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 $\mathbb{C}(V)$ 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 $\mathbb{C}(V)^G$. 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 $\mathbb{C}(V)^G$ finitely generated as a k-algebra?*
- *If so, can one determine an explicit upper bound for the degrees of a system of generators of $\mathbb{C}(V)^G$?*
- *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:

$$\beta(V) := \min\{d \mid \mathbb{C}(V)^G \text{ is generated by invariants of degree} \le d\}.$$

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* $\mathbb{C}(V)^{\mathrm{SL}_2}$ *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 $\mathscr{C}_d(W)$ of a fixed order d form a module over the ring of invariants. In fact, one easily sees that $\mathscr{C}_d(W) = (\mathbb{C}(W) \otimes V_d)^{\mathrm{SL}_2}$ 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 $\mathscr{C}(W) := \bigoplus_d \mathscr{C}_d(W)$ 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, $\mathscr{C}(W)$ is itself a ring of invariants:

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

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 $\ell = (\ell_1, \ell_2, \ldots, \ell_N) \in V_1^N$ as a $2 \times N$-matrix

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

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 $\mathbb{C}(V)$ is completely reducible. Then the invariant ring $\mathbb{C}(V)^G$ 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 $\mathbb{C}(V) = k[x_1, x_2, \ldots, x_n]$ is finitely generated.
   (This is the famous "Basissatz;" it is theorem 1 of Hilbert's paper.)
2. There exits a linear projection $R\colon \mathbb{C}(V) \to \mathbb{C}(V)^G$ which is a $\mathbb{C}(V)^G$-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 $\mathbb{C}(V)$ 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 $\mathbb{C}(V)^G = k[f_1, f_2, \ldots, f_r]$. 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

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

Applying R from (2) yields

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