Some Remarks on the Complexity of Invariant Algebras

Klaus Pommerening
Johannes-Gutenberg-Universität
Mainz, Germany

February 1986 – english version January 2012 – last change October 25, 2016

Introduction

This is the general objective of invariant theory:

> Let a group G operate on a ring A (commutative with 1) as a group of automorphisms. Determine the subring A^G consisting of the fixed points of this action.

In the most interesting cases the ring A is an algebra of functions on a set on which the group G acts. Then the elements of G transform the functions in a natural way, and the fixed points in A are the invariant functions, or shortly, the invariants.

Among these function algebras we single out the most important special case: The set on which the group G acts is a finite-dimensional vector space V over a field k, and the action of G comes from a representation of G on V. As our function algebra we take the k-algebra $\mathcal{O}(V)$ of k-valued polynomial functions on V. If k is infinite, this algebra $\mathcal{O}(V)$ is isomorphic with the polynomial ring $k[X_1, \ldots, X_n]$ in $n = \dim V$ variables in a natural way (after choosing a basis of V).

> If k is finite, then every function $V \longrightarrow k$ is polynomial. There are q^{q^n} of them where $q = \#k$ and $n = \dim V$. Each $X_i^q - X_i$ vanishes on V, and $\mathcal{O}(V) \cong k[X]/(X_1^q - X_1, \ldots, X_n^q - X_n)$. See the discussion in [19].

The invariants are the polynomial functions $f\colon V \longrightarrow k$ that satisfy the functional equation

$$f(g \cdot v) = f(v) \quad \text{for all } g \in G \text{ and } v \in V. \tag{1}$$

This equation expresses the fact that the function is independent of certain external circumstances (for example the choice of a coordinate system), or

that it has certain symmetry properties. In physics conservation laws materialize in this way. Determining the invariant algebra is equivalent with completely solving the functional equation (1). Determining a system of generators of the invariant algebra means finding enough "fundamental" solutions from which all the others emerge by simple algebraic combinations.

In the second half of the 19^{th} century this topic evolved into a huge branch of mathematics: invariant theory. Its exponents invented an immense plenitude of concrete methods for determining invariants. Quite early they also asked the question whether there is always a finite system of generators. This question also lies at the heart of HILBERT's 14^{th} problem. In this generality it is unsolved until today; there are a lot of positve results but also some counterexamples, and there remains a large uncharted territory in between.

As a research topic of central interest invariant theory almost completely died out in the beginning of the 20^{th} century, on the one hand choked by the abundance of single concrete results whose expenses grew into gigantic dimensions, on the other hand paralyzed by the immense difficulty of HILBERT's 14^{th} problem where even the new-fashioned methods of commutative algebra—after some early successes—failed to produce further promising approaches. It was only in the 1950s that a turbulent new expansion of invariant theory began, when it became clear that the then new theory of algebraic groups provided a convenient framework.

The best known positive result holds for the case where G is a reductive group and its representation on V is given by a homomorphism $G \longrightarrow GL(V)$ of algebraic groups. Let us skip the intricate story of this result (and also the definition of the involved concepts), however emphasize that restricting the consideration to algebraic groups is *no* substantial loss of generality, and likewise not the restriction to an algebraically closed ground field. However reductive groups constitute a proper special case.

> Examples for reductive groups are: finite groups, general and special linear groups (GL and SL), orthogonal and symplectic groups, the multiplicative group $\mathbb{G}_m = k^\times$, simple algebraic groups. And more generally: All groups that originate from these examples by finitely many extensions.
>
> Non-reductive groups are: the additive group $\mathbb{G}_a = (k, +)$, groups of upper triangular matrices etc. More generally: All groups that have a normal subgroup isomorphic with $\mathbb{G}_a$.

For non-reductive groups there are only a few sporadic positive results on finite generation of invariants, see [13], and some *counterexamples*, beginning with NAGATA's, see also [5] [22].

From now on let us confine to reductive algebraic groups. Then we have a finitely generated invariant algebra. However the lessons from classical

invariant theory teach us that the task of explicitly finding a system of generators is daunting. Instead we should ask a question that—in a very broad sense—is a topic of theoretical computer science, or more precisely of complexity theory: *How complex is the determination of a system of generators?* More precisely we ask: *How large is a minimal system of generators? Is there any chance to enumerate them all?* As we shall see this leads to some interesting combinatorial problems.

The complexity of an algorithm is the number of single steps leading to the result. (We don't want to bother here with a general exact definition of this concept.)

Now let us consider a representation of a reductive group G on a finite-dimensional vector space V over a field k. What can we say about algorithms that produce a system of generators for the invariant algebra $\mathcal{O}(V)^G$? First of all there is no known general algorithm for this task, only algorithms for special cases. However such a situation is familiar in complexity theory. The complexity of a *problem* is the minimal complexity of all possible algorithms for its solution; and for this we sometimes can get results without even knowing a single algorithm.

In this sense a lower bound for the complexity of determining generators for the algebra $\mathcal{O}(V)^G$ is the minimal size of a system of generators. Because this is the number of steps we need alone for writing down a system of generators.

1 The Embedding Dimension

For a finitely generated k-algebra A the minimal size of a system of generators is called the **embedding dimension** of the algebra:

$$\operatorname{ebd} A = \min\{m \mid A = k[f_1, \ldots, f_m] \text{ where } f_1, \ldots, f_m \in A\}.$$

> By the way the embedding dimension of a finitely generated algebra A is the minimal dimension m of an affine scheme k^m into which the corresponding scheme $\operatorname{spec}(A)$ embeds.

For our algebras of invariants we define

$$e_{G,V} = \operatorname{ebd} \mathcal{O}(V)^G.$$

The algebra $\mathcal{O}(V)$ has a grading by the degree of its polynomials. Because the group G acts by linear transformations it respects the grading. In particular a polynomial is invariant if and only if all of its homogeneous components are invariant. Therefore the invariant algebra is a homogeneous subalgebra, hence itself graded:

$$\mathcal{O}(V)^G = \bigoplus_{j \in \mathbb{N}} \mathcal{O}(V)^G_j$$

where $\mathcal{O}(V)_j = \{\text{homogeneous polynomials of degree} j\} \cup \{0\}$.

Now each graded finitely generated subalgebra R of $\mathcal{O}(V)$—such as $\mathcal{O}(V)^G$—has a finite generating system consisting of homogeneous elements: Simply take the homogeneous parts of any system of generators. However it's not immediately obvious that there always is a generating system of minimal length consisting of homogeneous elements; for this we consider a slightly more general situation:

Proposition 1 *Let k be a field and A be an $\mathbb{N}^l$-graded k-algebra with $A_0 = k$ and let $\mathfrak{m} = \bigoplus_{\nu \neq 0} A_\nu$. Assume $\dim_k \mathfrak{m}/\mathfrak{m}^2 = n$ is finite. Then the minimal cardinality of a set of generators of A is n, and there is a set of* homogeneous *generators of cardinality n. Moreover each minimal set of homogeneous generators contains exactly n elements.*

For a proof see [17].

From this fact we derive the following coarse algorithm for constructing a minimal system of generators for an invariant algebra:

1. After each step of the procedure we have a finite set M consisting of homogeneous polynomials in $\mathcal{O}(V)^G$, starting with $M = \emptyset$, and a current degree d, starting with $d = 1$, such that $\mathcal{O}(V)^G_j = k[M]_j$ for $0 \leq j \leq d-1$.

2. Then in the next step we construct a homogeneous basis of $(\mathcal{O}(V)^G_d \bmod k[M]_d)$ and add its elements to M. Furthermore we increase d by 1.

3. If $k[M] = \mathcal{O}(V)^G$, stop. Otherwise continue with 1.

If $\mathcal{O}(V)^G$ is finitely generated, then this procedure stops after finitely many steps and gives a minimal system of generators for $\mathcal{O}(V)^G$. However the specification of the algorithm is incomplete since it doesn't contain instructions on how to get the basis in 2, and it doesn't say how to check the stop condition in 3. In fact for 2, classical invariant theory mainly used the symbolic method, and 3 was first answered for an interesting special case by Hilbert in [8] who gave a huge upper bound for the degrees of a generating system of SL_n-invariants. For a more actual version see [20].

We have yet to analyze if our minimal system of generators is also of minimal length. This however is easy: Take any minimal system M of homogeneous generators, and consider the set M_d of elements of degree d in M. Induction on d immediately gives that $\mathcal{O}(V)^G_d = k[M_1 \cup \ldots \cup M_d]_d$ for all d. Therefore M_d must be a basis of $\mathcal{O}(V)^G_d \bmod k[M_1 \cup \ldots \cup M_{d-1}]_d$.

In this context there is another measure for the complexity of an invariant algebra, roughly related to the embedding dimension:

$$d_{G,V} := \min\{d \mid \sum_{j=0}^{d} \mathcal{O}(V)^G_d \text{ generates } \mathcal{O}(V)^G\}.$$

This is also the minimal upper bound for the degrees of the elements of a (not of every!) minimal set of homogeneous generators. We have the obvious inequalitites (where $n = \dim V$)

$$e_{G,V} \leq \sum_{j=0}^{d_{G,V}} \dim \mathcal{O}(V)_j^G \leq \sum_{j=0}^{d_{G,V}} \dim \mathcal{O}(V)_j \leq \sum_{j=0}^{d_{G,V}} \binom{n+j-1}{j} = \binom{n+d_{G,V}}{d_{G,V}}.$$

An explicit upper bound for $d_{G,V}$ or for $e_{G,V}$ would immediately provide a stop criterion for the above procedure.

2 Finite Groups

Let the finite group G act linearly on the finite dimensional k-vector space V. Hurwitz already in the 1890s showed that the invariant algebra $\mathcal{O}(V)^G$ is finitely generated if $\operatorname{char} k = 0$ (or at least $\operatorname{char} k \nmid \#G$). The general result (without restrictions on the characteristic) was given by Emmy Noether in 1926 [12]; this however was not constructive. She also in 1916 gave a constructive (although not practically useful) proof [11] for characteristic 0 that gives information about the complexity—the Noether bound. J. Fogarty extended this result to the case $\operatorname{char} k \nmid \#G$, and D. Benson considerably simplified the proof, see [3].

Proposition 2 *Let the finite group G of order $m = \#G$ act linearly on the n-dimensional k-vector space V over the field k with $\operatorname{char} k \nmid m$. Then:*

(i) *The invariant algebra $\mathcal{O}(V)^G$ is generated by finitely many polynomials of degree $\leq m$.*

(ii) $d_{G,V} \leq m$.

(iii) *The embedding dimension of $\mathcal{O}(V)^G$ is $e_{G,V} \leq \binom{n+m}{m}$.*

(iv) $e_{G,V} \geq n$.

Proof. The last statement (iv) follows because $\mathcal{O}(V)$ is an integral ring extension of $\mathcal{O}(V)^G$, hence

$$e_{G,V} \geq \operatorname{trdeg} \mathcal{O}(V)^G = \operatorname{trdeg} \mathcal{O}(V) = n.$$

The statements (ii) and (iii) immediately follow from (i).

For (i) choose a basis of V and identify $\mathcal{O}(V)$ with the polynomial ring $A = k[X_1, \ldots, X_n]$. Let $\mathfrak{m} = A_+ = \bigoplus_{\nu>0} A_\nu$ and $\mathfrak{a} = \mathfrak{m}^G A$ (the Hilbert ideal). By the following Lemma 1 we have

$$A_m = \mathfrak{m}^m \subseteq \mathfrak{a} \cap A_m \subseteq \sum_{w \in W} Aw,$$

where $W \subset \mathfrak{a}$ is a basis of the finite dimensional vector space $\sum_{\nu=1}^{m} \mathfrak{a} \cap A_\nu$. For $d > m$ we have

$$\mathfrak{a} \cap A_d \subseteq A_d = < A_{d-m} A_m > \subseteq \sum_{w \in W} Aw.$$

Hence W generates the ideal $\mathfrak{a}$:

Claim: $A^G = k[W]$. We take an arbitrary homogeneous $f \in A^G$ of degree d and reason by induction over d, the start $d = 0$ being trivial. For $d > 0$ we have $f \in A_+^G \subseteq \mathfrak{a}$, hence we may write $f = \sum a_i w_i$ with $w_i \in W$ and $a_i \in A$. We apply the mean value operator

$$\natural \colon A \longrightarrow A^G, \quad a \mapsto a^\natural = \frac{1}{m} \sum_{g \in G} g \cdot a.$$

It is k-linear, fixes the elements of A^G, and maps $a_i w_i \mapsto a_i^\natural w_i$. Now $a_i^\natural \in A^G$ is of degree $< d$, hence in $k[W]$. $\diamond$

Lemma 1 (Benson**)** *Let A be a commutative ring with 1, $G \leq \operatorname{Aut} A$ be a finite group of order m where m is invertible in A, and $\mathfrak{b}$ be a G-stable ideal of A. Then $\mathfrak{b}^m \subseteq \mathfrak{b}^G A$.*

Proof. We take m arbitrary elements of $\mathfrak{b}$ and index them by the elements of G, forming a family $(f_g)_{g \in G}$. Then for any $h \in G$

$$\prod_{g \in G} (hg \cdot f_g - f_g) = (f_{h^{-1}} - f_{h^{-1}}) \prod_{g \neq h^{-1}} (hg \cdot f_g - f_g) = 0.$$

The lefthand side expands as

$$\sum_{M \subseteq G} \left(\prod_{g \in M} hg \cdot f_g \right) \cdot (-1)^{\#(G-M)} \left(\prod_{g \in G-M} f_g \right).$$

Summing this expression over h yields

$$0 = \sum_{M \subseteq G} \left((-1)^{\#(G-M)} \left[\sum_{h \in G} h(\prod_{g \in M} g \cdot f_g) \right] \prod_{g \in G-M} f_g \right).$$

The summand for $M = \emptyset$ is

$$(-1)^m \cdot \left[\sum_{h \in G} h \cdot 1 \right] \cdot \prod_{g \in G} f_g = (-1)^m \cdot m \cdot \prod_{g \in G} f_g$$

The sumands for $M \neq \emptyset$ are of the form $[\sum_{h \in G} ha] \cdot b$ with $[\sum_{h \in G} ha] \in \mathfrak{b}^G$ and $b \in A$. Therefore $\prod_{g \in G} f_g \in \mathfrak{b}^G A$. $\diamond$

Note that the lower bound for $e_{G,V}$ in (iv) is sharp: The value n is assumed for reflection groups. The upper bound is too pessimistic, we may at least save one dimension since we don't need the constants in a system of generators. But even this bound could be reached only if G acts trivially on all $\mathcal{O}(V)_j$ with $|j| \leq m$. But then $\mathcal{O}(V)^G = \mathcal{O}(V)$, hence $d_{G,V} = 1$ and $e_{G,V} = n$, hence $\#\rho(G) = 1$ where $\rho : G \longrightarrow GL(V)$ denotes the representation. For some more results see [21].

Corollary 1 *Let G be a fixed finite group of order $\#G = m$ and consider an arbitrary representation on a k-vector space V of dimension n. Then*

$$e_{G,V} \leq \frac{1}{m!} \cdot n^m + \mathrm{O}(n^{m-1});$$

in particular $e_{G,V}$ grows polynomially with $\dim V$ (for fixed m).

For the proof simply expand $\binom{m+n}{m}$.

Problem Determine

$$e_{mn} = \max\{e_{G,V} \mid \#G = m,\ \dim V = n,\ G \text{ acts linearly on } V\}.$$

By Proposition 2 we have

$$e_{mn} \leq \binom{m+n}{m}.$$

3 Finite Cyclic Groups

Let k be a field that contains a primitive r-th root of unity, in particular $\operatorname{char} k \nmid r$. Then each representation of the cyclic group $\mathcal{Z}_r$ of order r is diagonalizable: We find a basis such that the corresponding operation on the polynomial ring $k[X] = k[X_1, \ldots, X_n]$ is given by the formula

$$A \cdot X_i = \varepsilon^{a_i} X_i \quad \text{for } i = 1, \ldots, n, \tag{2}$$

with suitable $a_i \in \mathbb{Z}$, $0 \leq a_i \leq r-1$, where A is a fixed generator of the cyclic group $\mathcal{Z}_r$ and ε, a fixed primitive r-th root of unity.

A polynomial $f = \sum_{\nu \in \mathbb{N}^n} c_\nu X^\nu$—with the usual notation $X^\nu = X_1^{\nu_1} \cdots X_n^{\nu_n}$—transforms to

$$A \cdot f = \sum_{\nu \in \mathbb{N}^n} \varepsilon^{(a|\nu)} c_\nu X^\nu,$$

where $(a|\nu) = a_1\nu_1 + \cdots + a_n\nu_n$. Thus f is invariant if and only if it has only monomials with $(a|\nu) \equiv 0 \pmod{r}$. A minimal system of generators of the

invariant algebra therefore consists exactly of the monomials X^ν for which ν is an indecomposable solution of the congruence

$$a_1x_1 + \cdots + a_nx_n \equiv 0 \pmod{r}. \tag{3}$$

By "indecomposable" we understand that $x \neq 0$ and there are no solutions $y, z \in \mathbb{N}^n - \{0\}$ such that $x = y + z$, see [14]. Note that $X^\lambda X^\nu = X^{\lambda+\nu}$. This consideration shows:

Proposition 3 *Let the cyclic group $G = \mathcal{Z}_r$ operate on the polynomial algebra $k[X]$ as in* (2)*. Then the invariant algebra $k[X]^G$ is finitely generated, and its embedding dimension equals the number of indecomposable solutions of the linear congruence* (3)*.*

Remark For this special case the proof that the invariant algebra is finitely generated is particularly easy: If $x \in \mathbb{N}^n$ is an indecomposable solution of (3), then obviously $0 \leq x_i \leq r$ for $i = 1, \ldots, n$. Therefore the number of indecomposable solutions is bounded by $(r+1)^n$.

Remark For the best known bounds see [15].

4 The Multiplicative Group

Let k be a field. Consider the multiplicative group $G = \mathbb{G}_m = (k^\times, \cdot)$ and an operation of this group on the polynomial ring $k[X] = k[X_1, \ldots, X_n]$ that is of "monomial" type

$$t \cdot X_i = t^{a_i} X_i \quad \text{with } a_i \in \mathbb{Z} \quad \text{for all } t \in \mathbb{G}_m \text{ and } i = 1, \ldots, n. \tag{4}$$

Note that for an algebraically closed field k all representations of $\mathbb{G}_m$ as an algebraic group are diagonalizable, hence the induced operations on the polynomial ring are of monomial type.

A polynomial $f = \sum_{\nu \in \mathbb{N}^n} c_\nu X^\nu$ transforms to

$$t \cdot f = \sum_{\nu \in \mathbb{N}^n} t^{(a|\nu)} c_\nu X^\nu.$$

Therefore f is invariant if and only if it has only monomials with $(a|\nu) = 0$, and these are exactly the invariant monomials. From Proposition 1 we conclude that $k[X]^G$ has a minimal system of generators that consists of invariant monomials. Clearly an invariant monomial X^ν is in this system of generators if and only if $\nu \in \mathbb{N}^n$ is an indecomposable solution of the linear diophantine equation

$$a_1x_1 + \cdots + a_nx_n = 0. \tag{5}$$

Using Gordan's Lemma [7] [14, Theorem 2] we get:

Proposition 4 *Let the multiplicative group $G = \mathbb{G}_m$ operate on the polynomial algebra $k[X]$ as in* (4)*. Then the invariant algebra $k[X]^G$ is finitely generated, and its embedding dimension equals the number of indecomposable solutions of the linear diophantine equation* (5)*.*

Examples

1. If all $a_j > 0$, then the semigroup of solutions contains only 0. Therefore $k[X]^G = k$, $\operatorname{ebd} k[X]^G = 0$.

2. If $a_j = 0$, then the j-th unit vector e_j is an indecomposable solution. Each other indecomposable solution x has the coordinate $x_j = 0$. A variable X_j with $a_j = 0$ accounts for exactly one dimension of $\operatorname{ebd} k[X]^G$. It's no restriction if we omit it.

3. Let $n = 2$, $a_1 = 1$, $a_2 = -1$. The diophantine equation is $x_1 - x_2 = 0$. The only indecomposable solution is $(1, 1)$. The invariant algebra is $k[X]^G = k[X_1X_2]$, its embedding dimension is $\operatorname{ebd} k[X]^G = 1$.

Remark This approach easily generalizes to split tori, i. e. finite direct products of several $\mathbb{G}_m$'s [23].

5 Invariants of Binary Forms

Sections 3 and 4 have another, more indirect application to invariant theory.

Proposition 5 *Let k be an algebraically closed field of characteristic* 0*, and let G be a reductive algebraic group over k with Lie algebra $\mathfrak{g}$, and V be a finite-dimensional G-module. Assume the point $g \in G$ has a closed orbit $G \cdot v$ (and hence a reductive stabilizer H). Then:*

(i) *There is an H-submodule W of V such that*

$$V \cong \mathfrak{g} \cdot v \oplus W$$

as H-modules.

(ii) *The embedding dimension of the invariant algebra of V for G is at least as large as that of W for H, i. e. $e_{G,V} \geq e_{H,W}$.*

For a proof see [9, §2.5]. The proof uses a geometric argument and follows from Luna's etale slice theorem [10]. Note that $\mathfrak{g} \cdot v = T_v(G \cdot v)$, the tangent space at the point v to the orbit $G \cdot v$.

So in cases where $H \cong \mathcal{Z}_r$ or $H \cong \mathbb{G}_m$ the results of Sections 3 or 4 provide lower bounds for $\operatorname{ebd} \mathcal{O}(V)^G$.

We assume that $\operatorname{char} k = 0$ and consider the $(d+1)$-dimensional representation of SL_2 on the space R_d of binary forms of degree d. Let I_d be the invariant algebra and e_d, its embedding dimension.

To apply Proposition 5 we also have to consider the operation of the Lie algebra $\mathfrak{g} = \mathfrak{sl}_2$ on R_d. This Lie algebra consists of the 2×2-matrices of trace 0, has the canonical basis

$$h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

and acts on R_d by derivations. The basic operation on R_1 is

$$hX = -X, \;\; hY = Y, \;\; eX = -Y, \;\; eY = 0, \;\; fX = 0, \;\; fY = -X.$$

For $r, s \geq 1$ we derive the formulas

$$\begin{aligned} hX^rY^s &= rX^{r-1}(hX)Y^s + sX^rY^{s-1}(hY) = -rX^rY^s + sX^rY^s, \\ eX^rY^s &= rX^{r-1}(eX)Y^s + sX^rY^{s-1}(eY) = -rX^{r-1}Y^{s+1}, \\ fX^rY^s &= rX^{r-1}(fX)Y^s + sX^rY^{s-1}(fY) = -sX^{r+1}Y^{s-1}. \end{aligned}$$

Examples

1. For odd $d \geq 5$ we take the element $v = X^{d-1}Y + XY^{d-1}$. The orbit $G \cdot v$ is closed, and the stabilizer G_v is the cyclic subgroup of order $r = d - 2$ generated by

$$D(\varepsilon) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

where $\varepsilon \in k$ is a primitive r-th root of unity [18]. Therefore we may apply Proposition 5. The action of $D(\varepsilon)$ on R_d has a basis consisting of the eigenvectors $X^d, \ldots, X^{d-j}Y^j, \ldots, Y^d$ with the eigenvalues $\varepsilon^{-d}, \ldots, \varepsilon^{-d+2j}, \ldots, \varepsilon^d$. Modulo $r = d - 2$ the values of the exponents are $0, \ldots, r-1$ where 0, 2, and $r-2$ each occur twice. The tangent space $\mathfrak{g}v$ has the basis

$$\begin{aligned} hv &= (d-2)(XY^{d-1} - X^{d-1}Y), && \text{with eigenvalue 1 for } D(\varepsilon), \\ ev &= -(d-1)X^{d-2}Y^2 - Y^d, && \text{with eigenvalue } \varepsilon^{-2} \text{ for } D(\varepsilon), \\ fv &= -X^d - (d-1)X^2Y^{d-2}, && \text{with eigenvalue } \varepsilon^2 \text{ for } D(\varepsilon). \end{aligned}$$

Thus the action of $D(\varepsilon)$ on W is diagonalizable with the simple eigenvalues $1, \varepsilon, \ldots, \varepsilon^{r-1}$, and we have to determine the indecomposable solutions of the congruence

$$0 \cdot x_1 + 1 \cdot x_2 + \cdots + (r-1) \cdot x_r \equiv 0 \pmod{r}.$$

From [15] we get:

- For $d = 5$ we have $r = 3$, and the four indecomposable solutions are $(1, 0, 0)$, $(0, 3, 0)$, $(0, 0, 3)$, $(0, 1, 1)$. Thus $e_5 \geq 4$. We know that $e_5 = 4$.
- For $d = 7$ we have $r = 5$, and the number of indecomposable solutions is 15. Thus $e_7 \geq 15$. We know that $e_7 = 30$ [4].
- For $d = 9$, $r = 7$, we get 47 indecomposable solutions, thus $e_9 \geq 47$. We know that $e_9 = 92$ [1].
- For $d \geq 11$ we don't know the exact values of e_d. The results from [15] give $e_{11} \geq 118$, $e_{13} \geq 347$, $e_{15} \geq 826$, $e_{17} \geq 1493$, $e_{19} \geq 3912$, $e_{21} \geq 7935$, $e_{23} \geq 12966$, $e_{25} \geq 29161$,

2. For odd $d \geq 5$ we may also consider $v = X^d + Y^d$. The orbit $G \cdot v$ is closed, and the stabilizer G_v is the cyclic subgroup of order d generated by

$$D(\varepsilon) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

where $\varepsilon \in k$ is a primitive d-th root of unity [18]. The action of $D(\varepsilon)$ on R_d has a basis consisting of the eigenvectors $X^d, \ldots, X^{d-j}Y^j, \ldots, Y^d$ with the eigenvalues $\varepsilon^{-d}, \ldots, \varepsilon^{-d+2j}, \ldots, \varepsilon^d$. Modulo d the values of the exponents are $0, \ldots, d-1$ where 0 occurs twice. The tangent space $\mathfrak{g}v$ has the basis

$$\begin{aligned} hv &= -dX^d + dY^d, && \text{with eigenvalue 1 for } D(\varepsilon), \\ ev &= -dX^{d-1}Y, && \text{with eigenvalue } \varepsilon^2 \text{ for } D(\varepsilon), \\ fv &= -dXY^{d-1}, && \text{with eigenvalue } \varepsilon^{-2} \text{ for } D(\varepsilon). \end{aligned}$$

Thus the action of $D(\varepsilon)$ on W is diagonalizable with the simple eigenvalues ε^i for

$$i \in I = \{0, \ldots, d-1\} - \{2, d-2\},$$

and we get a lower bound for e_d by the number of indecomposable solutions of the congruence

$$\sum_{i \in I} i \cdot x_i \equiv 0 \pmod{d}.$$

This gives

$$(e_5 \geq 4), \quad e_7 \geq 17, \quad (e_9 \geq 46), \quad e_{11} \geq 165,$$

$$e_{13} \geq 426, \quad (e_{15} \geq 743), \quad e_{17} \geq 2251,$$

where the bounds in parantheses are weaker then the previous ones, but the other ones are stronger.

3. For even $d = 2r$ with odd $r \geq 3$ we take $v = X^r Y^r$. The orbit $G \cdot v$ is closed, and the stabilizer G_v is the canonical maximal torus $T \subseteq G$ consisting of the diagonal matrices

$$D(t) = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix},$$

see [18]. The action of $D(t)$ on R_d has a basis consisting of the eigenvectors $X^{d-j}Y^j$ for $j = 1, \ldots d$ with the eigenvalues t^{-d+2j}.

We compute the tangent space $\mathfrak{g}v$:

$$\begin{aligned} hv &= -rX^rY^r + rX^rY^r = 0, \\ ev &= -rX^{r-1}Y^{r+1}, \\ fv &= -rX^{r+1}Y^{r-1}, \end{aligned}$$

Thus the tangent space has the 2-element basis $\{X^{r-1}Y^{r+1}, X^{r+1}Y^{r-1}\}$ consuming the eigenvalues t^2 and t^{-2}, and the complementary subspace W has the basis

$$\{X^{d-2j}Y^j \mid j = 0, \ldots, d,\ j \neq r \pm 1\}$$

of size $d - 1$. On this basis $D(t)$ acts diagonally with the eigenvalues

$$t^{-d},\ t^{-d+2},\ \ldots,\ t^{-4},\ 1,\ t^4,\ \ldots,\ t^{d-2},\ t^d.$$

Hence the embedding dimension $e_{T,W}$ equals the number of indecomposable solutions of the linear diophantine equation

$$\sum_{j=0}^{r-2}(-d+2j)x_j + 0 \cdot x_r + \sum_{j=r+2}^{d}(2j-d)x_j = 0.$$

The one trivial solution is $x_r = 1$ and all other coordinates zero. For the remaining solutions we reformulate the equation, and find that $e_{T,W} = 1 +$ the number of indecomposable solutions of the linear diophantine equation

$$\sum_{i=2}^{r} i \cdot y_i = \sum_{i=2}^{r} i \cdot z_i.$$

This number $e_{T,W}$ is a lower bound for e_d. Equations of this type are treated in [16]. The algorithm from [16] yields the explicit values 4, 46, 304, 1482 for $r = 3, 5, 7, 9$. Thus we have the bounds $e_6 \geq 5$ (which is the correct value), $e_{10} \geq 47$ (where the correct value is known to be $e_{10} = 106$, see [2]), $e_{14} \geq 305$, $e_{18} \geq 1483$.

Example 1 also gives a general bound using the lower bound from [15]:

Corollary 1 (Kac) *Let $d \geq 9$ be odd. Then $e_d \geq 2 \cdot p(d-2)$ where p is the partition function. In particular e_d grows at least as fast as $\frac{1}{d}\exp(\sqrt{d})$.*

Note that Kac [9] gives the result without the factor 2, however this factor is only a minor improvement.

References

[1] A. Brouwer, M. Popoviciu: The invariants of the binary nonic. J. Symbolic Comp. 45 (2010), 709–720.

[2] A. Brouwer, M. Popoviciu: The invariants of the binary decimic. J. Symbolic Comp. 45 (2010), 837–843.

[3] H. Derksen, G. Kemper: *Computational Invariant Theory*. Springer-Verlag, Berlin 2002.

[4] J. Dixmier, D. Lazard: Le nombre minimum d'invariants fondamentaux pour les formes binaires de dégré 7. Port. Math. 43 (1986), 277–392.

[5] G. Freudenburg: A linear counterexample to the fourteenth problem of Hilbert in dimension eleven. Proc. Amer. Math. Soc. 135 (2007), 51–57.

[6] J. Fogarty: On Noether's bound for polynomial invariants of a finite group. Electronic Research Announcements of the AMS 7 (2001), 5–7.

[7] P. Gordan: Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coeffizienten einer endlichen Anzahl solcher Formen ist. J. reine angew. Math. 69 (1868), 323–354.

[8] D. Hilbert: Über die vollen Invariantensysteme. Math. Ann. 42 (1893), 313–373. Math. Ann. 102 (1930), 520.

[9] V. G. Kac: Root systems, representations of quivers and invariant theory. In: *Invariant Theory*, Montecatini 1982, ed. by F. Gherardelli. Springer Lect. Notes Math. 996 (1983), 74–108.

[10] D. Luna: Slices étales. Bull. Soc. Math. France Mém. 33 (1973), 81–102.

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

[12] E. Noether: Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. Nachr. Ges. Wiss. Göttingen (1926), 28–35.

[13] K. Pommerening: Invariants of unipotent groups. In: *Invariant Theory*, ed. by S.S.Koh. Springer Lecture Notes Math. 1278 (1987), 8–17

[14] K. Pommerening: A remark on subsemigroups (Dickson's Lemma). Online:
http://www.staff.uni-mainz.de/pommeren/MathMisc/Dickson.pdf

[15] K. Pommerening: The indecomposable solutions of linear congruences. Online:
http://www.staff.uni-mainz.de/pommeren/MathMisc/LinCong.pdf

[16] K. Pommerening: The indecomposable solutions of linear diophantine equations. Online:
http://www.staff.uni-mainz.de/pommeren/MathMisc/LinDio.pdf

[17] K. Pommerening: On systems of generators of graded algebras. Online:
http://www.staff.uni-mainz.de/pommeren/MathMisc/GradAlgpdf

[18] K. Pommerening: On stabilizers of binary forms. Online:
http://www.staff.uni-mainz.de/pommeren/MathMisc/StabBin.pdf

[19] K. Pommerening: Polynomial functions. Online:
http://www.staff.uni-mainz.de/pommeren/MathMisc/PolMaps.pdf

[20] V. Popov: The constructive theory of invariants. Math. USSR Izvest. 19 (1982),359–376.

[21] B. Schmid: Finite groups and invariant theory. In: *Topics in Invariant Theory*, ed. by M.-P. Malliavin. Springer Lect. Notes Math. 1478 (1991), 35–66.

[22] B. Totaro: Hilbert's 14th problem over finite fields and a conjecture on the cone of curves. Compositio Mathematica 144 (2008), 1176–1198.

[23] D. Wehlau: Constructive invariant theory for tori. Ann. Inst. Fourier 43 (1993), 1055–1066