Contents lists available at SciVerse ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

Finite separating sets and quasi-affine quotients

Emilie Dufresne

Mathematisches Institut, Universität Basel, Rheinsprung 21, CH-4051 Basel, Switzerland

A B S T R A C T

Nagata's famous counterexample to Hilbert's fourteenth problem shows that the ring of invariants of an algebraic group action on an affine algebraic variety is not always finitely generated. In some sense, however, invariant rings are not far from affine. Indeed, invariant rings are always quasi-affine, and there always exist finite separating sets. In this paper, we give a new method for finding a quasi-affine variety on which the ring of regular functions is equal to a given invariant ring, and we give a criterion to recognize separating algebras. The method and criterion are used on some known examples and in a new construction.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

The ring of invariants of an algebraic group action on an affine variety is the subalgebra formed by those regular functions which are constant on the orbits. A central question in Invariant Theory, thought to be the inspiration for Hilbert's fourteenth problem, is to ask if the ring of invariants is always finitely generated, that is, if it is always equal to the ring of regular functions on some affine variety. Nagata [13] gave a negative answer in 1958: a 32-dimensional linear representation of a non-reductive group. In 1990, Roberts gave a new, significantly simpler counterexample: an action of the additive group on a 7-dimensional affine space ([15], see Example 4.2). It led to similar smaller examples by Freudenburg in dimension 6 ([6], see Example 4.4), and Daigle and Freudenburg in dimension 5 ([1], see Example 4.1), the smallest known counterexample to Hilbert's fourteenth problem.

Invariant rings are not far from finitely generated. Not only did Nagata prove that they are at least rings of regular functions on some quasi-affine variety (see [14, Chapter V.5]), but also Derksen and Kemper showed that there always exists a finite separating set, that is, there always is a finite collection of invariants which can distinguish between any two points which are distinguished by some invariant (see [2, Proposition 2.3.12]). The first result was made constructive by Derksen and Kemper in the case of an action of a connected unipotent group on a factorial variety (see [3, Algorithm 3.8]), but the algorithm is not very practical. The second result is highly non-constructive. Until now, only one example appeared in the literature: Winkelmann [19] found a quasi-affine variety on which the regular functions are the invariants from the Daigle–Freudenburg example (see Example 4.1), and jointly with Kohls [4], we constructed a finite separating set for the same invariant ring.

In this paper, we give a new method for finding a quasi-affine variety on which the ring of regular functions is equal to a given invariant ring. In addition, we give a criterion to recognize separating algebras. The method and criterion are used on known examples in Section 4, and to construct a new example in Section 5.

2. Main result

Let $\Bbbk$ be an algebraically closed field, and let G be an algebraic group over $\Bbbk$. Suppose G acts on V, an irreducible, normal affine algebraic $\Bbbk$-variety (so that $\Bbbk[V]$, the ring of regular functions on V, is a normal, finitely generated $\Bbbk$-domain). Such

---

an action induces a representation of G on $\Bbbk[V]$ via $\sigma \cdot f = f \circ (-\sigma)$. The elements of $\Bbbk[V]$ which are fixed by G form a subalgebra $\Bbbk[V]^G$, called the *ring of invariants*.

By definition, invariants are constant on orbits. Thus, for two points $u, v \in V$ and $f \in \Bbbk[V]^G$, if $f(u) \neq f(v)$, then u and v belong to distinct orbits, and we say f *separates* u and v. Accordingly, a subset $E \subseteq \Bbbk[V]^G$ is called a *separating set* if any two points $u, v \in V$ which are separated by some invariant are separated by an element of E [2, Definition 2.3.8]. A subalgebra $A \subset \Bbbk[V]^G$ which is a separating set is called a *separating algebra*. More generally, if U is a subset of V, we say E is a separating set on U if the elements of E separate any 2 points of U which are separated by some invariant in $\Bbbk[V]^G$ (cf. [9, Definition 1.1]).

We recall the notation introduced in [3, Section 2.1], which fills the gap between colon operations on ideals and Nagata's ideal transform (see [14, Chapter V.5]). If A and B are subsets of a commutative ring S, we define the following colon operations [3, Definition 2.1]:

$$(A : B)_S := \{f \in S \mid fB \subseteq A\}, \quad \text{and}$$

$$(A : B^\infty)_S := \bigcup_{r=1}^{\infty} (A : B^r)_S = \{f \in S \mid \exists r \geq 1, \text{ such that } fB^r \subseteq A\}.$$

When A and B are ideals, these are the usual colon ideals. If R is a domain with field of fractions $Q(R)$ and $0 \neq f \in R$, then

$$(R : (f)^\infty)_{Q(R)} = R_f.$$

If $R = \Bbbk[X]$ is the ring of regular functions on an irreducible affine variety and Y is the zero set in X of the ideal I, then $(R : I^\infty)_{Q(R)}$ is the ring of regular functions on the quasi-affine variety $X \setminus Y$ [3, Lemma 2.3]. Thus, $(R : I^\infty)_{Q(R)}$ corresponds exactly to the ideal transform of Nagata. For $h_1, \ldots, h_r \in \Bbbk[X]$, we write $\mathcal{V}_X(h_1, \ldots, h_r)$ to denote the common zero set in X of the regular functions $h_1, \ldots, h_r$.

Theorem 2.1. *Let $A \subset \Bbbk[V]^G$ be a finitely generated subalgebra and let $f_1, \ldots, f_r \in A$ such that $A_{f_i} = \Bbbk[V]^G_{f_i}$ for each i.*

(1) *If $\mathcal{V}_V(f_1, \ldots, f_r) \subseteq V$ has codimension at least 2 (if $(f_1, \ldots, f_r)\Bbbk[V]$ has height at least 2 in $\Bbbk[V]$), then $\Bbbk[V]^G$ is equal to the ring of regular functions on the quasi-affine variety $W \setminus \mathcal{V}_W(f_1, \ldots, f_r)$, where $W = \mathrm{Spec}(A)$, that is, $\Bbbk[V]^G = (A : (f_1, \ldots, f_r)^\infty)_{Q(A)}$.*

(2) *If A is a separating algebra on $\mathcal{V}_V(f_1, \ldots, f_r) \subseteq V$, then A is a separating algebra on all of V.*

Proof. (1): Our assumptions imply that $Q(A) = Q(\Bbbk[V]^G)$. Since $\Bbbk[V]$ is normal and since $(f_1, \ldots, f_r)\Bbbk[V]$ has height at least 2, it follows that $(A : (f_1, \ldots, f_r)^\infty)_{Q(A)}$ is a subset of

$$(\Bbbk[V] : (f_1, \ldots, f_r)^\infty)_{\Bbbk(V)} \cap Q(A) = \Bbbk[V] \cap Q(\Bbbk[V]^G) = \Bbbk[V]^G.$$

Take $f \in \Bbbk[V]^G$. Since $f \in \Bbbk[V]^G_{f_i} = A_{f_i}$, there is $s_i \geq 0$ such that $f_i^{s_i}f \in A$. If $s = s_1 + \cdots + s_r$, then $f((f_1, \ldots, f_r)A)^s \subseteq A$. Therefore, $f \in (A : (f_1, \ldots, f_r)^\infty)_{Q(A)}$.

(2): Suppose $u, v \in V$ are separated by $f \in \Bbbk[V]^G$. If both u and v are in $\mathcal{V}_V(f_1, \ldots, f_r)$, our assumptions imply that u and v are separated by an element of A. If only one of u, v is in $\mathcal{V}_V(f_1, \ldots, f_r)$, then u and v are separated by an f_i. If neither u nor v is in $\mathcal{V}_V(f_1, \ldots, f_r)$, and if no f_i separates u and v, then there is a j such that $f_j(u) = f_j(v) \neq 0$. Since $\Bbbk[V]^G = (A : (f_1, \ldots, f_r)^\infty)_{Q(A)} \subseteq A_{f_j}$, there exists $m \geq 0$ such that $f_j^m f \in A$. As $(f_j^m f)(u) = f_j(u)^m f(u) = f_j(v)^m f(u) \neq f_j(u)^m f(u) = (f_j^m f)(v)$, an element of A separates u and v. $\square$

If B is a $\Bbbk$-algebra, then

$$\mathfrak{f}_B := \{0\} \cup \{f \in B \mid B_f \text{ is a finitely generated } \Bbbk\text{-algebra}\}$$

is a radical ideal of B, called the *finite generation locus ideal* [3, Proposition 2.10]. It is equal to B exactly when B is finitely generated. Using Theorem 2.1 relies on finding enough elements in the finite generation ideal.

Corollary 2.2. *Suppose A and $f_1, \ldots, f_r$ satisfy the conditions of Theorem 2.1(1). If $\Bbbk[V]^G \subseteq \Bbbk + (f_1, \ldots, f_r)\Bbbk[V]$, then A is a separating algebra.*

Proof. If $\Bbbk[V]^G \subseteq \Bbbk + (f_1, \ldots, f_r)\Bbbk[V]$, then all invariants are constant on $\mathcal{V}_V(f_1, \ldots, f_r)$ and so the condition of Theorem 2.1(2) is automatically satisfied. $\square$

Remark 2.3. Theorem 2.1 implies that if we have $A \subset \Bbbk[V]^G$ and an ideal I of A such that $\Bbbk[V]^G$ is equal to the ring of regular functions on $\mathrm{Spec}(A) \setminus \mathcal{V}(I)$, then under some additional assumptions, A is a separating algebra. On the other hand, if $A \subseteq \Bbbk[V]^G$ is a normal finitely generated separating algebra with $Q(A) = Q(\Bbbk[V]^G)$, then there is an ideal I of A such that $\Bbbk[V]^G$ is equal to the ring of regular functions on $\mathrm{Spec}(A) \setminus \mathcal{V}(I)$. This can be deduced from [19, Theorem 2 and Lemma 7] as follows.

Each $E \subseteq \Bbbk[V]$ induces an equivalence relation $\sim_E$ on V. For $u, v \in V$, we write $u \sim_E v$ if and only if $f(u) = f(v)$ for all $f \in E$. In [19, Lemma 7], Winkelmann shows that there exists a normal, finitely generated subalgebra $A \subset \Bbbk[V]^G$ such that $\sim_A = \sim_{\Bbbk[V]^G}$. In the proof of [19, Theorem 2], he shows that we can assume A is normal and $Q(A) = Q(\Bbbk[V]^G)$. Then, there is an ideal I of A such that

$$\Bbbk[V]^G = (A : I^\infty)_{Q(A)}.$$

The key observation is that $\sim_A = \sim_{\Bbbk[V]^G}$ exactly when A is a separating algebra. In particular, [19, Lemma 7] implies the existence of a finitely generated separating algebra.

3. Additive group actions

For the examples discussed in Sections 4 and 5, we concentrate on algebraic actions of the additive group $\mathbb{G}_a = (\mathbb{k}, +)$, and assume that $\mathbb{k}$ has characteristic 0. Such an action corresponds to a *locally nilpotent derivation (LND)*, that is, a $\mathbb{k}$-linear map $D : \mathbb{k}[V] \to \mathbb{k}[V]$ such that

(1) for all $a, b \in \mathbb{k}[V]$, we have $D(ab) = aD(b) + bD(a)$, and
(2) for all $b \in \mathbb{k}[V]$, there exists $m \geq 0$ such that $D^m(b) = 0$.

The $\mathbb{G}_a$-action on V is given by the $\mathbb{k}$-algebra homomorphism:

$$\theta : \quad \mathbb{k}[V] \quad \longrightarrow \quad \mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[T]$$
$$f \quad \longmapsto \quad \theta(f),$$

where $\mathbb{k}[T] = \mathbb{k}[\mathbb{G}_a]$ is the ring of regular functions on the algebraic group $\mathbb{G}_a$. This $\mathbb{G}_a$-action induces an action on $\mathbb{k}[V]$ via $a \cdot f = \theta(f)|_{T=-a}$. The correspondence between D and the $\mathbb{G}_a$-action is given by

$$\theta(f) = \sum_{k=0}^{\infty} \frac{D^k(f)}{k!} T^k.$$

The ring of invariants $\mathbb{k}[V]^{\mathbb{G}_a}$ coincides with the kernel of D, which we write $\mathbb{k}[V]^D$. For convenience, we will describe $\mathbb{G}_a$-actions on V by giving the corresponding LND on $\mathbb{k}[V]$. For more information on LND, we refer to the excellent book of Freudenburg [7].

If $s \in \mathbb{k}[V]$ is a slice, that is, if $D(s) = 1$, then $s : V \to \mathbb{G}_a$ is $\mathbb{G}_a$-equivariant, and there is a $\mathbb{G}_a$-equivariant isomorphism $\mathbb{G}_a \times s^{-1}(0) \xrightarrow{\sim} V$, given by $(a, v) \mapsto a \cdot v$, which identifies the invariants $\mathbb{k}[V]^{\mathbb{G}_a}$ with $\mathbb{k}[s^{-1}(0)]$. In general, if $s \in \mathbb{k}[V]$, $f := D(s) \neq 0$, and $D^2(s) = 0$, then s/f is a slice on $V_f = V \setminus \mathcal{V}_V(f)$. Such an s is called a *local slice*. We then obtain generators for $\mathbb{k}[V]_f^D$ as follows (it is the first step of van den Essen's algorithm):

Lemma 3.1 (*See [18, Sections 3 and 4]*). *Take $s \in \mathbb{k}[V]$ such that $f = D(s) \neq 0$ and $D^2(s) = 0$. If $\mathbb{k}[V] = \mathbb{k}[b_1, \ldots, b_r]$, then $\mathbb{k}[V]_f^D$ is generated by f, $1/f$, and $\{f^{e_i}\theta(b_i)|_{T=-s/f} \mid i = 1, \ldots, r\}$, where e_i is minimal so that $f^{e_i}\theta(b_i)|_{T=-s/f} \in \mathbb{k}[V]$.*

As $\mathbb{G}_a$ is a connected unipotent group, when V is factorial, the finite generation ideal $\mathfrak{f}_{\mathbb{k}[V]^D}$ generates an ideal of height at least 2 in $\mathbb{k}[V]$ (see the proof of correctness of [3, Algorithm 2.22]). Therefore, there always exist $\{f_1, \ldots, f_m\}$ and A satisfying the conditions of Theorem 2.1(1). Combining some existing algorithms, one can compute such $\{f_1, \ldots, f_m\}$ and A as follows. First, use [8, Algorithm 3.20] to compute $f_0 \in \mathfrak{f}_{\mathbb{k}[V]^D}$, and $g_{0,1}, \ldots, g_{0,s_0} \in \mathbb{k}[V]^N$, such that $\mathbb{k}[V]_{f_0}^D = \mathbb{k}[f_0, 1/f_0, g_{0,1}, \ldots, g_{0,s_0}]$. Next, use [3, Algorithm 2.13] with $S = \mathbb{k}[V]$, $R_0 = \mathbb{k}[f_0, g_{0,1}, \ldots, g_{0,s_0}]$, and $\mathfrak{a} = f_0 R$ to compute further elements $\{f_1, \ldots, f_r\}$ of $\mathfrak{f}_{\mathbb{k}[V]^D}$ until the ideal $(f_0, f_1, \ldots, f_r)\mathbb{k}[V]$ has height at least 2. The last step is to use van den Essen's Algorithm to compute $g_{i,1}, \ldots, g_{i,s_i} \in \mathbb{k}[V]^D$ such that $\mathbb{k}[V]_{f_i}^D = \mathbb{k}[f_i, 1/f_i, g_{i,1}, \ldots, g_{i,s_i}]$. Taking $\{f_0, \ldots, f_r\}$ and $A = \mathbb{k}[f_0, \ldots, f_r, g_{i,j} \mid i = 0, \ldots, r, j = 1, \ldots, s_r]$ will satisfy the conditions of Theorem 2.1(1).

4. First examples

Example 4.1 (*Daigle and Freudenburg [1]*). Let $V := \mathbb{k}^5$, and let $R := \mathbb{k}[x, s, t, u, v]$ be the ring of regular functions on V. Define a LND on R via:

$$\Delta := x^3 \frac{\partial}{\partial s} + s \frac{\partial}{\partial t} + t \frac{\partial}{\partial u} + x^2 \frac{\partial}{\partial v}.$$

Daigle and Freudenburg proved in [1] that the ring of invariants R^Δ is not finitely generated. In [19, Section 4], Winkelmann defined a subalgebra

$$
\begin{aligned}
A : &= \mathbb{k}[f_1, f_2, f_3, f_4, f_5, f_6]^1 \\
&= \mathbb{k}[x, 2x^3t - s^2, 3x^6u - 3x^3ts + s^3, xv - s, x^2ts - s^2v \\
&\quad + 2x^3tv - 3x^5u, -18x^3tsu + 9x^6u^2 + 8x^3t^3 + 6s^3u - 3t^2s^2],
\end{aligned}
$$

and proved that R^Δ is equal to the ring of regular functions on $\mathrm{Spec}(A) \setminus \mathcal{V}(x, 2x^3t - s^2)$. With Kohls [4], we proved that A is a separating algebra. We will show how both results follow from Theorem 2.1.

---

[1] In fact, we have $A = \mathbb{k}[f_1, f_2, f_4, f_5, f_6]$, since $f_3 = -f_1f_5 + f_2f_4$.

We have $x^3 = \Delta(s) \in R^\Delta$ and $f_2 = 2x^3t - s^2 = \Delta(3x^3u - st) \in R^\Delta$. Lemma 3.1 yields the following generators

for $R_x^\Delta = R_{x^3}^\Delta$: and for $R_{f_2}^\Delta$:

$x, 1/xv$ $\qquad$ $f_2, 1/f_2$

$\theta(x)|_{-s/x^3} = x = f_1$ $\qquad$ $\theta(x)|_{-(3x^3u-st)/f_2} = x = f_1$

$\theta(s)|_{-s/x^3} = 0$ $\qquad$ $f_2\theta(s)|_{-(3x^3u-st)/f_2} = -f_3/2$

$x^3\theta(t)|_{-s/x^3} = f_2/2$ $\qquad$ $f_2^2\theta(t)|_{-(3x^3u-st)/f_2} = x^3f_6/2$

$x^6\theta(u)|_{-s/x^3} = f_3/3$ $\qquad$ $f_2^3\theta(u)|_{-(3x^3u-st)/f_2} = f_6f_3/6$

$x\theta(v)|_{-s/x^3} = f_4,$ $\qquad$ $f_2\theta(v)|_{-(3x^3u-st)/f_2} = f_5.$

Observe that A contains the above polynomials, and so $A_x = R_x^\Delta$ and $A_{f_2} = R_{f_2}^\Delta$. As $\mathcal{V}_{\mathbb{k}^5}(x^3, 2x^3t - s^2) = \mathcal{V}_{\mathbb{k}^5}(x, s)$ has codimension 2, Theorem 2.1(1) implies that R^Δ is the ring of regular functions on $\mathrm{Spec}(A) \setminus \mathcal{V}(x, 2x^3t - s^2)$.

Using the fact that Δ is graded and commutes with $\frac{\partial}{\partial u}$ and $\frac{\partial}{\partial v}$, one can show that $R^{\mathbb{G}_a} \subseteq \mathbb{k} \oplus (x, s)R$ (see [4, Proposition 3.2]). Corollary 2.2 then implies that A is a separating algebra. $\square$

Example 4.2 (*Roberts [15]*). Let $B := \mathbb{k}[x_1, x_2, x_3, y_1, y_2, y_3, v]$, and let $2 \leq m \in \mathbb{Z}$. Consider the LND defined on B via:

$$D := x_1^{m+1}\frac{\partial}{\partial y_1} + x_2^{m+1}\frac{\partial}{\partial y_2} + x_3^{m+1}\frac{\partial}{\partial y_3} + (x_1x_2x_3)^m\frac{\partial}{\partial v}.$$

Roberts [15] proved that B^D is not finitely generated.

For each i, $D(y_i) = x_i^{m+1} \in B^D$, and Lemma 3.1 yields the following invariants:

$\phi_1 = x_1^{m+1}y_2 - x_2^{m+1}y_1, \quad \phi_2 = x_1^{m+1}y_3 - x_3^{m+1}y_1, \quad \phi_3 = x_2^{m+1}y_3 - x_3^{m+1}y_2,$

$\phi_4 = (x_1x_2)^my_3 - x_3v, \quad \phi_5 = (x_1x_3)^my_2 - x_2v, \quad \phi_6 = (x_2x_3)^my_1 - x_1v.$

Let $A = \mathbb{k}[x_1, x_2, x_3, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6]$. By construction, we have $B_{x_i}^D = A_{x_i}$. As $\mathcal{V}_{\mathbb{k}^7}(x_1, x_2, x_3)$ has codimension 3, Theorem 2.1(1) implies that B^D is the ring of regular functions on $\mathrm{Spec}(A) \setminus \mathcal{V}(x_1, x_2, x_3)$.

As $B^D \subseteq \mathbb{k} \oplus (x_1, x_2, x_3)B$ (see [15, Lemma 2]), Corollary 2.2 implies A is a separating algebra. $\square$

Remark 4.3. Part (1) of Theorem 2.1 does not imply part (2). Indeed, $A' := \mathbb{k}[x_1, x_2, x_3, \phi_1, \phi_2, \phi_3, \phi_5, \phi_6]$ is not a separating algebra, as A' does not separate $(0, 0, 1, 0, 0, 0, 1)$ from the origin, although $\phi_4(0, 0, 1, 0, 0, 0, 1) = 1$. On the other hand, by Lemma 3.1, $A'_{x_1} = B_{x_1}^D$ and $A'_{x_2} = B_{x_2}^D$. Since $\mathcal{V}_{\mathbb{k}^7}(x_1, x_2)$ has codimension 2, Theorem 2.1(1) implies that B^D is the ring of regular functions on $\mathrm{Spec}(A') \setminus \mathcal{V}(x_1, x_2)$.

Example 4.4 (*Freudenburg [6]*). Let $B := \mathbb{k}[x, y, s, t, u, v]$, and define a LND on B via:

$$D := x^3\frac{\partial}{\partial s} + y^3s\frac{\partial}{\partial t} + y^3t\frac{\partial}{\partial u} + x^2y^2\frac{\partial}{\partial v}.$$

Freudenburg [6] showed that B^D is not finitely generated.

Let A be the $\mathbb{k}$-algebra generated by:

$x, y, -y^2s + xv, -\frac{1}{2}y^3s^2 + x^3t,$

$-x^2y^3st + 3x^5u + y^4s^2v - 2x^3ytv,$

$-\frac{3}{2}y^6s^2t^2 + 4x^3y^3t^3 + 3y^6s^3u - 9x^3y^3stu + \frac{9}{2}x^6u^2.$

We have $D(s) = x^3 \in B^D$ and $D(3x^3u - y^3st) = 2x^3y^3t - y^6s^2 \in B^D$. Comparing with the generators given by Lemma 3.1, we see that $A_{2x^3y^3t - y^6s^2} = B_{2x^3y^3t - y^6s^2}^D$, and $A_x = B_x^D$. As

$$\mathcal{V}_{\mathbb{k}^6}(x, 2x^3y^3t - y^6s^2) = \mathcal{V}_{\mathbb{k}^6}(x, ys) = \mathcal{V}_{\mathbb{k}^6}(x, y) \cup \mathcal{V}_{\mathbb{k}^6}(x, s)$$

has codimension 2, Theorem 2.1(1) implies that B^D is the ring of regular functions on $\mathrm{Spec}(A) \setminus \mathcal{V}(x, 2x^3y^3t - y^6s^2)$.

We have $B^D \subseteq \mathbb{k} \oplus (x, y)B$ (see [6, Lemma 1]). A careful study of the list of generators given by Tanimoto for B^D [16, Theorem 1.6] reveals that $B^D \subseteq \mathbb{k}[y] \oplus (x, s)B$. As A contains y, A is a separating algebra on both $\mathcal{V}_{\mathbb{k}^6}(x, y)$ and $\mathcal{V}_{\mathbb{k}^6}(x, s)$. Hence, it is a separating algebra on $\mathcal{V}_{\mathbb{k}^6}(x, 2x^3y^3t - y^6s^2)$. By Theorem 2.1(2), A is a separating algebra on all of $\mathbb{k}^6$.

5. A new 7-dimensional example

The new 7-dimensional example discussed in this section illustrates the difficulty involved in applying Theorem 2.1(2). Let $B := \Bbbk[x_1, x_2, x_3, y_1, y_2, y_3, v]$, and define a LND on B via:

$$D := x_1^a \frac{\partial}{\partial y_1} + x_2^a \frac{\partial}{\partial y_2} + x_3^a \frac{\partial}{\partial y_3} + (y_1 y_2 y_3)^b \frac{\partial}{\partial v},$$

where $1 \leq a, b \in \mathbb{Z}$. We do not know if B^D is finitely generated.

Noting that $D(y_i) = x_i^a \in B^D$, we apply Lemma 3.1 to define $A \subset B^D$ so that $A_{x_i} = B_{x_i}^D$:

$$A := \Bbbk[x_1, x_2, x_3, x_1^a y_2 - x_2^a y_1, x_1^a y_3 - x_3^a y_1, x_2^a y_3 - x_3^a y_2, h_1, h_2, h_3],$$

where

$$h_i = x_i^{(2b+1)a} \theta(v)|_{T=-y_i/x_i^a}, \quad i = 1, 2, 3,$$

and $\theta : B \to B[T]$ is the map giving the $\mathbb{G}_a$-action. As $\mathcal{V}_{\Bbbk^7}(x_1, x_2, x_3)$ has codimension 3, by Theorem 2.1(1) B^D is the ring of regular functions on $\mathrm{Spec}(A) \setminus \mathcal{V}(x_1, x_2, x_3)$.

In Lemma 5.3 below, we will show that $B^D \subseteq \Bbbk \oplus (x_1, x_2, x_3)B$. By Corollary 2.2, it then follows that A is a separating algebra.

Our argument to prove Lemma 5.3 relies on the relationship between our new 7-dimensional example and a generalization of an example first proposed by Maubach [11, Chapter 5]. Let $R := \Bbbk[x, y, z, u, w]$, and let $1 \leq a, b \in \mathbb{Z}$. Define a LND on R:

$$\Delta := x^a \frac{\partial}{\partial y} + y \frac{\partial}{\partial z} + z \frac{\partial}{\partial u} + u^b \frac{\partial}{\partial w}.$$

In the case $a = 1$, $b = 2$, Maubach asked if R^Δ is finitely generated. The question remains open.

In [7, Section 7.2.3], Freudenburg explains how the Daigle–Freudenburg example (see Example 4.1) can be derived from Roberts' example (see Example 4.2) by "removing all symmetries". We follow the same argument to derive Maubach's example from our new 7-dimensional example. Consider the faithful action on B by the 3-dimensional multiplicative group $\mathbb{G}_m^3$ given by:

$$(\lambda, \mu, \nu) \cdot (x_1, x_2, x_3, y_1, y_2, y_3, v) := (\lambda x_1, \mu x_2, \nu x_3, \lambda^a y_1, \mu^a y_2, \nu^a y_3, (\lambda \mu \nu)^b v).$$

This action commutes with D. Additionally, D commutes with the action of the symmetric group S_3 given by:

$$\sigma \cdot (x_1, x_2, x_3, y_1, y_2, y_3, v) := (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, y_{\sigma(1)}, y_{\sigma(2)}, y_{\sigma(3)}, v).$$

The group S_3 acts on $\mathbb{G}_m^3$ by conjugation, and so $\mathbb{G}_m^3 \rtimes S_3$ acts on B. Since the $\mathbb{G}_m^3$-action has no non-constant invariants, we consider the subgroup H of $\mathbb{G}_m^3$ given by $\lambda \mu \nu = 1$. This subgroup H is isomorphic to $\mathbb{G}_m^2$, and the group $G := H \rtimes S_3$ acts on B. The invariant ring of H is generated by monomials:

$$B^H = \Bbbk[x_1 x_2 x_3, x_1^a y_2 y_3, x_2^a y_1 y_3, x_3^a y_1 y_2, x_1^a x_2^a y_3, x_1^a x_3^a y_2, x_2^a x_3^a y_1, y_1 y_2 y_3, v].$$

Since H is normal in G, $B^G = (B^H)^{S_3}$. Moreover, B^G is a polynomial ring in 5 variables given as a subalgebra of B by:

$$\Bbbk[x_1 x_2 x_3, x_1^a y_2 y_3 + x_2^a y_1 y_3 + x_3^a y_1 y_2, x_1^a x_2^a y_3 + x_1^a x_3^a y_2 + x_2^a x_3^a y_1, y_1 y_2 y_3, v].$$

Setting

$$
\begin{aligned}
x &:= x_1 x_2 x_3, \\
y &:= (x_1^a x_2^a y_3 + x_1^a x_3^a y_2 + x_2^a x_3^a y_1)/3, \\
z &:= (x_1^a y_2 y_3 + x_2^a y_1 y_3 + x_3^a y_1 y_2)/6, \\
u &:= y_1 y_2 y_3/6, \\
w &:= v/6^b,
\end{aligned}
$$

we have $B^G = R$, and the LND induced by D coincides with Δ. As G is a reductive group and since $R^\Delta = (B^D)^G$, if B^D is finitely generated, so is R^Δ.

Lemma 5.1. $B^D \subseteq \Bbbk[y_1, y_2, y_3] \oplus (x_1, x_2, x_3)B.$

Proof. If $B' := \Bbbk[y_1, y_2, y_3, v] \cong B/(x_1, x_2, x_3)$, then D induces a locally nilpotent derivation on B':

$$D' := (y_1 y_2 y_3)^b \frac{\partial}{\partial v},$$

with kernel $B'^{D'} = \Bbbk[y_1, y_2, y_3]$. Thus, if $f \in \Bbbk[V]^{\mathbb{G}_a}$, we can write

$$f := x_1 f_1 + x_2 f_2 + x_3 f_3 + h,$$

where h can be viewed as an element of B'. As $D(f) = 0$, we have $D'(h) = 0$, and so $f \in \Bbbk[y_1, y_2, y_3] \oplus (x_1, x_2, x_3)B$. $\quad\square$

Lemma 5.2. $R^{\Delta} \subseteq \Bbbk \oplus (x, y, z)R.$

Proof. If $R' := \Bbbk[y, z, u, w] \cong R/(x)$, then Δ induces a locally nilpotent derivation on R':

$$\Delta' := y\frac{\partial}{\partial z} + z\frac{\partial}{\partial u} + u^b\frac{\partial}{\partial v}.$$

Since this is an elementary monomial derivation in four variables, the ring of invariants is generated by at most four elements [10], which we compute with van den Essen's Algorithm [18, Section 4]. First, we write down the algebra map $\theta' : R' \to R'[T]$ corresponding to Δ':

$$\theta'(y) = y,$$
$$\theta'(z) = z + yT,$$
$$\theta'(u) = u + zT + \tfrac{1}{2}yT^2,$$
$$\theta'(w) = w + \sum_{l=1}^{2b+1} \frac{1}{l}T^l \sum_{m=0}^{b} \binom{b}{b-m, 2m+1-l, l-m-1} \frac{1}{2^{l-m-1}} u^{b-m}z^{2m+1-l}y^{l-m-1}.$$

Choosing the local slice z, the first step of the algorithm yields the following three generators:

$$y,$$
$$h := yu - \tfrac{1}{2}z^2,$$
$$h' := y^{b+1}w + \sum_{l=1}^{2b+1} \frac{(-1)^l}{l} \sum_{m=0}^{b} \binom{b}{b-m, 2m+1-l, l-m-1} \frac{1}{2^{l-m-1}} u^{b-m}z^{2m+1}y^{b-m}.$$

The second step of the algorithm yields the fourth generator:

$$h'' = \frac{1}{y^n}\left(\frac{1}{\alpha^2}h^{2b+1} + 2^{2b+1}h'^2\right),$$

where

$$\alpha := \sum_{j=0}^{b} \frac{(-1)^{j+b+1}}{(j+b+1)2^j}\binom{b}{j} = (-1)^{b+1}2^b/\binom{2b+1}{b+1},$$

and n is maximal so that y^n divides $\frac{4}{3}h^2 + \frac{1}{\alpha}h'^{2b+1}$. It only remains to check that $y, h, h', h'' \in (y, z)R'$. This is clear for $y, h,$ and h'. Modulo z, we have

$$h'' \equiv \frac{1}{y^n}\left(\frac{1}{\alpha^2}(uy)^{2b+1} + 2^{2b+1}(wy^{b+1})^2\right).$$

Since the terms divisible by y^{2b} in $\frac{1}{\alpha^2}h^{2b+1}$ and $2^{2b+1}h'^2$ do not cancel, $n \leq 2b$. It follows that $h'' \in (y, z)R'$, and so $R'^{\Delta'} \subseteq \Bbbk \oplus (y, z)R'$, hence $R^{\Delta} \subseteq \Bbbk \oplus (x, y, z)R.$ $\square$

Lemma 5.3. $B^D \subseteq \Bbbk \oplus (x_1, x_2, x_3)B.$

Proof. The linear $\mathbb{G}_m^3$-action on B induces a $\mathbb{Z}^3$-grading (here, really a $\mathbb{N}^3$-grading) ω on B via characters where $B_{(0,0)} = B^G = \Bbbk$ (see [12, Proposition 4.14]). The derivation D commutes with the $\mathbb{G}_m^3$-action, implying that $B^D \subset B$ is a $\mathbb{N}^3$-graded subalgebra. Therefore, it suffices to show that every non-constant ω-homogeneous element of B^D is in the ideal $(x_1, x_2, x_3)B$.

Suppose, for a contradiction, that f is a non-constant ω-homogeneous element of B^D not contained in the ideal $(x_1, x_2, x_3)B$. By Lemma 5.1, it is of the form $f = f_1 + f_2$, where $f_1 \in \Bbbk[y_1, y_2, y_3]$ and $f_2 \in (x_1, x_2, x_3)B$. As f is ω-homogeneous, so are f_1 and f_2. Hence, f_1 is supported at the monomial $y_1^{l_1}y_2^{l_2}y_3^{l_3}$. Let F be the orbit product of f under the S_3-action. We then have $F = F_1 + F_2$, where $F_2 \in (x_1, x_2, x_3)B$ and $F_1 \in \Bbbk[y_1, y_2, y_3]$ is supported at the monomial $y_1^l y_2^l y_3^l$. As D commutes with the S_3-action, $D(F) = 0$. The linear action of $H \cong \mathbb{G}_m^2$ induces a $\mathbb{Z}^2$-grading on B via characters, where $B_{(0,0)} = B^H$ (see again [12, Proposition 4.14]). Let F' be the component of F of degree $(0, 0)$, then F' is H-invariant and contains the term F_1. As S_3 acts on B^H and F is S_3-invariant, F' is S_3-invariant. It follows that $F' \in (B^H)^{S_3} = B^G = R$. As D commutes with the H-action, D is graded with respect to the induced $\mathbb{Z}^2$-grading, and so $D(F') = 0$, that is, F' is an element of R^{Δ} supported at the monomial u^l, a contradiction to Lemma 5.2. $\square$

Remark 5.4. As in our joint work with Maurischat [5], one can define a characteristic-free analog to this new 7-dimensional example. The map θ has rational coefficients with denominators all dividing $(3b + 1)!$. Thus, we can interpret θ as a locally finite iterative higher derivation over any field of characteristic $p > 3b + 1$. Use [17, Theorem 1.1] (the positive characteristic analog of Lemma 3.1) to define $A \subset B^\theta$ so that $A_{x_i} = B_{x_i}^D$:

$$A = \Bbbk[x_1, x_2, x_3, x_1^a y_2 - x_2^a y_1, x_1^a y_3 - x_3^a y_1, x_2^a y_3 - x_3^a y_2, f_1, f_2, f_3],$$

where

$$f_i = x_i^{(2b+1)a}\theta(v)\big|_{T=\frac{-y_i}{x_i^a}}, \quad i = 1, 2, 3.$$

Theorem 2.1(1) implies that B^D is the ring of regular functions on $\mathrm{Spec}(A) \setminus \mathcal{V}(x_1, x_2, x_3)$. We can show that $B^\theta \subseteq \Bbbk \oplus (x_1, x_2, x_3)B$, and so, by Corollary 2.2, A is a separating algebra. The only significant difference with the characteristic zero case is that in Lemma 5.2, we must prove that the algorithm really ends after obtaining the fourth generator. This can be done as in the original argument of Maubach [10, Case 3, theorem 3.1], using that modulo y, h'' does not depend only on z.

Acknowledgments

References

[1] Daniel Daigle, Gene Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension 5, J. Algebra 221 (2) (1999) 528–535.
[2] Harm Derksen, Gregor Kemper, Computational Invariant Theory, in: Encyclopaedia of Mathematical Sciences., Number 130, Springer-Verlag, Berlin, Heidelberg, New York, 2002.
[3] Harm Derksen, Gregor Kemper, Computing invariants of algebraic groups in arbitrary characteristic, Adv. Math. 217 (5) (2008) 2089–2129.
[4] Emilie Dufresne, Martin Kohls, A finite separating set for Daigle and Freudenburg's counterexample to Hilbert's fourteenth problem, Comm. Algebra 38 (11) (2010) 3987–3992.
[5] Emilie Dufresne, Andreas Maurischat, On the finite generation of additive group invariants in positive characteristic, J. Algebra 324 (8) (2010) 1952–1963.
[6] Gene Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension six, Transform. Groups 5 (1) (2000) 61–71.
[7] Gene Freudenburg, Algebraic Theory of Locally Nilpotent Derivations, in: Encyclopaedia of Mathematical Sciences, Springer, Berlin Heidelberg, 2006.
[8] Tobias Kamke, Algorithms for the Computation of Invariant Rings, Ph.D. Thesis, Technische Universität München, Zentrum Mathematik, Garching, Germany, 2009.
[9] Gregor Kemper, Separating invariants, J. Symbolic Comput. 44 (9) (2009) 1212–1222.
[10] Stefan Maubach, Triangular monomial derivations on $k[X_1, X_2, X_3, X_4]$ have kernel generated by at most four elements, J. Pure Appl. Algebra 153 (2) (2000) 165–170.
[11] Stefan Maubach, Polynomial endomorphisms and kernels of derivations, Ph.D. Thesis, University of Nijmegen, Nijmegen, Netherlands, 2003. http://webdoc.ubn.kun.nl/mono/m/maubach_s/polyenank.pdf.
[12] Shigeru Mukai, An introduction to invariants and moduli, in: Cambridge Studies in Advanced Mathematics, vol. 81, Cambridge University Press, Cambridge, 2003, Translated from the 1998 and 2000 Japanese editions by W. M. Oxbury.
[13] Masayoshi Nagata, On the fourteenth problem of Hilbert, in: Proc. Internat. Congress Math. 1958, Cambridge Univ. Press, New York, 1960, pp. 459–462.
[14] Masayoshi Nagata, Lectures on the fourteenth problem of Hilbert, Tata Institute of Fundamental Research, Bombay, 1965.
[15] Paul Roberts, An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert's fourteenth problem, J. Algebra 132 (2) (1990) 461–473.
[16] Ryuji Tanimoto, On Freudenburg's counterexample to the fourteenth problem of Hilbert, Transform. Groups 11 (2) (2006) 269–294.
[17] Ryuji Tanimoto, An algorithm for computing the kernel of a locally finite iterative higher derivation, J. Pure Appl. Algebra 212 (10) (2008) 2284–2297.
[18] Arno van den Essen, An algorithm to compute the invariant ring of a $\mathbf{G}_a$-action on an affine variety, J. Symbolic Comput. 16 (6) (1993) 551–555.
[19] Jörg Winkelmann, Invariant rings and quasiaffine quotients, Math. Z. 244 (1) (2003) 163–174.