A FINITE SEPARATING SET FOR DAIGLE AND FREUDENBURG'S COUNTEREXAMPLE TO HILBERT'S FOURTEENTH PROBLEM

EMILIE DUFRESNE AND MARTIN KOHLS

Abstract. This paper gives the first explicit example of a finite separating set in an invariant ring which is not finitely generated, namely, for Daigle and Freudenburg's 5-dimensional counterexample to Hilbert's Fourteenth Problem.

1. Introduction

Hilbert's Fourteenth Problem asks if the ring of invariants of an algebraic group action on an affine variety is always finitely generated. The answer is negative in general: Nagata [11] gave the first counterexample in 1959. In characteristic zero, the Maurer-Weitzenböck Theorem [15] tells us that linear actions of the additive group have finitely generated invariants, but nonlinear actions need not have finitely generated invariants. Indeed, there are several such examples, the smallest being Daigle and Freudenburg's 5-dimensional counterexample [1] to Hilbert's Fourteenth Problem.

Although rings of invariants are not always finitely generated, there always exists a finite separating set [2, Theorem 2.3.15]. In other words, if $\Bbbk$ is a field and if a group G acts on a finite dimensional $\Bbbk$-vector space V, then there always exists a finite subset E of the invariant ring $\Bbbk[V]^G$ such that if, for two points $x, y \in V$, we have $f(x) = f(y)$ for all $f \in E$, then $f(x) = f(y)$ for all $f \in \Bbbk[V]^G$. This notion was introduced by Derksen and Kemper [2, Section 2.3], and has gained a lot of attention in the recent years, for example see [3, 4, 5, 6, 8, 12].

The proof of the existence of a finite separating set is not constructive, and until now, no example was known for infinitely generated invariant rings. The main result of this paper is to give the first example: a finite separating set for Daigle and Freudenburg's 5-dimensional counterexample to Hilbert's Fourteenth Problem.

Acknowledgments. We thank Gregor Kemper for funding visits of the first author to TU München.

Date: December 3, 2009.

2. Daigle and Freudenburg's Counterexample

We now introduce the notation used throughout the paper, and set up the example. We recommend the book of Freudenburg [7] as an excellent reference for locally nilpotent derivations.

Let $\Bbbk$ be a field of characteristic zero, and let $\mathbb{G}_a$ be its additive group. If $V = \Bbbk^5$ is a 5-dimensional vector space over $\Bbbk$, then $\Bbbk[V] = \Bbbk[x, s, t, u, v]$ is a polynomial ring in five variables. Daigle and Freudenburg [1] define a locally nilpotent $\Bbbk$-derivation on $\Bbbk[V]$:

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

This derivation D induces an action of $\mathbb{G}_a$ on V. If r is an additional indeterminate, then the corresponding map of $\Bbbk$-algebras is

$$\mu : \Bbbk[V] \to \Bbbk[V][r], \quad f \mapsto \mu(f) = \mu_r(f) = \sum_{k=0}^{\infty} \frac{D^k(f)}{k!} r^k, \tag{1}$$

where $\Bbbk[V][r] \cong \Bbbk[V] \otimes_{\Bbbk} \Bbbk[\mathbb{G}_a]$. The induced action of $\mathbb{G}_a$ on $\Bbbk[V]$ is:

$$(-a) \cdot f := \mu_a(f) \quad \text{for all } a \in \mathbb{G}_a, f \in \Bbbk[V].$$

In particular, for $a \in \mathbb{G}_a$, we have

$$(-a)\cdot x = x, \quad (-a)\cdot s = s + ax^3, \quad (-a)\cdot t = t + as + \frac{a^2}{2}x^3,$$

$$(-a)\cdot u = u + at + \frac{a^2}{2}s + \frac{a^3}{6}x^3, \quad (-a)\cdot v = v + ax^2.$$

The invariant ring $\Bbbk[V]^{\mathbb{G}_a}$ coincides with the kernel of D. Define a grading on $\Bbbk[V]$ by assigning $\deg x = 1$, $\deg s = \deg t = \deg u = 3$, $\deg v = 2$. As the action of $\mathbb{G}_a$ on $\Bbbk[V]$ and the derivation D are homogeneous with respect to this grading, the ring of invariants is a graded subalgebra. We write $\Bbbk[V]^{\mathbb{G}_a}_+$ to denote the unique maximal homogeneous ideal of $\Bbbk[V]^{\mathbb{G}_a}$. Daigle and Freudenburg [1] proved that $\Bbbk[V]^{\mathbb{G}_a} = \ker D$ is not finitely generated as a $\Bbbk$-algebra. The main result of this paper is to exhibit a finite geometric separating set.

Theorem 2.1. *Let $\mathbb{G}_a$ act on V as above. The following 6 homogeneous polynomials are invariants and form a separating set E in $\Bbbk[V]^{\mathbb{G}_a}$:*

$$f_1 = x, \quad f_2 = 2x^3t - s^2, \quad f_3 = 3x^6u - 3x^3ts + s^3,$$
$$f_4 = xv - s, \quad f_5 = x^2ts - s^2v + 2x^3tv - 3x^5u,$$
$$f_6 = -18x^3tsu + 9x^6u^2 + 8x^3t^3 + 6s^3u - 3t^2s^2.$$

Remark 2.2. In [16, Lemma 12], Winkelmann shows that these six invariants separate orbits outside $\{p \in V : x(p) = s(p) = 0\}$, which as we will see later, is the easy case. (Note that in [16] there is a typo in the invariant we denoted by f_6.)

3. Proof of Theorem 2.1

In this section, we prove our main result. We start by establishing some useful facts.

Lemma 3.1. $\Bbbk[V]^{\mathbb{G}_a} \subseteq \Bbbk[f_1, f_2, f_3, f_4, \frac{1}{x}]$.

Proof. As x is a constant, the derivation D extends naturally to $\Bbbk[V]_x$ via $D\left(\frac{f}{x^n}\right) := \frac{D(f)}{x^n}$ for all $f \in \Bbbk[V], n \in \mathbb{N}$, and we have $\Bbbk[V]^{\mathbb{G}_a} \subseteq (\Bbbk[V]_x)^{\mathbb{G}_a}$. The element $\frac{s}{x^3} \in \Bbbk[V]_x$ satisfies $D\left(\frac{s}{x^3}\right) = 1$, that is, it is a slice. By the Slice Theorem (see [14, Proposition 2.1], or [7, Corollary 1.22]), we obtain a generating set of the invariant ring $\Bbbk[V]_x^{\mathbb{G}_a}$ by applying μ to the generators of $\Bbbk[V]_x = \Bbbk[x, s, t, u, v, \frac{1}{x}]$ and "evaluating" at $r = -\frac{s}{x^3}$. Therefore, we have

$$\begin{aligned} \Bbbk[V]_x^{\mathbb{G}_a} &= \Bbbk\left[\mu_{-\frac{s}{x^3}}(x), \mu_{-\frac{s}{x^3}}(s), \mu_{-\frac{s}{x^3}}(t), \mu_{-\frac{s}{x^3}}(u), \mu_{-\frac{s}{x^3}}(v), \mu_{-\frac{s}{x^3}}(\tfrac{1}{x})\right] \\ &= \Bbbk\left[f_1, 0, \frac{f_2}{2x^3}, \frac{f_3}{3x^6}, \frac{f_4}{x}, \frac{1}{x}\right]. \end{aligned}$$

□

Proof of Theorem 2.1. First, note that f_i is invariant for $i = 1, \ldots, 6$. Let $p_i = (\chi_i, \sigma_i, \tau_i, \omega_i, \nu_i)$, $i = 1, 2$, be two points in V such that $f_i(p_1) = f_i(p_2)$ for each $i = 1, \ldots, 6$. We will show that $f(p_1) = f(p_2)$ for all $f \in \Bbbk[V]^{\mathbb{G}_a}$. Since $f_1 = x$, we have $\chi_1 = \chi_2$. If $\chi_1 = \chi_2 \neq 0$, then Lemma 3.1 implies $f(p_1) = f(p_2)$ for all $f \in \Bbbk[V]^{\mathbb{G}_a}$. Thus, we may assume $\chi_1 = \chi_2 = 0$. It follows that $\sigma_1 = -f_4(p_1) = -f_4(p_2) = \sigma_2$. Define a linear map

$$\gamma : \Bbbk^5 \to \Bbbk^4, \quad (\chi, \sigma, \tau, \omega, \nu) \mapsto (\sigma, \tau, \omega, \nu),$$

and a $\Bbbk$-algebra morphism

$$\rho : \Bbbk[x, s, t, u, v] \to \Bbbk[s, t, u, v], \quad f(x, s, t, u, v) \mapsto f(0, s, t, u, v).$$

Define a $\Bbbk$-linear locally nilpotent derivation on $\Bbbk[s, t, u, v]$ via

$$\Delta = s\frac{\partial}{\partial t} + t\frac{\partial}{\partial u}.$$

One easily verifies that $\Delta \circ \rho = \rho \circ D$. In particular, ρ induces a map $\ker D \to \ker \Delta$. The kernel of Δ is known (or can be computed with van den Essen's Algorithm [14]): it corresponds to the binary forms of degree 2, that is,

$$\ker \Delta = \Bbbk[s, 2us - t^2, v]. \tag{2}$$

Since $\chi_i = 0$, we have $f(p_i) = \rho(f)(\gamma(p_i))$ for $i = 1, 2$ and any $f \in \Bbbk[V]$. Thus, to show $f(p_1) = f(p_2)$ for all $f \in \Bbbk[V]^{\mathbb{G}_a} = \ker D$, it suffices to show $f(\gamma(p_1)) = f(\gamma(p_2))$ for all $f \in \rho(\ker D) \subseteq \Bbbk[s, 2us - t^2, v]$.

If $\sigma_1 = \sigma_2 \neq 0$, then the values of $s, 2us - t^2, v$ on $\gamma(p_i)$ are uniquely determined by the values of $\rho(f_4) = -s$, $\rho(f_5) = -s^2v$, and $\rho(f_6) = 3s^2(2us - t^2)$ on $\gamma(p_i)$ for $i = 1, 2$. Since

$$\rho(f_i)(\gamma(p_1)) = f_i(p_1) = f_i(p_2) = \rho(f_i)(\gamma(p_2)) \quad \text{for all } i = 1, \ldots, 6,$$

the case $\sigma_1 = \sigma_2 \neq 0$ is done. Assume $\chi_1 = \chi_2 = \sigma_1 = \sigma_2 = 0$, then by Proposition 3.2, $f(p_1) = f(p_2) = f(0, 0, 0, 0, 0)$ for all $f \in \Bbbk[V]^{\mathbb{G}_a}$. □

Proposition 3.2. *We have* $\Bbbk[V]^{\mathbb{G}_a} \subseteq \Bbbk \oplus (x, s)\Bbbk[V]$.

This proposition is the key to the proof of Theorem 2.1. It could be obtained from a careful study of the generating set of $\Bbbk[V]^{\mathbb{G}_a}$ given by Tanimoto [13]. We give a more self-contained proof, which relies only on the van den Essen-Maubach Kernel-check Algorithm (see [14], and [10, p. 32]).

Proof of Proposition 3.2. It suffices to show that $\Bbbk[V]_+^{\mathbb{G}_a} \subseteq (x, s)\Bbbk[V]$. By way of contradiction, suppose there exists $f \in \Bbbk[V]_+^{\mathbb{G}_a}$ of the form $f = xp + sq + h(t, u, v)$, where $p, q \in \Bbbk[V]$, and $h(t, u, v) \neq 0$.

Without loss of generality, we can assume f is homogeneous of positive degree. We apply the map ρ from the proof of Theorem 2.1. By Equation (2), we have $f(0, s, t, u, v) \in \Bbbk[s, 2us - t^2, v]$, so we have $f(0, 0, t, u, v) = h(t, u, v) \in \Bbbk[0, -t^2, v]$, and we set $h(t, v) := h(t, u, v) \in \Bbbk[t, v]$. Since f is homogeneous, so is h, and there is a unique monomial $t^d v^e$ in h such that the exponent e of v is maximal. Clearly, $D \circ \frac{\partial}{\partial v} = \frac{\partial}{\partial v} \circ D$, and so, for all k, we have

$$\frac{\partial^k f}{\partial v^k} = x\frac{\partial^k p}{\partial v^k} + s\frac{\partial^k q}{\partial v^k} + \frac{\partial^k h(t, v)}{\partial v^k} \in \Bbbk[V]^{\mathbb{G}_a}.$$

If $d = 0$, then taking $k = e-1$, implies v is the only monomial appearing in $\frac{\partial^{e-1} h(t,v)}{\partial v^{e-1}}$ (since v has degree 2, and t has degree 3, t cannot have nonzero exponent). Thus, there is a homogeneous invariant of degree 2 of the form $x\tilde{p} + s\tilde{q} + v \in \Bbbk[V]^{\mathbb{G}_a}$, but as x^2 spans the space of invariants of degree 2, we have a contradiction.

Assume now that $d > 0$. If $k = e$, then t^d is the only monomial appearing in $\frac{\partial^e h(t,v)}{\partial v^e}$. Thus, replacing f by $\frac{\partial^e f}{\partial v^e}$, and dividing by the coefficient of t^d, we can assume $f = xp + sq + t^d$, where $p, q \in \Bbbk[V]$ and $d > 0$. Since $f(x, s, t, u, v) \in \ker D$, Lemma 3.3 (a) implies the element

$$\begin{aligned} g(x, t, u, v) &:= f(x, xv, t, u, v) \\ &= x\tilde{p} + xv\tilde{q} + t^d \in \Bbbk[x, t, u, v] \end{aligned} \tag{3}$$

lies in the kernel of the derivation $\Delta' := x^2\frac{\partial}{\partial v} + xv\frac{\partial}{\partial t} + t\frac{\partial}{\partial u}$ defined on $\Bbbk[x, t, u, v]$. As no monomial of the form t^k (with $k > 0$) appears in the four generators of $\ker \Delta'$ (by Lemma 3.3 (b)), the monomial t^d cannot appear as a monomial in $g \in \ker \Delta'$, and so we have a contradiction. □

In the following Lemma, we write $\Bbbk[x, v, t, u]$ rather than $\Bbbk[x, t, u, v]$, so that the derivation Δ' is triangular.

Lemma 3.3. *Define a $\Bbbk$-algebra map*

$$\begin{aligned} \phi : \Bbbk[x, s, t, u, v] &\to \Bbbk[x, v, t, u], \\ f(x, s, t, u, v) &\mapsto \phi(f)(x, v, t, u) := f(x, xv, t, u, v), \end{aligned}$$

and a derivation Δ' on $\Bbbk[x, v, t, u]$:

$$\Delta' = x^2 \frac{\partial}{\partial v} + xv \frac{\partial}{\partial t} + t \frac{\partial}{\partial u}.$$

It follows that

(a) $\Delta' \circ \phi = \phi \circ D$, *in particular, ϕ maps* $\ker D$ *to* $\ker \Delta'$;
(b) $\ker \Delta' = \Bbbk[h_1, h_2, h_3, h_4]$, *where*

$$h_1 = x, \quad h_2 = 2xt - v^2, \quad h_3 = 3x^3u - 3xvt + v^3,$$

$$\begin{aligned} h_4 &= 8xt^3 + 9x^4u^2 - 18x^2tuv - 3t^2v^2 + 6xuv^3 \\ &= (h_2^3 + h_3^2)/x^2. \end{aligned}$$

Proof. (a): For $f = f(x, s, t, u, v) \in \Bbbk[x, s, t, u, v]$, we have

$$\begin{aligned} (\Delta' \circ \phi)(f) &= (x^2 \frac{\partial}{\partial v} + xv \frac{\partial}{\partial t} + t \frac{\partial}{\partial u}) f(x, xv, t, u, v) \\ &= x^3 \phi(\frac{\partial f}{\partial s}) + x^2 \phi(\frac{\partial f}{\partial v}) + xv \phi(\frac{\partial f}{\partial t}) + t \phi(\frac{\partial f}{\partial u}) \\ &= \phi\left(x^3 \frac{\partial f}{\partial s} + x^2 \frac{\partial f}{\partial v} + s \frac{\partial f}{\partial t} + t \frac{\partial f}{\partial u} \right) = (\phi \circ D)(f). \end{aligned}$$

(b): Since Δ' is a triangular monomial derivation of a four dimensional polynomial ring, by Maubach [9], its kernel is generated by at most four elements. In fact, [9, Theorem 3.2, Case 3] gives the same generators for $\ker \Delta'$, up to multiplication by a scalar (the formula for h_4 contains a typo).

Alternatively, one can use van den Essen's Algorithm. As in the proof of Lemma 3.1, the derivation Δ' can be extended to $\Bbbk[x, v, t, u]_x$, and as $\Delta'(\frac{v}{x^2}) = 1$, the Slice Theorem [14, Proposition 2] yields

$$(\ker \Delta')_x = \mu_{-\frac{v}{x^2}} \left(\Bbbk[x, v, t, u, \tfrac{1}{x}] \right) = \Bbbk[h_1, h_2, h_3, \tfrac{1}{x}], \tag{4}$$

where μ is defined similarly as in Equation (1). Consider the additional invariant $h_4 := (h_2^3 + h_3^2)/x^2 \in \Bbbk[x, v, t, u]$. We claim $\ker \Delta' = \Bbbk[h_1, h_2, h_3, h_4] =: R$. Equation (4) implies $R \subseteq \ker \Delta' \subseteq R_x$. Next, we look at the ideal of relations modulo x between the generators of R,

$$\begin{aligned} I &:= \{P \in \Bbbk[X_1, X_2, X_3, X_4] \mid P(h_1, h_2, h_3, h_4) \in (x)\Bbbk[x, v, t, u]\} \\ &= \{P \in \Bbbk[X_1, X_2, X_3, X_4] \mid P(0, -v^2, v^3, -3t^2v^2) = 0\} \\ &= (X_1, X_2^3 + X_3^2)\Bbbk[X_1, X_2, X_3, X_4]. \end{aligned}$$

Since $(h_2^3 + h_3^2)/x = xh_4 \in R$, we have that $P(f_1, f_2, f_3, f_4)/x \in R$ for every $P \in I$, and the Kernel-check algorithm implies $\ker \Delta' = R$ (see [7, p. 184]). □

References

[1] Daniel Daigle and Gene Freudenburg. A counterexample to Hilbert's fourteenth problem in dimension 5. *J. Algebra*, 221(2):528–535, 1999.

[2] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[3] M. Domokos. Typical separating invariants. *Transform. Groups*, 12(1):49–63, 2007.

[4] Jan Draisma, Gregor Kemper, and David Wehlau. Polarization of separating invariants. *Canad. J. Math.*, 60(3):556–571, 2008.

[5] Emilie Dufresne. Separating invariants and finite reflection groups. *Adv. Math.*, 221:1979–1989, 2009.

[6] Emilie Dufresne, Jonathan Elmer, and Martin Kohls. The Cohen-Macaulay property of separating invariants of finite groups. *Transformation groups*, 2009, to appear.

[7] Gene Freudenburg. *Algebraic theory of locally nilpotent derivations*, volume 136 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2006. Invariant Theory and Algebraic Transformation Groups, VII.

[8] Gregor Kemper. Separating invariants. *Journal of Symbolic Computation*, 44(9):1212 – 1222, 2009. Effective Methods in Algebraic Geometry.

[9] 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):165–170, 2000.

[10] Stefan Maubach. Polynomial endomorphisms and kernels of derivations. *Ph.D. thesis, Univ. Nijmegen, The Netherlands*, 2003.

[11] Masayoshi Nagata. On the 14-th problem of Hilbert. *Amer. J. Math.*, 81:766–772, 1959.

[12] Müfit Sezer. Constructing modular separating invariants. *J. Algebra*. doi:10.1016/j.jalgebra.2009.07.011.

[13] Ryuji Tanimoto. On Freudenburg's counterexample to the fourteenth problem of Hilbert. *Transform. Groups*, 11(2):269–294, 2006.

[14] 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):551–555, 1993.

[15] R. Weitzenböck. Über die Invarianten von linearen Gruppen. *Acta Math.*, 58(1):231–293, 1932.

[16] Jörg Winkelmann. Invariant rings and quasiaffine quotients. *Math. Z.*, 244(1):163–174, 2003.

Mathematics Center Heidelberg (MATCH), Ruprecht-Karls-Universität Heidelberg, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany

E-mail address: emilie.dufresne@iwr.uni-heidelberg.de

Technische Universität München, Zentrum Mathematik-M11, Boltzmannstrasse 3, 85748 Garching, Germany

E-mail address: kohls@ma.tum.de