V)$ be a representation of a group G on a vector space V of dimension $n < \infty$. For simplicity, we assume that the base field k is algebraically closed and of characteristic zero. As usual, the group G acts linearly on the k-algebra $\mathcal{O}(V)$ of polynomial functions on V, the *coordinate ring* of V. Of special interest is the subalgebra of invariant functions, the *invariant ring*, which will be denoted by $\mathcal{O}(V)^G$. It carries a lot of information about the representation itself, its orbit structure and its geometry, cf. [MFK94], [Kra85].

The ring of invariants was a major object of research in the last century. We refer to the encyclopedia article [Mey99] of Meyer from 1899 for a survey (see also [Kra85]). There are a number of natural questions in this context:

– *Is the invariant ring $\mathcal{O}(V)^G$ finitely generated as a k-algebra?*

– *If so, can one determine an explicit upper bound for the degrees of a system of generators of $\mathcal{O}(V)^G$?*

– *Are there algorithms to calculate a system of generators and what is their complexity?*

The first question is essentially Hilbert’s 14th problem, although his formulation was more general (see [Hil01]). The answer is positive for *reductive* groups by results of Hilbert, Weyl, Mumford, Nagata and others (see [MFK94]), but negative in general due to the famous counterexample of Nagata [Nag59]. We will not discuss this here. For a nice summary of Hilbert’s 14th problem we refer to [New78, pp. 90–92].

Our main concern is the second question. For this purpose let us introduce the number $\beta(V)$ associated to a given representation V of G:

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

In the following we discuss upper bounds for $\beta(V)$. We start with a historical sketch followed by a survey of classical and recent results. In the last paragraph we add a few remarks about algorithms.

2 Gordan's work on binary forms

The first general finiteness result was obtained by Paul Gordan in 1868 ([Gor68]). This was clearly one of the highlights of classical invariant theory of the 19th century which has seen a lot of interesting work in this area by famous mathematicians, like Boole, Sylvester, Cayley, Aronhold, Hermite, Eisenstein, Clebsch, Gordan, Lie, Klein, Cappelli and others.

Theorem 2.1 — *For every finite dimensional* SL_2*-module* V *the ring of invariants* $\mathcal{O}(V)^{\mathrm{SL}_2}$ *is finitely generated as a* k*-algebra.*

Beside invariants Gordan also studies *covariants* and shows that they form a finitely generated k-algebra. (This is in fact contained in the theorem above as we will see below.) We shortly recall the definition.

Let V_d denote the *binary forms of degree* d, i.e., the vector space of homogeneous polynomials in x, y of degree d. The group SL_2 acts on this $(d+1)$-dimensional vector space by substitution:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot p(x,y) := p(ax+cy, bx+dy) \quad \text{for } p(x,y) \in V_d.$$

It is well-known that the modules V_d $(d = 0, 1, \dots)$ form a complete set of representatives of the simple SL_2-modules.

Definition 2.2 — *Let* W *be an* SL_2*-module. A covariant of degree* m *and order* d *of* W *is an equivariant homogeneous polynomial map* $\varphi\colon W \to V_d$ *of degree* m*, i.e., we have* $\varphi(g \cdot w) = g \cdot \varphi(w)$ *for* $g \in \mathrm{SL}_2$ *and* $\varphi(tw) = t^m \varphi(w)$ *for* $t \in k$*.*

A covariant can be multiplied by an invariant function. Thus the covariants $\mathcal{C}_d(W)$ of a fixed order d form a module over the ring of invariants. In fact, one easily sees that $\mathcal{C}_d(W) = (\mathcal{O}(W) \otimes V_d)^{\mathrm{SL}_2}$ in a canonical way. More generally, multiplication of binary forms defines a bilinear map $V_d \times V_e \to V_{d+e}$. With this multiplication the vector space $\mathcal{C}(W) := \bigoplus_d \mathcal{C}_d(W)$ of covariants becomes a graded k-algebra, the *ring of covariants*, which contains the ring of invariants as its component of degree 0. In fact, $\mathcal{C}(W)$ is itself a ring of invariants:

$$\mathcal{C}(W) = \bigoplus_d (\mathcal{O}(W) \otimes V_d)^{\mathrm{SL}_2} = (\mathcal{O}(W) \otimes \mathcal{O}(V_1))^{\mathrm{SL}_2} = \mathcal{O}(W \oplus V_1)^{\mathrm{SL}_2}.$$

This algebra has an important additional structure given by *transvection* (in German: "Überschiebung"). It is based on the Clebsch-Gordan formula which tells us that there is a canonical decomposition

$$V_d \otimes V_e \simeq V_{d+e} \oplus V_{d+e-2} \oplus \cdots \oplus V_{d-e}$$

as an SL_2-module where we assume that $d \geq e$. Then the *ith transvection* of two covariants φ, ψ of order d, e, respectively, is defined by

$$(\varphi, \psi)_i := \mathrm{pr}_i \circ (\varphi \otimes \psi)$$

where pr_i is the linear projection of $V_d \otimes V_e$ onto V_{d+e-2i}. This is clearly a covariant of order $d + e - 2i$ and degree $\deg \varphi + \deg \psi$.

By representing a binary form as a product of linear forms, i.e., by considering the equivariant surjective morphism $V_1^d \to V_d$ given by multiplication, one can produce a natural system of generators for the vector space of covariants whose elements are represented by so-called *symbolic expressions.* This is based on the fact that the invariants and covariants of an arbitrary direct sum of linear forms $W = V_1^N$ are well-known and easy to describe. Represent an element of $\ell = (\ell_1, \ell_2, \dots, \ell_N) \in V_1^N$ as a $2 \times N$-matrix

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_N \\ b_1 & b_2 & b_3 & \cdots & b_N \end{pmatrix} \qquad \text{where } \ell_i = a_i x + b_i y.$$

Then the invariants are generated by the 2×2-minors $[i, j] := \det \begin{pmatrix} a_i & a_j \\ b_1 & b_j \end{pmatrix}$ and the covariants of order d by the maps $\ell \mapsto \ell_{i_1} \ell_{i_2} \cdots \ell_{i_d}$. This approach is classically called *symbolic method* (cf. [GrY03], [Schu68]).

By rather technical manipulations of these symbolic expressions Gordan was able to prove that the ring of covariants is finitely generated. He starts with a finite number of very simple covariants and shows that one only needs finitely many (multiple) transvections in order to obtain a complete system of generators. Gordan's method is constructive and he easily produces a system of generators for the invariants and covariants of V_d for $d \leq 5$.

Using the same method of symbolic expressions Camille Jordan is able to give the following explicit bounds for the degrees of the generators ([Jor76, Jor79]).

Theorem 2.3 — *The ring of covariants of $W = \bigoplus V_{d_i}$ where $d_i \leq d$ for all i is generated by the covariants of order $\leq 2d^2$ and degree $\leq d^6$, for $d \geq 2$.*

In particular, we obtain in our previous notation $\beta(V_d) \leq d^6$. This is really a big achievement. Today, a similar polynomial bound is not known for any other semi-simple group! We refer to the work of Jerzy Weyman [Wey93] for a modern interpretation of Gordan's method.

3 Hilbert's general finiteness results

In 1890 David Hilbert proved a very general finiteness result using completely new methods ([Hil90]). He formulated it only for the groups SL_n and GL_n, but he was fully aware that his results generalize to other groups provided that there exists an analogue to the Ω-process (see [Hil90, pp. 532–534]).

Finiteness Theorem — *Let V be a G-module and assume that the linear representation of G on $\mathcal{O}(V)$ is completely reducible. Then the invariant ring $\mathcal{O}(V)^G$ is finitely generated as a k-algebra.*

This result applies to *linearly reductive groups*, i.e., algebraic groups whose rational representations are completely reducible. Finite groups, tori and the classical groups are examples of such groups.

The proof of Hilbert uses the following two main facts:

1. Every ideal in the polynomial ring $\mathcal{O}(V) = k[x_1, x_2, \ldots, x_n]$ is finitely generated.
   (This is the famous "Basissatz;" it is theorem 1 of Hilbert's paper.)
2. There exits a linear projection $R\colon \mathcal{O}(V) \to \mathcal{O}(V)^G$ which is a $\mathcal{O}(V)^G$-module homomorphism and satisfies $R(g \cdot f) = R(f)$ for all $g \in G$.
   (R is called *Reynolds operator.*)

In Hilbert's situation (i.e. $G = \mathrm{SL}_n$ or GL_n) this operator R corresponds to Cayley's Ω-process (cf. [Hil90], [We46, VIII.7] or [Spr89, II.2.3]). For finite groups it is given by

$$R\colon f \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot f$$

Using these two facts Hilbert's proof of the Finiteness Theorem is not difficult:

Proof. Let I be the ideal of $\mathcal{O}(V)$ generated by all G-invariant homogeneous polynomials of positive degree. By (1) we can find finitely many homogeneous G-invariant generators $f_1, f_2, \ldots, f_r$ of I. We claim that $\mathcal{O}(V)^G = k[f_1, f_2, \ldots, f_r]$. In fact, we show by induction on d that every homogeneous invariant polynomial f of degree d lies in $k[f_1, f_2, \ldots, f_r]$.

The case $d = 0$ is trivial. Suppose $d > 0$. Then $f \in I$ and we can write it in the form

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_r f_r \qquad \text{where } a_1, a_2, \ldots, a_r \in \mathcal{O}(V).$$

Applying R from (2) yields

$$f = b_1 f_1 + b_2 f_2 + \cdots + b_r f_r \qquad \text{where } b_i = R(a_i) \in \mathcal{O}(V)^G \text{ for all } i.$$

Since we can replace each b_i by its homogeneous part of degree $d - \deg(f_i)$ we may assume that b_i is homogeneous of degree $< d$. Hence, by induction, $b_1, b_2, \ldots, b_r \in k[f_1, f_2, \ldots, f_r]$ and so $f \in k[f_1, f_2, \ldots, f_r]$. □

It is clear that this proof is highly non-constructive and does not provide any tools to determine a system of generators. Also it does not give an upper bound for the degrees of the generators f_i. When Gordan took notice of the new methods of Hilbert he made his famous exclamation: "Das ist Theologie und nicht Mathematik."[1]

In view of many complaints about the non-constructiveness of his proof Hilbert wrote a second paper [Hil93] in which he describes a way to construct generators of the ring of invariants. This paper is very important for the development of algebraic geometry as we will see below. Let us first introduce the *nullcone* $\mathcal{N}_V$ in V:

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

It is also called *null-fiber* since it is the fiber $\pi^{-1}(\pi(0))$ of the *quotient morphism* $\pi\colon V \to V/\!\!/G$ defined by the inclusion $\mathcal{O}(V)^G \hookrightarrow \mathcal{O}(V)$ (see [Kra85]). Now Hilbert proves the following result.

Proposition 3.1 — *If $h_1, h_2, \ldots, h_r$ are homogeneous invariants such that the zero set of $h_1, h_2, \ldots, h_r$ in V is equal to $\mathcal{N}_V$ then $\mathcal{O}(V)^G$ is a finitely generated module over the subalgebra $k[h_1, h_2, \ldots, h_r]$.*

For the proof of this proposition Hilbert formulates (and proves) his famous *Nullstellensatz.* In fact, if I is the ideal of $\mathcal{O}(V)$ generated by all G-invariant homogeneous polynomials of positive degree (see the proof of the Finiteness Theorem above) then it follows from the Nullstellensatz that $I^m \subset (h_1, h_2, \ldots, h_r)$ for some $m > 0$ since both ideals have the same zero set. It follows that there exists an integer $N > 0$ such that every homogeneous invariant of degree $\geq N$ belongs to the ideal $(h_1, h_2, \ldots, h_r)$. From this one easily sees that the invariants of degree $< N$ generate $\mathcal{O}(V)^G$ as a module over the subalgebra $k[h_1, h_2, \ldots, h_r]$.

Let us define another number $\sigma(V)$ associated to a representation V:

$$\sigma(V) := \min\{d \mid \mathcal{N}_V \text{ is defined by homogeneous invariants of degree} \leq d\}.$$

Equivalently, $\sigma(V)$ is the smallest integer d such that for every $v \in V \setminus \mathcal{N}_V$ there is a non-constant homogeneous invariant f of degree $\leq d$ such that $f(v) \neq 0$. Hilbert shows that there is an upper bound for $\sigma(V)$ in terms of the data of the representation. (He only considers the case $G = \mathrm{SL}_n$.)

The next step in the proof of Hilbert is the following result (which is nowadays called "Noether's Normalization Lemma!").

[1] "This is theology and not mathematics!"

Proposition 3.2 — *There exist algebraically independent homogeneous invariants $p_1, p_2, \dots, p_s$ such that $\mathcal{O}(V)^G$ is a finitely generated module over the polynomial ring $k[p_1, p_2, \dots, p_s]$.*

Such a set $p_1, p_2, \dots, p_s$ is called a *homogeneous system of parameters.*

Sketch of proof. Suppose that $f_1, f_2, \dots, f_r$ are homogeneous invariants with degrees $d_1, d_2, \dots, d_r$ defining $\mathcal{N}_V$, as in Proposition 3.1. Let $d := \operatorname{lcm}(d_1, d_2, \dots, d_r)$, the least common multiple. The powers $f_1' := f_1^{d/d_1}, f_2' := f_2^{d/d_2}, \dots, f_r' := f_r^{d/d_r}$ also have the nullcone as common set of zeroes and these functions are all homogeneous of the same degree d. Now it is not difficult to show that there exist algebraically independent linear combinations $p_1, p_2, \dots, p_s$ of $f_1', f_2', \dots, f_r'$ such that $\mathcal{O}(V)^G$ is integral over $k[p_1, p_2, \dots, p_s]$. □

The final step is the existence of a *primitive element.* Hilbert shows that we can find another homogeneous invariant p such that $k[p_1, p_2, \dots, p_s, p]$ and $\mathcal{O}(V)^G$ have the same field of fractions K. Then he remarks that $\mathcal{O}(V)^G$ is the integral closure of $k[p_1, p_2, \dots, p_s, p]$ in this field K. At this point Hilbert refers to Kronecker whose general theory of fields contains a method to compute the integral closure of $k[p_1, p_2, \dots, p_s]$ within the field $k(p_1, p_2, \dots, p_s, p)$. But he does not give an explicit upper bound for $\beta(V)$.

The importance of these two papers of Hilbert for the development of commutative algebra and algebraic geometry can hardly be overestimated. As already mentioned above they contain the Finiteness Theorem, Hilbert's Basis Theorem, the Nullstellensatz, Noether's Normalization Lemma, the Hilbert-Mumford Criterion and the finiteness of the syzygy-complex. It seems that these completely new methods and deep results were not really estimated by some of the mathematicians of that time. Following is part of a letter written by Minkowski to Hilbert on February 9th, 1892 ([Min73, page 45]):[2]

> (...) Dass es nur eine Frage der Zeit sein konnte, wann Du die alten Invariantenfragen soweit erledigt haben würdest, dass kaum noch das Tüpfelchem auf dem i fehlt, war mir eigentlich schon seit lange nicht zweifelhaft. Dass es aber damit so schnell geht, und alles so überraschend einfach gelingt, hat mich aufrichtig gefreut, und beglückwünsche ich Dich dazu. Jetzt, wo Du in Deinem letzten Satze sogar das rauchlose Pulver gefunden hast, nachdem schon Theorem I nur noch vor Gordans Augen Dampf gab, ist es wirklich an der Zeit, dass die Burgen der Raubritter Stroh, Gordan, Stephanos und wie sie alle heissen mögen, welche die

[2]We like to thank Reinhold Remmert for showing us this letter and Lance Small for his help with the translation.

einzelreisenden Invarianten überfielen und in's Burgverliess sperrten, dem Erdboden gleich gemacht werden, auf die Gefahr hin, dass aus diesen Ruinen niemals wieder neues Leben spriesst.[3] (...)

4 Popov's bound for semi-simple groups

It took almost a century until Vladimir Popov determined a general bound for $\beta(V)$ for any semi-simple group G ([Pop81, Pop82]), combining Hilbert's ideas with the following fundamental result due to Hochster and Roberts [HoR74].

Theorem 4.1 — *If G is a reductive group then the invariant ring $\mathcal{O}(V)^G$ is Cohen-Macaulay.*

Recall that being Cohen-Macaulay means in our situation that for each homogeneous system of parameters $p_1, p_2, \ldots, p_s$ of $\mathcal{O}(V)^G$ it follows that $\mathcal{O}(V)^G$ is a finite *free* module over $P := k[p_1, p_2, \ldots, p_s]$. So there exists homogeneous *secondary* invariants $h_1, h_2, \ldots, h_m$, such that

$$\mathcal{O}(V)^G = Ph_1 \oplus Ph_2 \oplus \cdots \oplus Ph_m.$$

Put $d_i := \deg(p_i)$ and $e_j := \deg(h_j)$. Then the *Hilbert-series* of $\mathcal{O}(V)^G$ has the following form:

$$F(\mathcal{O}(V)^G, t) = \frac{\sum_{j=1}^m t^{e_j}}{\prod_{i=1}^s (1 - t^{d_i})}.$$

Moreover, Knop showed in [Kno89, Satz 4] that the degree of the rational function $F(\mathcal{O}(V)^G, t)$ is always $\leq -\dim \mathcal{O}(V)^G$. Thus

$$\max_j e_j \leq d_1 + d_2 + \cdots + d_s - s$$

and we get

$$\beta(V) \leq d\,s \leq d \dim V \quad \text{where } d := \max_{i=1,\ldots,s} d_i.$$

It remains to find an upper bound for the degrees of a homogeneous system of parameters. Popov first determined an estimate for $\sigma(V)$ in case of a connected semisimple group G, following the original ideas of Hilbert:

$$\sigma(V) \leq c(G)\,(\dim V)^{2m-r+1} \omega(V)^r$$

[3] (...) For a long time I have not doubted that it is only a question of time until you solved the old problems of invariant theory without leaving the tiniest bit. But I was frankly delighted that it happened so quickly and that your solution is so surprisingly simple, and I congratulate you. Now, after you have discovered with your last theorem the smokeless gunpowder where already your Theorem 1 only for Gordan generated steam, it is really the right time to raze to the ground the castles of the robber knights Stroh, Gordan, Stephanos and others who may be so called who attacked the lonely traveling invariants and put them into the dungeon. Hopefully, from these ruins never again shall new life arise. (...)

where $m := \dim G$, $r := \operatorname{rank} G$, $c(G) := \frac{2^{m+r}(m+1)!}{3^m(\frac{m-r}{2})!^2}$ and $\omega(V)$ is the maximal exponent in a weight of V.

Thus, there are homogeneous invariants $f_1, f_2, \dots, f_r$ of degree $\leq \sigma(V)$ whose zero set equals $\mathcal{N}_V$. We have seen in the proof of Proposition 3.2 that there exists a homogeneous system of parameters $p_1, p_2, \dots, p_s$ where all p_j are of degree $d := \operatorname{lcm}(\deg f_1, \deg f_2, \dots, \deg f_r) \leq \operatorname{lcm}(1, 2, \dots, \sigma(V))$ where $\operatorname{lcm}(\dots)$ denotes the least common divisor. Summing up we finally get the following result [Pop81].

Theorem 4.2 — *For a representation of a semi-simple group G on a vector space V one has*

$$\sigma(V) \leq \frac{2^{m+r}(m+1)!}{3^m(\frac{m-r}{2})!^2} \cdot (\dim V)^{2m-r+1}\omega(V)^r$$

where $m := \dim G$, $r := \operatorname{rank} G$ and $\omega(V)$ is the maximal exponent in a weight of V, and

$$\beta(V) \leq \dim V \ \operatorname{lcm}(1, 2, \dots, \sigma(V)).$$

Example. For the binary forms of degree d one gets

$$\sigma(V_d) \leq \frac{2^7}{3^2} d(d+1)^6$$

and so the upper bound for $\beta(V_d)$ will be worse than $(d^6)!$. Compare this with the result of Jordan in §2.

5 Noether's bounds for finite groups

The situation for finite groups is much better. Already in 1916 Emmy Noether proved the following result [Noe16].

Theorem 5.1 — *For a finite groups G we have $\beta(V) \leq |G|$ for every G-module V, i.e., invariants are generated in degree $\leq |G|$.*

Proof. As before define the Reynolds operator $R\colon \mathcal{O}(V) \to \mathcal{O}(V)^G$ by

$$Rf := \frac{1}{|G|} \sum_{g \in G} g \cdot f.$$

It is well-known that the vector space $\mathcal{O}(V)_e$ of homogeneous polynomials of degree e is linearly spanned by the eth powers $(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n)^e$ of linear forms, $\alpha_1, \alpha_2, \dots, \alpha_n \in k$. In fact, this span is a $\mathrm{GL}(V)$-submodule of $\mathcal{O}(V)_e$ which is a simple module. So, the vector space $\mathcal{O}(V)_e^G$ is spanned by the invariants

$$R(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n)^e \quad \text{where } \alpha_1, \alpha_2, \dots, \alpha_n \in k.$$

Suppose $G = \{g_1, g_2, \ldots, g_d\}$ where $d := |G|$ and define

$$y_i := g_i \cdot (\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n),\ i = 1, \ldots, d.$$

Then

$$R(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n)^e = \tfrac{1}{d}(y_1^e + y_2^e + \cdots + y_d^e) =: P_e.$$

Now we use the fact that every such "power sum" P_e for $e > d$ can be expressed as a polynomial in the power sums $P_1, P_2, \ldots, P_d$, because $P_1, P_2, \ldots, P_d$ generate the algebra of symmetric polynomials in $k[y_1, y_2, \ldots, y_d]$. Therefore, every invariant of degree $> d$ is a polynomial in the invariants of degree $\leq d$. □

In view of this result we define $\beta(G)$ for a finite group G as the maximum of all $\beta(V)$:

$$\beta(G) := \max\{\beta(V) \mid V \text{ a representation of } G\}.$$

We have $\beta(G) \leq |G|$ by Noether's theorem, but this bound is not always sharp. For example, it is easy to see that $\beta(\mathbb{Z}/2 \times \mathbb{Z}/2) = 3$. In fact, Barbara Schmid showed that equality only occurs when G is a cyclic group ([Sch89, Sch91]). For commutative finite groups she proved the following result.

Proposition 5.2 — *If G is a commutative finite group then $\beta(G)$ equals the maximal number ℓ such that there exists an equation $g_1 + g_2 + \cdots + g_\ell = 0$ where $g_i \in G$ with the property that for every strict subset $\{i_1, i_2, \ldots, i_s\} \subsetneqq \{1, 2, \ldots, \ell\}$ we have $g_{i_1} + g_{i_2} + \cdots + g_{i_s} \neq 0$.*

Schmid was able to calculate the β invariant for several "small" groups. In general, this seems to be a very difficult problem.

Examples 1. The following examples can be found in [Sch89, Sch91]:

1. $\beta((\mathbb{Z}/2)^N) = N + 1$.
2. If p is a prime and $G = \mathbb{Z}/p^{r_1} \times \mathbb{Z}/p^{r_2} \times \cdots \times \mathbb{Z}/p^{r_s}$ we get $\beta(G) = \sum_{i=1}^{s} p^{r_i} - s + 1$.
3. If G is the dihedral group D_n of order $2n$ then $\beta(D_n) = n + 1$.
4. $\beta(S_3) = 4$, $\beta(A_4) = 6$, $\beta(S_4) \leq 12$.

Remark. It was pointed out to us by Nolan Wallach that one can show that

$$\beta(S_n) \geq e^{C\sqrt{n \ln n}} \quad \text{for } n \gg 0 \quad \text{where } 1 > C > 0$$

by using large cyclic subgroups of the symmetric group S_n (see [Mil87]). Thus we cannot expect any polynomial bound for $\beta(S_n)$.

6 The case of tori

In this section we assume that $G = T$ is a torus of rank r, acting faithfully on an n-dimensional vector space V with weights $\omega_1, \omega_2, \ldots, \omega_n$. The character group $X^\star(T)$ of T is isomorphic to $\mathbb{Z}^r$ and has a natural embedding into $X^\star(T) \otimes_{\mathbb{Z}} \mathbb{R}$. Choosing an isomorphism $X^*(T) \xrightarrow{\sim} \mathbb{Z}^r$ we obtain an isomorphism $X^\star(T) \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\sim} \mathbb{R}^r$ and therefore a volume form dV on $X^\star(T) \otimes_{\mathbb{Z}} \mathbb{R}$ which is independent of the chosen basis of $X^*(T)$.

We can identify the set of monomials in $x_1, x_2, \ldots, x_n$ with $\mathbb{N}^n$. It is clear that the invariant monomials correspond to those $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$ which satisfy

$$\alpha_1\omega_1 + \alpha_2\omega_2 + \cdots + \alpha_n\omega_n = 0.$$

Now we are ready to state and prove the following result due to David Wehlau [Weh93].

Theorem 6.1 **—** *In the situation above we have*

$$\beta(V) \leq (n-r)r! \operatorname{vol}(\mathscr{C}_V)$$

where $\mathscr{C}_V$ is the convex hull of $\omega_1, \omega_2, \ldots, \omega_n$ in $\mathbb{R}^r$.

Proof. Denote by S the set of invariant monomials (as a subset of $\mathbb{N}^n$). The subcone $\mathbb{Q}_+S \subseteq \mathbb{Q}_+^n$ has finitely many extremal rays $\ell_1, \ell_2, \ldots, \ell_s$, and $\ell_i \cap \mathbb{N}^n = \mathbb{N}\, R_i$ for some unique monomial R_i. Suppose M is some invariant monomial. The dimension of $\mathbb{Q}_+S$ is $n-r$, so M lies in some $(n-r)$-dimensional simplicial cone with extremal rays $\ell_{j_1}, \ell_{j_2}, \ldots, \ell_{j_{n-r}}$ for certain indices $j_1, j_2, \ldots, j_{n-r}$. So

$$M = \alpha_1 R_{j_1} + \alpha_2 R_{j_2} + \cdots + \alpha_{n-r} R_{j_{n-r}}, \qquad \alpha_1, \alpha_2, \ldots, \alpha_{n-r} \in \mathbb{Q}_+.$$

Write $\alpha_j = a_j + \gamma_j$ where $a_j \in \mathbb{N}$ and $0 \leq \gamma_j < 1$. In multiplicative notation we get

$$M = R_{j_1}^{a_1} R_{j_2}^{a_2} \ldots R_{j_{n-r}}^{a_{n-r}} N$$

where the degree of N satisfies

$$\begin{aligned} \deg(N) &= \gamma_1 \deg(R_{j_1}) + \gamma_2 \deg(R_{j_2}) + \cdots + \gamma_{n-r} \deg(R_{j_{n-r}}) \\ &\leq (n-r) \max\{\deg(R_i) \mid i = 1, 2, \ldots, s\}. \end{aligned}$$

Now we want to bound $\deg(R_i)$. After a permutation of the variables we may assume that $R_i = (\mu_1, \mu_2, \ldots, \mu_t, 0, 0, \ldots, 0)$ where $\mu_1, \mu_2, \ldots, \mu_t \in \mathbb{N} \setminus \{0\}$. The characters $\omega_1, \omega_2, \ldots, \omega_t$ span a $(t-1)$-dimensional vector space: If it were less then there would be a solution $T = (\tau_1, \tau_2, \ldots, \tau_t, 0, 0, \ldots, 0) \in \mathbb{Q}^n$ independent of R_i, and $R_i \pm \varepsilon T \in \mathbb{Q}_+S$ for small ε contradicting the extremality of the ray ℓ_i. After another permutation of $x_{t+1}, x_{t+2}, \dots, x_n$ we may assume that $\omega_1, \omega_2, \omega_3, \dots, \omega_{r+1}$ span an r-dimensional vector space. The equations

$$\alpha_1\omega_1 + \alpha_2\omega_2 + \cdots + \alpha_{r+1}\omega_{r+1} = \alpha_{r+2} = \alpha_{r+3} = \cdots = \alpha_n = 0$$

have a one-dimensional solution space. By Cramer's rule, we can find a non-zero solution $A = (\alpha_1, \alpha_2, \dots, \alpha_{r+1}, 0, \dots, 0)$ in the usual way:

$$\begin{aligned}\alpha_i &= (-1)^i \det(\omega_1, \omega_2, \dots, \omega_{i-1}, \omega_{i+1}, \dots, \omega_{r+1}) \\ &= \pm r! \operatorname{vol}(\mathscr{C}(0, \omega_1, \omega_2, \dots, \omega_{i-1}, \omega_{i+1}, \dots, \omega_{r+1})) \qquad i = 1, 2, \dots, r+1.\end{aligned}$$

Now A is a rational (even an integral) multiple of R_i. Therefore

$$\begin{aligned}\deg(R_i) \le |\alpha_1| + |\alpha_2| + \cdots + |\alpha_{r+1}| &= r! \sum_{i=1}^{r+1} \operatorname{vol}(\mathscr{C}(0, \omega_1, \dots, \widehat{\omega}_i, \dots, \omega_{r+1})) \\ &= r! \operatorname{vol}(\mathscr{C}(\omega_1, \omega_2, \dots, \omega_{r+1})) \le r! \operatorname{vol}(\mathscr{C}_V),\end{aligned}$$

and so $\beta(V) \le (n-r) r! \operatorname{vol}(\mathscr{C}_V)$. $\square$

Remark. In his paper Wehlau was able to give a slightly better bound:

$$\beta(V) \le \max\{n - r - 1, 1\}\, r! \operatorname{vol}(\mathscr{C}_V).$$

It is conjectured that one even has the sharp bound $\beta(V) \le r! \operatorname{vol}(\mathscr{C}_V)$.

7 A general bound for reductive groups

The degree bounds for semi-simple groups and for tori which we have seen in §4 and §6 depend on n, the dimension of the vector space. On the other hand, a general theorem of Hermann Weyl states that for a given representation of a reductive group G on V the invariants of many copies of V are obtained from those of $n = \dim V$ copies by *polarization* (see [We46]). Here polarization means the iterated application of the following procedure: Let f be a homogeneous invariant of degree d and write

$$f(v + tw) = f(v) + t f_1(v, w) + t^2 f_2(v, w) + \cdots + t^d f(w), \quad t \in k.$$

Then the f_i are homogeneous invariants of $V \oplus V$ of bidegree $(d - i, i)$.

In particular, we see that $\beta(V^N) \le \beta(V^{\dim V})$ for all N. More precisely, we have the following result.

Proposition 7.1 — *Let $V_1, V_2, \dots, V_r$ be irreducible representations of a reductive group G. Then the invariants of $W := V_1^{m_1} \oplus V_2^{m_2} \oplus \cdots \oplus V_r^{m_r}$ are obtained from those of*

$$V_1^{\dim V_1} \oplus V_2^{\dim V_2} \oplus \cdots \oplus V_r^{\dim V_r}$$

by polarizing. In particular, $\beta(W) \le \beta(\bigoplus_j V_j^{\dim V_j})$.

The proposition shows that our bound $\beta(V)$ only depends on the irreducible representations occurring in V and not on their multiplicity. For a finite group G it implies that $\beta(G) = \beta(V_{\text{reg}})$ where V_{reg} is the regular representation (cf. §5).

Example. If $G = T$ is a torus then it is obvious that the degrees of a minimal system of generators for the invariants only depend on the weights of V and not on their multiplicity (cf. §6, proof of Theorem 5.1). Since the number of different weights in V is $\leq \#(\mathcal{C}_V \cap \mathbb{Z}^r)$ we obtain from Theorem 6.1

$$\beta(V) \leq (\#(\mathcal{C}_V \cap \mathbb{Z}^r) - r)\, r!\, \operatorname{vol}(\mathcal{C}_V).$$

In her thesis [His96] Hiss was able to improve Popov's bound and to generalize it to arbitrary connected reductive groups, using some ideas of Knop's. In particular, her bounds for $\sigma(V)$ and $\beta(V)$ do not depend on $\dim V$ as indicated by Proposition 7.1 above. Let us first introduce some notation. The vector space V is embedded in $\mathbb{P}(V \oplus \mathbb{C}) = \mathbb{P}^{n+1}$ in the usual way. We define another constant $\delta(V)$ by

$$\delta(V) := \max\{\deg(Gp) \mid p \in V \setminus \mathcal{N}_V\}$$

where $\deg(Gp)$ is the degree of the projective closure $\overline{Gp}$ of the orbit Gp in $\mathbb{P}^{n+1}$. Recall that this degree is given by the number of points in the intersection of Gp with a generic affine subspace of codimension equal to $\dim Gp$. (See the following §8 for some basic facts about the degree of a quasi-projective variety.)

Let $B = TU$ be a Borel subgroup with its usual decomposition into a torus part T and a unipotent part U and let $\mathfrak{u}$ be the Lie-algebra of U. We define the *nilpotency degree* N_V of the representation V as

$$N_V := \min\{\ell \mid X^{\ell+1}v = 0 \text{ for all } v \in V,\ X \in \mathfrak{u}\}.$$

Finally, we denote by $\mathcal{C}_V$ the convex hull of the weights of the action of the maximal torus T on V (cf. §6). The following result is due to Karin Hiss [His96].

Theorem 7.2 — *Let G be a connected reductive group of dimension m and rank r and let V be a representation of G. Then*

$$\sigma(V) \leq \delta(V) \leq c(G)\, N_V^{m-r} \operatorname{vol}(\mathcal{C}_V) \quad \textit{where} \quad c(G) := \frac{2^r (m+1)!\, r!}{(\frac{m-r}{2})!^2}.$$

Sketch of Proof. If $p \notin \mathcal{N}_V$, then 0 cannot lie in the closure of Gp. For a generic linear subspace W of codimension $\dim Gp - 1$ the projection $\psi\colon V \to V/W$ has the following properties:

1. $\psi(\overline{Gp})$ is closed and has codimension 1 in V/W;
2. $\psi(\overline{Gp})$ does not contain 0;

3. $\psi|_{\overline{Gp}}$ is a finite and birational morphism onto its image and so $\deg Gp = \deg \psi(Gp)$ (see §8 Proposition 8.3 (1)).

Therefore, there exists a $f \in \mathcal{O}(V/W)$ of degree $d = \deg Gp$ vanishing on $\psi(\overline{Gp})$ and satisfying $f(0) = 1$. Now $h := f \circ \psi \in \mathcal{O}(V)$ has degree d, $h(0) = 1$ and h vanishes on Gp. Applying the Reynolds operator we obtain an invariant Rh of degree $\leq d$ satisfying $Rh(0) = 1$ and $Rh(p) = 0$. It follows that one of the homogeneous parts h_i of Rh of degree > 0 must satisfy $h_i(p) \neq 0$. So for every $p \in V \setminus \mathcal{N}_V$ there exists a homogeneous invariant of degree $\leq d$ which does not vanish in p. Hence, $\sigma(V) \leq d \leq \delta(V)$.

Now we want to find a bound for $\delta(V)$. For simplicity we assume that the stabilizer of p is trivial. Let $\mathfrak{u}^-$ be the nilpotent subalgebra opposite to $\mathfrak{u}$. We define a morphism $\varphi\colon \mathfrak{u}^- \times T \times \mathfrak{u} \to V/W$ by

$$\varphi(u^-, t, u) = (\exp(u^-)\, t\, \exp(u)) \cdot p + W.$$

The image of φ is a dense subset of $\psi(Gp)$. The map φ is of degree $\leq N_V$ in u^- and u and the weights appearing are contained in $\mathcal{C}_V$. Therefore,

$$\varphi^\star(\mathcal{O}(V/W)_{\leq \ell}) \subseteq \mathcal{O}(\mathfrak{u}^-)_{\leq \ell N_V} \otimes \mathcal{O}(T)_{\ell \mathcal{C}_V} \otimes \mathcal{O}(\mathfrak{u})_{\leq \ell N_V}$$

with obvious notation. Increasing ℓ we eventually find an ℓ_0 such that

$$(*) \qquad \dim \mathcal{O}(V/W_{\leq \ell_0}) > \dim(\mathcal{O}(\mathfrak{u}^-)_{\leq \ell_0 N_V} \otimes \mathcal{O}(T)_{\ell_0 \mathcal{C}_V} \otimes \mathcal{O}(\mathfrak{u})_{\leq \ell_0 N_V})$$

because $\dim V/W = m + 1 > m = \dim(\mathfrak{u}^- \times T \times \mathfrak{u})$. For such an ℓ_0 there exists a non-zero $f \in \ker(\varphi^\star)$ with degree $\leq \ell_0$. Hence, the hypersurface $\psi(\overline{Gp})$ has degree $\leq \ell_0$ and so $\delta(V) \leq \ell_0$. It remains to determine an ℓ_0 satisfying $(*)$. This eventually leads to the formula given in the theorem. □

To illustrate the last argument in the proof consider the parametrization of the cusp $\varphi\colon k \to k^2$, $t \mapsto (t^2, t^3)$. The homomorphism $\varphi^\star\colon \mathcal{O}(k^2) = k[x, y] \to \mathcal{O}(k) = k[t]$ is defined by $\varphi^\star(x) = t^2$ and $\varphi^\star(y) = t^3$. The image of a polynomial in x and y of degree $\leq \ell$ will be a polynomial in t of degree $\leq 3\ell$ and so $\varphi^\star(k[x, y]_{\leq \ell}) \subseteq k[t]_{\leq 3\ell}$. Now we have $\dim(k[x, y]_{\leq \ell}) = \binom{\ell+2}{2}$ and $\dim(k[t]_{\leq 3\ell}) = 3\ell + 1$. The smallest value of ℓ with $\binom{\ell+2}{2} > 3\ell + 1$ is 4. Therefore, there must exist an f of degree ≤ 4 which vanishes on the cusp. (Of course, there is even a polynomial of degree 3 doing the same, namely $x^3 - y^2$.)

Example. For binary forms of degree d we get

$$\sigma(V_d) \leq \delta(V_d) \leq 96\, d^3.$$

That is a very good estimate (cf. §4 Example). In fact, Lucy Moser-Jauslin [Mos92] has computed the degree of any orbit in V_d:

$$\delta(V_d) \geq \text{degree of a generic orbit } = \begin{cases} d(d-1)(d-2), & d \geq 6 \text{ even}, \\ 2d(d-1)(d-2), & d \geq 5 \text{ odd}. \end{cases}$$

It should be pointed out that the degree of a generic orbit in $\mathbb{P}(V_d)$ was already given by Enriques and Fano (see loc. cit. Remark in section 8).

8 Degrees of orbits in representation spaces

It was pointed out by Vladimir Popov that the degree $\delta(V)$ of a generic orbit in a representation space V might be an interesting "invariant" for that representation. In the previous section we showed that it playes an important rôle in the study of upper bounds for the degrees of a generating set for the ring of invariants $\mathcal{O}(V)^G$. In fact, for every closed orbit Gv different from 0 there is a (non-constant) homogeneous invariant function of degree $\leq \delta(V)$ which does not vanish in v.

Before discussing a general degree formula found by Kazarnovskii we want to recall a few facts about degrees of quasi-projective varieties. For more details we refer to [Ful84].

***Definition 8.1* —** *The degree of a quasi-projective variety $X \subset \mathbb{P}^n$ of dimension d is defined to be the degree of the closure $\overline{X}$ in $\mathbb{P}^n$, i.e.,*

$$\deg X := \# \overline{X} \cap H_1 \cap H_2 \cap \ldots \cap H_d$$

where $H_1, H_2, \ldots, H_d$ are d hyperplanes in $\mathbb{P}^n$ in general position.

In this definition we use the fact that the number of points in the intersection $\overline{X} \cap H_1 \cap H_2 \cap \ldots \cap H_d$ is independent of the choice of the hyperplanes H_i if they are chosen general enough. (One can show that the cardinality of the intersection equals the degree if the intersection is transversal.) Clearly, for a quasi-affine variety $X \subset \mathbb{C}^n$ we have

$$\deg X = \# X \cap A$$

where A is an affine subspace of $\mathbb{C}^n$ of dimension $n-d$ in general position.

The next lemma is well-known. It says that the degree of a projective variety is equal to the *multiplicity* of its homogeneous coordinate ring.

***Lemma 8.2* —** *Let $Z \subset \mathbb{P}^n$ be a projective variety of dimension d and let $R = \bigoplus_{i \geq 0} R_i$ be its homogeneous coordinate ring. Then*

$$\deg Z = \operatorname{mult} R := d! \lim_{i \to \infty} \frac{\dim R_i}{i^d}.$$

For an affine variety $X \subset \mathbb{C}^n$ the coordinate ring $\mathcal{O}(X)$ has a natural filtration given by the subspaces $\mathcal{O}(X)_{\leq i}$ of functions f which are restrictions of polynomials of degree $\leq i$. It follows from Lemma 8.2 that

$$\deg X = d! \lim_{i \to \infty} \frac{\dim \mathcal{O}(X)_{\leq i}}{i^d}, \quad d := \dim X.$$

In fact, the homogeneous coordinate ring R of the closure of X in $\mathbb{P}^n$ is given by $R = \bigoplus_{i \geq 0} \mathcal{O}(X)_{\leq i}\, t^i \subset R[t]$.

Another consequence of Lemma 8.2 is the following result which describes the behavior of the degree under finite morphisms. The first statement was used in the proof of Theorem 7.2 in §7.

Proposition 8.3 — *Let $\psi \colon \mathbb{C}^n \to \mathbb{C}^m$ be a linear map and let $\varphi \colon \mathbb{P}^n \setminus \mathbb{P}(W) \to \mathbb{P}^m$ be the projection from a subspace $\mathbb{P}(W)$.*

(1) *If $X \subset \mathbb{C}^n$ is a closed irreducible subvariety such that $\psi|_X \colon X \to \psi(X)$ is a finite morphism then*

$$\deg X = \deg \psi|_X \cdot \deg \psi(X).$$

(2) *If $Y \subset \mathbb{P}^n$ is an irreducible projective variety such that $Y \cap \mathbb{P}(W) = \emptyset$ then $\varphi|_Y : Y \to \varphi(Y)$ is a finite morphism and*

$$\deg Y = \deg \varphi|_Y \cdot \deg \varphi(Y).$$

As usual, the degree of a dominant morphism is defined to be the degree of the field extension of the corresponding fields of rational functions. It equals the number of points in a general fiber (see [Kra85, Anhang I.3.5]).

Sketch of Proof. It is easy to see that (1) follows from (2). Moreover, statement (2) is a consequence of Lemma 8.2 and the following claim:

Claim. *Let $R = \bigoplus_{i \geq 0} R_i$ be a graded domain where $\dim R_i < \infty$ and $R_0 = \mathbb{C}$, and let $S = \bigoplus_{i \geq 0} S_i \subset R$ be a graded subalgebra. Assume that both are generated by their elements in degree 1 and that R is a finite S-module. Then*

$$\operatorname{mult} R = [\operatorname{Quot}(R) : \operatorname{Quot}(S)] \cdot \operatorname{mult} S.$$

To see this let $R = \sum_{j=1}^N S f_j$ with homogeneous elements $f_j \in R$. Then $\operatorname{Quot}(R) = \sum_{j=1}^N \operatorname{Quot}(S) f_j$ and we can assume that the first $d := [\operatorname{Quot}(R) : \operatorname{Quot}(S)]$ elements form a basis. It follows that $R \supset \bigoplus_{j=1}^d S f_j$ and that there is a homogeneous $f \in S$ such that $fR \subset \bigoplus_{j=1}^d S f_j$. From this the claim follows immediately. $\square$

Example. To any subvariety $X \subset V = \mathbb{C}^n$ we can associate two projective varieties, namely its closure $\overline{X}$ in $\mathbb{P}^n = \mathbb{P}(V \oplus \mathbb{C})$ and the closure $\overline{\pi(X)}$ of the image of X in $\mathbb{P}(V)$. Assume that X is irreducible and that the closure of X in V is not a cone (i.e., X and $\overline{\pi(X)}$ have the same dimension). Then

$$\deg X = \deg \overline{X} = d \cdot \deg \overline{\pi(X)}$$

where $d = \#\, \mathbb{C}x \cap X$ for a general $x \in X$. This follows from Proposition 8.3 (2) applied to the projection $\mathbb{P}(V \oplus \mathbb{C}) \setminus \{P\} \to \mathbb{P}(V)$ from the point $P = (0, 1)$.

In particular, if $\rho\colon G \to \mathrm{GL}(V)$ is a representation and $Gv \subset V$ a non-conical orbit then

$$\deg Gv = (G_{\bar{v}} : G_v) \deg G\bar{v}$$

where $\bar{v}$ is the image of v in $\mathbb{P}(V)$.

9 Kazarnovskii's degree formula

A general formula for the degree of a generic orbit in V^n, $n := \dim V$, for an arbitrary representation V of a connected reductive group G was obtained by Kazarnovskii in the paper [Kaz87]. We will give a short proof of his formula which was suggested by the referee and which completes a partial result obtained by the first author. Moreover, we will use the formula to deduce another upper bound for $\delta(V)$.

First we need some notation. As before, we put $m := \dim G$ and $r := \operatorname{rank} G$. Moreover, we fix a Borel subgroup B and a maximal torus $T \subset B$ and denote by $\alpha_1, \alpha_2, \ldots, \alpha_\ell$, $\ell := \frac{m-r}{2}$, the positive roots. Let 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 W.

For any representation $\rho\colon G \to \mathrm{GL}(V)$ we denote by $\mathscr{C}_V \subset E := X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}$ the convex hull of 0 and the weights of V. On E we use the volume form dV given by any isomorphism $E \simeq \mathbb{R}^r$ which identifies $X^*(T)$ with $\mathbb{Z}^r$. Finally, we fix a W-invariant scalar product $(\ ,\ )$ on E and denote, for any $\gamma \in E$, by $\check{\gamma} \in E^*$ the dual element defined by $\check{\gamma}(\alpha) := \frac{2(\alpha,\gamma)}{(\gamma,\gamma)}$.

Now the result of Kazarnovskii can be stated as follows.

Theorem 9.1 — *Let $\rho\colon G \to \mathrm{GL}(V)$ be a representation of dimension n with finite kernel. Then the degree of a generic orbit in $V^n := \underbrace{V \oplus V \oplus \cdots \oplus V}_{n \text{ copies}}$ is equal to*

$$\delta_{gen}(V) = \frac{m!}{|W|(e_1!e_2!\cdots e_r!)^2}\ \frac{1}{|\ker(\rho)|} \int_{\mathscr{C}_V} (\check{\alpha}_1\check{\alpha}_2 \ldots \check{\alpha}_\ell)^2 dV.$$

Proof. It is clear from the formula that we can replace G by its image $\rho(G)$ in $\mathrm{GL}(V)$ and therefore assume that the representation ρ is faithful. By definition, $\delta_{\mathrm{gen}}(V)$ is the degree of the closure $\overline{G}$ of G in $\mathbb{P}(\mathrm{End}(V)\oplus\mathbb{C})$. Let X be the closure of the cone spanned by G in $\mathrm{End}(V\oplus\mathbb{C})$ where $\mathbb{C}$ is considered as the trivial representation of G:

$$X := \overline{\mathbb{C}^*G} \subset \mathrm{End}(V)\oplus\mathbb{C} \subset \mathrm{End}(V\oplus\mathbb{C}).$$

Clearly, the (graded) algebra $\mathcal{O}(X)$ is the homogeneous coordinate ring of $\overline{G} \subset \mathbb{P}(\mathrm{End}(V)\oplus\mathbb{C})$. Denote by $R=\bigoplus_{j\geq 0} R_j$ the normalization of $\mathcal{O}(X)$ in its field of fractions. Then

$$\delta_{\mathrm{gen}}(V) = m!\lim_{j\to\infty}\frac{\dim\mathcal{O}(X)_j}{j^m} = m!\lim_{j\to\infty}\frac{\dim R_j}{j^m}.$$

(For the second equality see the claim in the proof of Proposition 8.3 of §8.)

Claim. *A simple module V_λ of highest weight λ appears in the homogeneous component R_j if and only if $\lambda\in -j\mathcal{C}_V\cap P\cap X^*(T)$ where P denotes the fundamental Weyl chamber. Moreover, the multiplicity of V_λ is* $\dim V_\lambda$.

The claim implies our theorem as follows. First recall Weyl's character formula (cf. [Hum72, IV.24.3]):

$$\dim V_\lambda = \frac{\prod_{i=1}^{\ell}\check{\alpha}_i(\lambda+\rho)}{\prod_{i=1}^{\ell}\check{\alpha}_i(\rho)} \qquad \text{where } \rho := \tfrac{1}{2}\textstyle\sum_{i=1}^{\ell}\alpha_i.$$

It follows that

$$\begin{aligned}\frac{\dim R_j}{j^m} &= \frac{1}{j^m\prod_{i=1}^{\ell}\check{\alpha}_i(\rho)^2}\sum_{\lambda\in -j\mathcal{C}_V\cap P\cap X^*(T)}\prod_{i=1}^{\ell}\check{\alpha}_i(\lambda+\rho)^2\\ &= \frac{1}{j^r\prod_{i=1}^{\ell}\check{\alpha}_i(\rho)^2}\sum_{\mu\in -\mathcal{C}_V\cap P\cap\frac{1}{j}X^*(T)}\prod_{i=1}^{\ell}\check{\alpha}_i(\mu+\frac{\rho}{j})^2.\end{aligned}$$

Passing to the limit $j\to\infty$ we obtain

$$\frac{\delta_{\mathrm{gen}}(V)}{m!} = \frac{1}{\prod_{i=1}^{\ell}\check{\alpha}_i(\rho)^2}\int_{-\mathcal{C}_V\cap P}(\check{\alpha}_1\check{\alpha}_2\cdots\check{\alpha}_\ell)^2\,dV$$

Since the function $\check{\alpha}_1\check{\alpha}_2\cdots\check{\alpha}_\ell$ is W-invariant and since the numbers $\check{\alpha}_i(\rho)$ are exactly the numbers $1,2,\ldots,e_1,1,2,\ldots,e_2,\ldots,1,2,\ldots,e_r$ (see [Hum90, 3.20 Theorem]) we finally get

$$\delta_{\mathrm{gen}}(V) = \frac{m!}{|W|\,(e_1!e_2!\cdots e_r!)^2}\int_{\mathcal{C}_V}(\check{\alpha}_1\check{\alpha}_2\cdots\check{\alpha}_\ell)^2\,dV.$$

It remains to prove the claim. The second statement is easy because X and its normalization $\tilde{X}$ are both $G \times G$ varieties and the equivariant morphism $G \to X$ induces an injection $R_j \hookrightarrow \mathcal{O}(G)$ for every j.

For the first statement let $\lambda \in -j\mathcal{C}_V \cap P \cap X^*(T)$ and define Y to be the closure of $\mathbb{C}^*G$ in $\operatorname{End}(V) \oplus \operatorname{End}(V_\lambda^*) \oplus \mathbb{C}$ where this time $\mathbb{C}^*$ acts by $t(\varphi, \psi, z) := (t\varphi, t^j\psi, tz)$:

$$Y := \overline{\mathbb{C}^*G} \subset \operatorname{End}(V) \oplus \operatorname{End}(V_\lambda^*) \oplus \mathbb{C}.$$

It follows that $\operatorname{End}(V_\lambda)$ occurs in $\mathcal{O}(Y)$ in degree j where the grading is given by the $\mathbb{C}^*$-action defined above. Moreover, the linear projection $\operatorname{End}(V) \oplus \operatorname{End}(V_\lambda^*) \oplus \mathbb{C} \to \operatorname{End}(V) \oplus \mathbb{C}$ induces a homogeneous morphism $p\colon Y \to X$ which is the identity on $\mathbb{C}^*G$. Thus, p is birational and it remains to show that p is finite, i.e., that $p^{-1}(0) = \{0\}$. Let $(0, \psi, 0) \in p^{-1}(0) \subset Y$. By the following Lemma 9.2 there is a one-parameter subgroup $t \mapsto (t^a, \sigma(t))$ of $\mathbb{C}^* \times G$ such that

$$\lim_{t \to 0}(t^a \rho(\sigma(t)), t^{aj} \rho_\lambda^*(\sigma(t)), t^a) = (0, \psi, 0).$$

It follows that $a > 0$ and that $a + (\sigma, \mu) > 0$ for all weights μ of V and therefore for all $\mu \in \mathcal{C}_V$. Hence, $ja + (\sigma, \nu) > 0$ for all $\nu \in j\mathcal{C}_V$ and so $\psi = \lim_{t \to 0} t^{ja} \rho_\lambda^*(\sigma(t)) = 0$ because all weights of V_λ^* are contained in $j\mathcal{C}_V$, by assumption.

□

The following lemma was used in the proof above. It is essentially due to Strickland (see [Str87]) and was communicated to us by DeConcini.

Lemma 9.2 — *Let $\rho\colon G \to \operatorname{GL}(V)$ be a representation of a reductive groups and let $T \subset G$ be a maximal torus. Then the closure $\overline{G}$ in $\operatorname{End} V$ is equal to $G\overline{T}G$.*

The proof follows immediately from the fact that for a reductive group G with maximal torus T we have $G(\mathbb{C}(\!(t)\!)) = G(\mathbb{C}[\![t]\!])\, T(\mathbb{C}(\!(t)\!))\, G(\mathbb{C}[\![t]\!])$ (Theorem of Ivahori; see [MFK94, Chap. 2, §1]).

Finally, we show that the generic degree given by Kazarnovskii's formula is an upper bound for all degrees of G-orbits and in particular for $\delta(V)$.

Proposition 9.3 — *For any representation $\rho\colon G \to \operatorname{GL}(V)$ of a reductive group G and any vector $v \in V$ we have*

$$\deg Gv \leq \delta_{gen}(V) \quad \textit{and} \quad \delta(V) \leq \delta_{gen}(V).$$

Proof. Given a generic $q \in V^n$ and an arbitrary $v \in V$ there exists a G-equivariant linear map $\psi\colon V^n \to V$ satisfying $\psi(q) = p$. Thus, the orbit of q is mapped onto the orbit of p. From this it is not difficult to see that $\delta_{\mathrm{gen}}(V) = \deg Gq \geq \deg Gv$. □

Example. For binary forms of degree d we have $G = \mathrm{SL}_2$, $W \simeq \mathbb{Z}/2$, $e_1 = 1$, $\mathscr{C}_V = [-d, d]$. Therefore,

$$\delta(V_d) \leq \frac{3!}{2} \int_{x=-d}^{d} x^2\, dx = 2d^3 \text{ if } d \text{ is odd} \quad \text{and} \quad \delta(V_d) \leq d^3 \text{ if } d \text{ is even.}$$

This improves the bound found by Hiss (see §7).

10 Algorithms

With the development of computers over the last decades the computational aspects of invariant theory gained importance:

> *How can one explicitly compute generators for the invariant ring? Are there finite algorithms and what is their complexity?*

We refer to Sturmfels' book [Stu93] for an excellent introduction into the subject and a source of references. Some algorithms are already implemented. For example, Kemper wrote the *invar* package in Maple for finite groups (see [Kem93, Kem95]) and for tori an algorithm to compute invariants is given by Sturmfels in loc. cit.

In the following we describe a new algorithm to compute invariants of arbitrary reductive groups which was discovered by the first author (see [Der97] Chap. I). It is implemented in the computer algebra system *SINGULAR* (see [GPS]). In some sense, it is a generalization of Sturmfels' algorithm.

Consider the morphism $\psi\colon G \times V \to V \times V$ defined by $\psi(g, v) = (v, gv)$ ($g \in G$, $v \in V$) and let $B \subset V \times V$ be the closure of the image of ψ:

$$B := \overline{\{(v, w) \in V \times V \mid Gv = Gw\}}.$$

Let $\mathfrak{b}$ be the homogeneous ideal in $\mathcal{O}(V \times V) = k[x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n]$ defining B. The algorithm is based on the following result:

Proposition 10.1 — *If $h_1(x, y), h_2(x, y), \ldots, h_s(x, y)$ are homogeneous generators of the ideal $\mathfrak{b}$ then*

$$\mathcal{O}(V)^G = k[R(h_1(x, 0)), R(h_2(x, 0)), \ldots, R(h_s(x, 0))]$$

where R is the Reynolds operator.

It is clear that homogeneous generators of $\mathfrak{b}$ can be computed using *Gröbner basis techniques.* Thus, the proposition gives us an algorithmic way to compute generators for the invariant ring. In case of a torus the algorithm is essentially the same as the one given by Sturmfels.

The proposition above also has some interesting theoretical consequences. In fact, it gives us a way to obtain an upper bound for $\beta(V)$. If $\mathfrak{b}$ is generated by homogeneous polynomials of degree $\leq d$ then, by Proposition 10.1, $\beta(V) \leq d$. The variety B is a cone, so we can view it as a projective variety in $\mathbb{P}(V \times V)$. It can be shown that the degree $\bar{\delta}(B)$ of B as a projective variety in $\mathbb{P}(V \times V)$ is at most the degree of the generic orbit closure in $\mathbb{P}(\wedge^n(V \times V))$ where G acts only on the second factor. Using the formula of Kazarnovskii one finds

$$\bar{\delta}(B) \leq \min(\, C(nL)^m, C' L^{m^2+m}\,)$$

where C, C' are positive constants, $n := \dim V$, $m := \dim G$ and L is the maximal euclidean length of all weights appearing in V. On the other hand, Eisenbud and Goto made the following conjecture [EiG84]:

Conjecture — *If B is connected (i.e., if G is connected) then the ideal $\mathfrak{b}$ is generated by homogeneous polynomials of degree $\leq \bar{\delta}(B)$.*

In fact, their conjecture is stronger and involves also higher syzygies; it can be translated into terms of local cohomology. Clearly, the conjecture implies that $\beta(V) \leq \bar{\delta}(B)$ which together with the upper bounds for $\bar{\delta}(B)$ would be a considerable improvement of the bounds found by Popov and Hiss.

Note added in Proof: The first author has recently shown that

$$\beta(V) \leq \max\left\{\frac{3}{8} s\sigma(V)^2, \sigma(V)\right\}$$

where $s = \dim \mathcal{O}(V)^G$ (see Derksen, H.: *Polynomial bounds for rings of invariants*, to appear). This is a considerable improvement of all degree bounds obtained so far, except for those of Jordan: For binary forms of degree d it gives $\beta(V_d) \leq \frac{3}{2} d^7$.

References

[Der97] H. Derksen, *Constructive Invariant Theory and the Linearization Problem*, Dissertation Basel, 1997

[EiG84] D. Eisenbud and S. Goto, *Linear free resolutions and minimal multiplicity*, J. of Algebra **88**, 1984, 89–133

[Ful84] W. Fulton, *Intersection Theory*, Ergebn. Math. und Grenzgebiete, 3. Folge **2**, Springer Verlag, Berlin-Heidelberg-New York, 1984

[Gor68] P. Gordan, *Beweis dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist*, J. reine u. angew. Math. **69**, 1868, 323–354

[GrY03] J. H. Grace and A. Young, *The Algebra of Invariants*, 1903, Chelsea Publishing Company, New York (Reprint)

[GPS] G.-M. Greuel, G. Pfister, H. Schönemann, *SINGULAR, A Computer Algebra System for Singularity Theory, Algebraic Geometry and Commutative Algebra*, available via ftp from `ftp://www.mathematik.uni-kl.de/pub/Math/Singular`

[Hil90] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36**, 1890, 473–534

[Hil93] ———, *Über die vollen Invariantensysteme*, Math. Ann. **42**, 1893, 313–373

[Hil01] ———, *Mathematische Probleme*, Archiv für Math. und Physik **1**, 1901, 44–63, 213–237; Gesammelte Abhandlungen Band III, 290–329, Springer Verlag, Berlin-Heidelberg-New York, 1970

[His96] K. Hiss, *Constructive invariant theory for reductive algebraic groups*, Thesis Brandeis University, Waltham, 1996

[HoR74] M. Hochster and J. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Adv. Math. **13**, 1974, 115–175

[Hum72] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Text in Math. **9**, Springer Verlag, New York-Heidelberg-Berlin, 1972

[Hum90] ———, *Reflection Groups and Coxeter Groups*, Cambridge Studies in Advanced Mathematics **29**, Cambridge University Press, Cambridge-New York-Port Chester-Melbourne-Sydney, 1990

[Jor76] C. Jordan, *Mémoire sur les covariants des formes binaires*, J. de Math. **3** (2), 1876, 177–232

[Jor79] ———, *Sur les covariants des formes binaires*, J. de Math. **3** (5), 1879, 345–378

[Kaz87] B. Ya. 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

[Kem93] G. Kemper, *The Invar package for calculating rings of invariants*, Preprintreihe IWR **93**-34, Universität Heidelberg, 1993

[Kem95] ———, *Calculating invariant rings of finite groups over arbitrary fields*, Preprintreihe IWR **95**-12, Universität Heidelberg, 1995

[Kno89] F. Knop, *Der kanonische Modul eines Invariantenringes*, J. Algebra **127**, 1989, 40–54

[Kra85] H. Kraft, *Geometrische Methoden in der Invariantentheorie*, Aspekte der Mathematik **D1**, Vieweg Verlag, Braunschweig-Wiesbaden, 2., durchgesehene Auflage, 1985

[Mey99] F. Meyer, *Invariantentheorie*, Encyklopädie der math. Wissenschaften, 1899, 320–403

[Mil87] W. Miller, *The maximum order of an element of a finite symmetric group*, Math. Monthly **94**, 1987, 497–506

[Min73] H. Minkowski, *Briefe an David Hilbert mit Beiträgen und herausgegeben von L. Rüdenberg und H. Zassenhaus*, Springer Verlag, Berlin-Heidelberg-New York, 1973

[Mos92] L. Moser-Jauslin, *The Chow rings of smooth complete* SL_2*-embeddings*, Compositio Math. **82**, 1992, 67–106

[MFK94] D. Mumford, J. Fogarty and F. Kirwan, *Geometric Invariant Theory*, Ergebnisse der Mathematik und Grenzgebiete **34**, Springer-Verlag, New York-Heidelberg-Berlin, 3rd edition, 1994

[Nag59] M. Nagata, *On the 14th problem of Hilbert*, Amer. J. Math. **81**, 1959, 766–772

[New78] P. E. Newstead, *Introduction to Moduli Problems and Orbit Spaces*, published for the Tata Institute of Fundamental Research, Bombay, Springer Verlag, Berlin-Heidelberg-New York, 1978

[Noe16] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77**, 1916, 89–92

[Pop81] V. Popov, *Constructive invariant theory*, Astérique **87**–**88**, 1981, 303–334

[Pop82] ———, *The constructive theory of invariants*, Math. USSR Izvest. **19**, 1982, 359–376

[Sch89] B. Schmid, *Generating invariants of finite groups*, C. R. Acad. Sci. Paris **308**, Série I, 1989, 1–6

[Sch91] ———, *Finite groups and invariant theory*, Séminaire d'Algèbre Paul Dubreil et M.-P. Malliavin, Lecture Notes in Math. **1478**, pp. 35–66, Springer Verlag, Berlin-Heidelberg-New York, 1991

[Schu68] I. Schur, *Vorlesungen über Invariantentheorie*, Grundlehren Math. Wiss. **143**, bearbeitet und herausgegeben von H. Grunsky, Springer-Verlag, New York-Heidelberg-Berlin, 1968

[Spr89] T. A. Springer, *Aktionen reduktiver Gruppen auf Varietäten*, Algebraische Transformationsgruppen und Invariantentheorie, edited by H. Kraft, P. Slodowy, T. A. Springer, DMV-Seminar Notes **13**, Birkhäuser Verlag, Basel-Boston, 1989

[Str87] E. Strickland, *A vanishing theorem for group compactifications*, Math. Ann. **277**, 1987, 165–171

[Stu93] B. Sturmfels, *Algorithms in Invariant Theory*, Springer Verlag, Berlin-Heidelberg-New York, 1993

[Weh93] D. Wehlau, *Constructive invariant theory for tori*, Ann. Inst. Fourier **43**, 1993, 1055–1066

[Wei32] R. Weitzenböck, *Über die Invarianten von linearen Gruppen*, Acta Math. **58**, 1932, 231–293

[We46] H. Weyl, *The Classical Groups, their Invariants and Representations*, Princeton Mathematical Series **1**, Princeton Univ. Press, Princeton, 1946

[Wey93] J. Weyman, *Gordan ideals in the theory of binary forms*, J. Algebra **161**, 1993, 370–391