ON THE FINITE GENERATION OF ADDITIVE GROUP INVARIANTS IN POSITIVE CHARACTERISTIC

EMILIE DUFRESNE AND ANDREAS MAURISCHAT

Abstract. Roberts, Freudenburg, and Daigle and Freudenburg have given the smallest counterexamples to Hilbert's fourteenth problem as rings of invariants of algebraic groups. Each is of an action of the additive group on a finite dimensional vector space over a field of characteristic zero, and thus, each is the kernel of a locally nilpotent derivation. In positive characteristic, additive group actions correspond to locally finite iterative higher derivations. We set up characteristic-free analogs of the three examples, and show that, contrary to characteristic zero, in every positive charateristic, the invariants are finitely generated.

1. Introduction

A main topic of interest in Invariant Theory is the question of the finite generation of invariant rings. Namely, if B is a finitely generated algebra over a field $\Bbbk$, and G is a group acting on B via $\Bbbk$-algebra homomorphisms, one asks if the ring of invariants B^G is finitely generated. This is a special case of Hilbert's Fourteenth Problem. When G is a finite group, this question has a positive answer for any B (from the work of Hilbert and Noether [10, 11]). If G is an affine algebraic group acting regularly on B, then whenever G is reductive, the ring of invariants is finitely generated (cf. Nagata [9]). On the other hand, if G is not reductive, then Popov (cf. [12]) showed that there exists a finitely generated $\Bbbk$-algebra B and an action of G on B such that B^G is not finitely generated. These results are valid in arbitrary characteristic.

Consider actions on a polynomial ring $B = \Bbbk[x_1, \ldots, x_n]$ of the simplest non reductive group, the additive group $\mathbb{G}_a$. In characteristic zero, several facts are known. By the Maurer-Weitzenböck Theorem (cf. [20]), every linear action of $\mathbb{G}_a$ on B has finitely generated invariants. If $n \leq 3$, then $B^{\mathbb{G}_a}$ is finitely generated for any algebraic action (cf. [21]). In dimensions 5, 6 and 7, however, there are well-known counterexamples. For $n = 7$, Roberts (cf. [13, 3]) gave an example of a $\mathbb{G}_a$-action where $B^{\mathbb{G}_a}$ is not finitely generated (from now on refered to as (R7)). For $n = 6$ and 5, examples where constructed by Freudenburg (F6) (cf. [4]), and Daigle and Freudenburg (DF5) (cf. [1]). These three counterexamples can be used to

Date: 25th May, 2010.

2000 *Mathematics Subject Classification.* 13A50.

Key words and phrases. Hilbert's fourteenth problem, locally finite iterative higher derivations.

construct counterexamples in any dimension $n \geq 5$ (cf. [17]). The dimension 4 case is still open for general $\mathbb{G}_a$-actions. For more information on $\mathbb{G}_a$-actions in characteristic zero, we refer the reader to the excellent book of Freudenburg [5].

In positive characteristic, much less is known. It is known that $B^{\mathbb{G}_a}$ is finitely generated if $n \leq 3$ (cf. [21]), and even polynomial if $n \leq 2$ (cf. [8]). The finite generation of the invariants was also proved for special classes of linear actions of $\mathbb{G}_a$ (cf. e.g. [14], [15], [16]), but not for all linear actions. On the other hand, to the authors's knowledge, there is no example of an algebraic $\mathbb{G}_a$-action on a polynomial ring where the ring of invariants was proven not to be finitely generated.

Locally finite iterative higher derivations (lfihd) are a generalization of locally nilpotent derivations which behave well in all characteristics: an algebraic action of the additive group always corresponds to a lfihd. In this paper, we adopt this point of view, and consider the positive characteristic analogs of the counterexamples (R7), (F6), and (DF5) mentioned above. Our main result is that, contrary to characteristic zero, in every positive characteristic, the arising rings of invariants are finitely generated. For Robert's example (R7), this was done by Kurano (c.f. [6]), but not for (F6) and (DF5). Furthermore, our approach is both constructive and more elementary.

The paper is structured as follows. In Section 2, we recall some facts concerning lfihd, and set up the examples. In Section 3, we prove that the invariants are finitely generated. We use the fact that the examples are related by homomorphisms which respect the lfihd. The key of the argument is the existence of a special invariant. We deduce the existence of the special element for (F6) and (R7) from the existence of the special element for (DF5). In Section 4, we establish the existence of the special element for (DF5). Our rather technical construction is in the spirit of van den Essen's simpler proof for (DF5) in characteristic zero (cf. [19]). Finally in Section 5, we explain how our argument can be extended to more general versions of (DF5), (F6), and (R7).

Acknowledgements. We thank Florian Heiderich for giving us the idea to explore the correspondence between additive group actions and locally finite iterative higher derivations. We also thank Kazuhiko Kurano for calling our attention to his paper, and thus encouraging us to extend our argument to more general versions of (F6) and (DF5).

2. Setup of the Examples

We first review a purely algebraic description of $\mathbb{G}_a$-actions. Throughout this paper, $\Bbbk$ denotes an algebraically closed field.[1] Let B be a finitely generated $\Bbbk$-algebra. An algebraic action of $\mathbb{G}_a$ on B is uniquely determined

[1]This is not a restriction: the property of finite generation of invariants is stable under algebraic extensions of the base field.

by a $\Bbbk$-algebra homomorphism $\theta : B \to B \otimes_\Bbbk \Bbbk[U] = B[U]$, where $\Bbbk[U] \cong \Bbbk[\mathbb{G}_a]$ is the ring of regular functions on $\mathbb{G}_a$. The correspondence is given by $\sigma \cdot b = \theta(b)|_{U=\sigma}$ for all $b \in B$ and $\sigma \in \mathbb{G}_a(\Bbbk) = \Bbbk$. Any $\Bbbk$-algebra homomorphism $\theta : B \to B[U]$ defines a family of $\Bbbk$-linear maps $\left(\theta^{(n)}\right)_{n\geq 0}$ via

$$\theta(b) =: \sum_{n=0}^{\infty} \theta^{(n)}(b)U^n$$

for all $b \in B$. A family $\left(\theta^{(n)}\right)_{n\geq 0}$ (resp. θ) corresponds to a $\mathbb{G}_a$-action if and only if it fulfills the following properties (cf. [7]):

(1) $\theta^{(0)} = \mathrm{id}_B$,
(2) for all $n \geq 0$ and $a, b \in B$, one has $\theta^{(n)}(ab) = \sum_{i+j=n} \theta^{(i)}(a)\theta^{(j)}(b)$,
(3) for all $b \in B$, there is $n \geq 0$ such that $\theta^{(j)}(b) = 0$ for all $j \geq n$,
(4) for all $j, k \geq 0$ and $b \in B$, one has $\theta^{(j)}(\theta^{(k)}(b)) = \binom{j+k}{j}\theta^{(j+k)}(b)$.

Whereas Properties (2) and (3) are equivalent to θ being a $\Bbbk$-algebra homomorphism, Properties (1) and (4) ensure that θ really determines a $\mathbb{G}_a$-action. A family $\left(\theta^{(n)}\right)_{n\geq 0}$ fulfilling these properties (resp. the corresponding θ) is called a *locally finite iterative higher derivation* (lfihd) on B. Throughout this paper, we adopt the point of view of lfihd.

Note that $\theta^{(1)}$ is a derivation in the usual sense, and in characteristic zero, Property (4) implies that $\theta^{(n)} = \frac{1}{n!}(\theta^{(1)})^n$. Thus, in characteristic zero, lfihd are in one to one correspondence with those derivations which are locally nilpotent (by Property (3)). Accordingly, the $\Bbbk$-algebra $B^\theta := \{b \in B \mid \theta^{(n)}(b) = 0 \ \forall n \geq 1\}$ is often called the ring of constants of θ. Since, it coincides with the ring of invariants $B^{\mathbb{G}_a}$ of the corresponding $\mathbb{G}_a$-action, we refer to B^θ as the "ring of invariants".

In characteristic zero, (DF5), (F6) and (R7) are realized as $\Bbbk$-algebras with a locally nilpotent derivation: the counterexample of Daigle and Freudenburg (DF5) is given by

$$\Bbbk[x, s, t, u, v] \quad \text{and} \quad \theta^{(1)} = x^3\frac{\partial}{\partial s} + s\frac{\partial}{\partial t} + t\frac{\partial}{\partial u} + x^2\frac{\partial}{\partial v},$$

the counterexample of Freudenburg (F6) is given by

$$\Bbbk[x, y, s, t, u, v] \quad \text{and} \quad \theta^{(1)} = x^3\frac{\partial}{\partial s} + y^3 s\frac{\partial}{\partial t} + y^3 t\frac{\partial}{\partial u} + x^2y^2\frac{\partial}{\partial v},$$

and the counterexample of Roberts (R7) is given by

$$\Bbbk[x_1, x_2, x_3, y_1, y_2, y_3, v] \text{ and } \theta^{(1)} = x_1^3\frac{\partial}{\partial y_1} + x_2^3\frac{\partial}{\partial y_2} + x_3^3\frac{\partial}{\partial y_3} + x_1^2x_2^2x_3^2\frac{\partial}{\partial v}.$$

To obtain locally finite iterative higher derivations which make sense in all positive characteristics, we rescale the variables t and u in (DF5) and (F6) by a factor of 2 and 6, respectively. Characteristic-free formulations of the examples are therefore given by:

Daigle-Freudenburg's example (DF5):
$B_5 := \Bbbk[x, s, t, u, v]$,

$$\theta(x) = x, \qquad \theta(s) = s + x^3U,$$
$$\theta(t) = t + 2sU + x^3U^2, \qquad \theta(u) = u + 3tU + 3sU^2 + x^3U^3,$$
$$\theta(v) = v + x^2U.$$

Freudenburg's example (F6):
$B_6 := \Bbbk[x, y, s, t, u, v]$,

$$\theta(x) = x, \qquad \theta(y) = y,$$
$$\theta(s) = s + x^3U, \qquad \theta(t) = t + 2y^3sU + x^3y^3U^2,$$
$$\theta(u) = u + 3y^3tU + 3y^6sU^2 + x^3y^6U^3, \qquad \theta(v) = v + x^2y^2U.$$

Roberts's example (R7):
$B_7 := \Bbbk[x_1, x_2, x_3, y_1, y_2, y_3, v]$,

$$\theta(x_i) = x_i, \qquad \theta(y_i) = y_i + x_i^3U \quad (i = 1, 2, 3),$$
$$\theta(v) = v + x_1^2x_2^2x_3^2U.$$

On the $\Bbbk$-algebras B_5, B_6, B_7, we define gradings w_5, w_6, w_7 by assigning the following degrees:

$$w_5(x) = 1,\ w_5(s) = w_5(t) = w_5(u) = 3,\ w_5(v) = 2;$$
$$w_6(x) = w_6(y) = 1,\ w_6(s) = 3,\ w_6(t) = 6,\ w_6(u) = 9, w_6(v) = 4;$$
$$w_7(x_i) = 1,\ w_7(y_i) = 3,\ (i = 1, 2, 3),\ w_7(v) = 6.$$

With respect to these gradings, the lfihd and the corresponding $\mathbb{G}_a$-actions are homogeneous, and so the rings of invariants are graded subalgebras. This provides useful additional structure. We will also use an additional grading w_4 on B_5 which is given by:

$$w_4(x) = 0,\ w_4(s) = 1,\ w_4(t) = 2,\ w_4(u) = 3,\ w_4(v) = 1.$$

We now have the proper setup to state our main theorem:

Theorem 2.1. *In every positive characteristic, the rings of invariants B_5^θ, B_6^θ, and B_7^θ, are finitely generated.*

3. Main Results

This section presents the main steps of our argument to prove Theorem 2.1. We will make use of Theorem 4.4, which states the existence of a certain invariant in B_5. First, we describe the connection between the examples:

Lemma 3.1.

(1) *The ring B_5 is isomorphic to $B_6/(y-1)$ and the lfihd on B_5 is the lfihd induced by this isomorphism from the lfihd on B_6.*

(2) *A homomorphism $\alpha : B_6 \to B_7$ respecting the lfihd is given by:*

$$\alpha(x) = x_1, \quad \alpha(y) = x_2x_3,$$
$$\alpha(s) = y_1, \quad \alpha(t) = (x_3^3y_2 + x_2^3y_3)y_1 - x_1^3y_2y_3,$$
$$\alpha(v) = v, \quad \alpha(u) = (x_2^6y_3^2 + x_2^3x_3^3y_2y_3 + x_3^6y_2^2)y_1 - (x_3^3y_2 + x_2^3y_3)x_1^3y_2y_3$$

Proof. This can be verified by a short computation. □

Proposition 3.2. *Let $\Bbbk$ be of positive characteristic p. Then in each of B_5, B_6, and B_7, there exists a homogeneous invariant of the form $v^p + vb' - b$ such that v does not appear in b and b'.*

Proof. By Theorem 4.4, there is a w_5-homogeneous element $v^p+vb'-b \in B_5^\theta$, such that $w_4(b) = p$ and $w_4(b') = p - 1$. Since $w_5(v^p) = 2p$, we have $w_5(b) = 2p$ and $w_5(b') = 2p - 2$. Furthermore, $B_5 \cong B_6/(y - 1)$, and so we obtain a w_6-homogeneous invariant element $v^p + v\tilde{b'} - \tilde{b}$ in $B_6[\frac{1}{y}]$ by homogenizing b and b' inside $B_6[\frac{1}{y}]$, that is, by setting

$$\tilde{b} := y^{4p} \cdot b\left(\frac{x}{y}, \frac{s}{y^3}, \frac{t}{y^6}, \frac{u}{y^9}\right) \text{ and } \tilde{b'} := y^{4p-4} \cdot b'\left(\frac{x}{y}, \frac{s}{y^3}, \frac{t}{y^6}, \frac{u}{y^9}\right).$$

Denote by d_x, d_s, d_t, d_u the exponents in a monomial of b of the variables x, s, t, u, respectively. By the conditions on b, we have $2p = w_5(b) = d_x + 3d_s + 3d_t + 3d_u$, and $p = w_4(b) = d_s + 2d_t + 3d_u$. It follows that

$$d_x + 3d_s + 6d_t + 9d_u \leq d_x + 3d_s + 3d_t + 3d_u + 2d_s + 4d_t + 6d_u = 2p + 2p = 4p.$$

Hence, the exponent of y in the denominator of $b(\frac{x}{y}, \frac{s}{y^3}, \frac{t}{y^6}, \frac{u}{y^9})$ is less or equal to $4p$, and so $\tilde{b} \in B_6$. A similar argument shows that $\tilde{b'} \in B_6$. Therefore, $v^p + v\tilde{b'} - \tilde{b}$ is an invariant element in B_6.

Finally, applying the homomorphism α from Lemma 3.1 to $v^p + v\tilde{b'} - \tilde{b}$ yields an invariant of the required form in B_7. □

As the lfihd θ are triangular, their restriction induces lfihd on $A_5 = \Bbbk[x, s, t, u]$, $A_6 = \Bbbk[x, y, s, t, u]$, and $A_7 = \Bbbk[x_1, x_2, x_3, y_1, y_2, y_3]$ which are also denoted by θ.

Lemma 3.3. *The rings of invariants A_5^θ, A_6^θ, and A_7^θ are finitely generated.*

Proof. We apply the characteristic-free version (cf. [16] or [2]) of van den Essen's Algorithm (cf. [18]). We do the details for (DF5), the other examples are done similarly. Since $\theta(s) = s + x^3U$ is a polynomial of degree 1 in U with leading coefficient x^3, the invariants of the localized ring $\Bbbk[x, s, t, u, \frac{1}{x}]$ are generated by $1/x$, $\theta(x)|_{U=-s/x^3} = x$, $\theta(t)|_{U=-s/x^3} = t - s^2/x^3$, and $\theta(u)|_{U=-s/x^3} = u - 3st/x^3 + 2s^3/x^6$. Hence, $A_5^\theta = \Bbbk[x, x^3t - s^2, x^6u - 3x^3st + 2s^3, 1/x] \cap A_5$. To obtain generators for A_5^θ, we must look at the relation ideal modulo x of the generators $f_1 := x^3t - s^2$ and $f_2 := x^6u - 3x^3st + 2s^3$, that is, the preimage of the ideal (x) for the map $\pi_1 : \Bbbk[X_1, X_2] \to \Bbbk[x, x^3t -$

$s^2, x^6u - 3x^3st + 2s^3], X_1 \mapsto f_1, X_2 \mapsto f_2$. This is clearly generated by $4X_1^3 + X_2^2$, and so we obtain a new generator for $\Bbbk[x,s,t,u]^\theta$, namely

$$f_3 := \frac{1}{x^6}\pi_1(4X_1^3 + X_2^2) = x^6u^2 + 2x^3t(2t^2 - 3su) + s^2(4su - 3t^2).$$

Now consider $\pi_2 : \Bbbk[X_1, X_2, X_3] \to \Bbbk[x, f_1, f_2, f_3], X_i \mapsto f_i$, $i = 1, 2, 3$. As $\pi_2^{-1}((x)) = (4X_1^3 + X_2^2) \trianglelefteq \Bbbk[X_1, X_2, X_3]$, there are no new generators. It follows that $\Bbbk[x,s,t,u]^\theta = \Bbbk[x, f_1, f_2, f_3]$.

For the other examples, the algorithm yields:

$$A_6^\theta = \Bbbk[x, y, x^3t - y^3s^2, x^6u - 3x^3x^3st + 2y^6s^3, \\ x^6u^2 + 2x^3y^3t(2t^2 - 3su) + y^6s^2(4su - 3t^2)],$$

and

$$A_7^\theta = \Bbbk[x_1, x_2, x_3, x_1^3y_2 - x_2^3y_1, x_1^3y_3 - x_3^3y_1, x_2^3y_3 - x_3^3y_2]. \qquad \square$$

We end the section with the proof of our main theorem:

Proof of Theorem 2.1. We now show that the finite generation of the invariants modulo v (Lemma 3.3) together with the existence of an invariant of the form $v^p + vb' - b$ (Proposition 3.2) imply that the ring of invariants is finitely generated. As the argument is the same for the three examples, we write B to denote the rings B_5, B_6, and B_7, and A to denote the rings A_5, A_6, and A_7.

As $v^p + vb' - b$ is monic as a polynomial in v, for any $f \in B^\theta$, there exist unique q and r such that $f = q \cdot (v^p + vb' - b) + r$ and $\deg_v(r) < p$. As $v^p + vb' - b$ and f are invariant, the uniqueness of q and r implies $q, r \in B^\theta$. Hence, B^θ is generated by $v^p + vb' - b$ and invariants of degree less than p as polynomials in v.

For each degree $m < p$ the set

$$I_m = \{a \in A^\theta \mid a \text{ is the leading coefficient of some } f \in B^\theta,\ \deg_v(f) = m\}$$

is an ideal in A^θ, and hence finitely generated, since A^θ is Noetherian by Lemma 3.3.

Therefore, B^θ is generated by generators of A^θ, $v^p + vb' - b$, and a (finite) set of polynomials whose leading coefficients generate the ideal I_m for each $0 < m < p$. $\square$

4. The 5-dimensional Example

The purpose of this section is to construct, for the 5-dimensional example of Daigle and Freudenburg (DF5), and in each positive characteristic p, a w_5-homogeneous invariant of the form $v^p + vb' - b$, where $b, b' \in \Bbbk[x,s,t,u] \subset B_5$ and $w_4(b) = p$, $w_4(b') = p - 1$.

The proof of Theorem 4.4 requires a sequence $c_n \in \mathbb{Q}[s,t,u]$, and so we must do some work over the field $\mathbb{Q}$. We consider Example (DF5) over $\mathbb{Q}$ by taking $B := \mathbb{Q}[x,s,t,u,v]$ and letting $A := \mathbb{Q}[x,s,t,u]$ be the subalgebra of B with the induced lfihd. In turn, the lfihd θ on A induces a lfihd $\bar{\theta}$ on the

quotient $C := A/(x-1) \cong \mathbb{Q}[s,t,u]$ via $\bar{\theta}(\bar{f}) := \overline{\theta(f)}$. The ring of invariants is $C^{\bar{\theta}} = \mathbb{Q}[t_1, u_1]$, where $t_1 = t - s^2$, and $u_1 = u - 3st + 2s^3$. The grading w_4 on B induces a grading on C which is also denoted by w_4.

Proposition 4.1. *Let $e : \mathbb{N} \to \mathbb{N}$ be given by $e(n) := \left\lfloor \frac{2n}{3} \right\rfloor$. There exist sequences of w_4-homogeneous polynomials $(h_n)_{n\in\mathbb{N}}$ in $C^{\bar{\theta}}$ and $(c_n)_{n\in\mathbb{N}}$ in C such that $h_0 = 1$, $h_1 = 0$,*

$$c_n := \sum_{i=0}^{n} \binom{n}{i} h_{n-i} s^i \in \mathbb{Q}[s,t,u] \text{ for all } n \geq 0,$$

and for all $n \geq 2$, the element c_n has degree $\deg(c_n) \leq e(n)$ with respect to the standard grading $\deg$ on $\mathbb{Q}[s,t,u]$. Furthermore, for all primes p, the coefficients of $h_0, h_1, \ldots, h_{p-2}$ and h_p are in the local ring $\mathbb{Z}_{(p)}$, and the coefficients of h_{p-1} are in $\frac{1}{p}\mathbb{Z}_{(p)}$.

Remark 4.2. For all $k, n \in \mathbb{N}$, the sequence $(c_n)_{n\in\mathbb{N}}$ satisfies $\bar{\theta}^{(k)}(c_n) = \binom{n}{k} c_{n-k}$. Indeed, we have

$$\begin{aligned} \bar{\theta}^{(k)}(c_n) &= \sum_{i=0}^{n} \binom{n}{i} h_{n-i} \binom{i}{k} s^{i-k} = \sum_{j=0}^{n-k} \binom{n}{j+k} h_{n-k-j} \binom{j+k}{k} s^j \\ &= \sum_{j=0}^{n-k} \binom{n}{k} \binom{n-k}{j} h_{n-k-j} s^j = \binom{n}{k} c_{n-k}. \end{aligned}$$

Proof of Proposition 4.1. Let $C = \bigoplus_{n\geq 0} C_n$ be the decomposition of C into homogeneous parts with respect to the grading w_4. For $n \geq k$, we have $\bar{\theta}^{(k)}(C_n) \subseteq C_{n-k}$.

We will show by induction on n that we can construct such sequences h_n and c_n so that $h_n, c_n \in C_n$. To satisfy the conditions on the coefficients of the h_n's, it suffices to ensure that the denominators of the coefficients of each h_n are only divisible by primes less than n, unless $n+1$ is a prime congruent to 1 modulo 6, in which case $n+1$ may also occur. When $n \equiv 2, 3, 4, 5 \mod 6$, we explain how to obtain h_n from $\{h_j \mid 0 \leq j \leq n-1\}$. The cases $n \equiv 0 \mod 6$ and $n \equiv 1 \mod 6$ must be constructed in one step, that is, when $n \equiv 1 \mod 6$, we show that we can construct h_{n-1} and h_n from $\{h_j \mid 0 \leq j \leq n-2\}$.

Assume that $n \equiv 2, 3, 4, 5 \mod 6$, and that we already have $\{h_j \in C_j \mid 0 \leq j \leq n-1\}$ such that the denominators of the coefficients of each h_j are only divisible by primes smaller than n. By the induction hypothesis, c_{n-1} has standard degree at most $e(n-1)$ for $n > 2$, and at most $e(2) = 1$ for $n = 2$, that is, at most $e(n)$ in all cases. Additionally, c_{n-1} is w_4-homogeneous of w_4-degree $n-1$. The same computation as in Remark 4.2 shows that $c := \sum_{i=1}^{n} \binom{n}{i} h_{n-i} s^i \in \mathbb{Q}[s,t,u]$ satisfies $\bar{\theta}^{(1)}(c) = n c_{n-1}$. Thus, it will suffice to find $h_n \in \mathbb{Q}[s,t,u]^{\bar{\theta}}$ such that $\deg(c + h_n) \leq e(n)$.

Taking

$$c = \sum_{i+2j+3k=n} \alpha_{i,j,k} s^i t^j u^k,$$

where $\alpha_{i,j,k} \in \mathbb{Q}$, one gets

$$\bar{\theta}^{(1)}(c) = \sum_{i+2j+3k=n} \alpha_{i,j,k} \left(i s^{i-1} t^j u^k + 2j s^{i+1} t^{j-1} u^k + 3k s^i t^{j+1} u^{k-1} \right)$$

$$= \sum_{i+2j+3k=n} \big((i+2)\alpha_{i+2,j-1,k} + 2j\alpha_{i,j,k} + 3(k+1)\alpha_{i+1,j-2,k+1} \big) s^{i+1} t^{j-1} u^k,$$

where $\alpha_{i',j',k'} := 0$ if $i' < 0$ or $j' < 0$. Since $\deg\left(\bar{\theta}^{(1)}(c)\right) \leq e(n)$, we have

$$(i+2)\alpha_{i+2,j-1,k} + 2j\alpha_{i,j,k} + 3(k+1)\alpha_{i+1,j-2,k+1} = 0,$$

whenever $i+2j+3k = n$ and $i+j+k \geq e(n)+1$. Hence, each $\alpha_{i,j,k}$ is a linear combination of certain $\alpha_{i',j',k'}$'s such that $j' < j$ and $i'+j'+k' \geq i+j+k$. Thus, if $i+j+k \geq e(n)+1$, then $\alpha_{i,j,k}$ is a linear combination of the $\alpha_{i',j',k'}$'s such that $j' = 0$ and $i'+k' \geq e(n)+1$. Therefore, it suffices to prove that there exists $h \in C^{\bar{\theta}}$, homogeneous of w_4-degree n, such that, for all i, k such that $i+3k = n$ and $i+k \geq e(n)+1$, the coefficient of $s^i u^k$ in h is equal to the coefficient of $s^i u^k$ in c. We then take $h_n = -h$ (note that h trivially satisfies $\deg\left(\bar{\theta}^{(1)}(h)\right) \leq e(n)$, since it is invariant, and so its coefficients satisfy the same linear relations).

The "relevant" $s^i u^k$ are those where $i+3k = n$ and $i+k \geq e(n)+1$, that is, where $0 \leq k \leq \left\lfloor \frac{n-e(n)-1}{2} \right\rfloor = \left\lfloor \frac{n-1}{6} \right\rfloor$. For short, we write $d := \left\lfloor \frac{n-1}{6} \right\rfloor$ to denote the maximum value k of a relevant $s^i u^k$.

By our assumption, h is a linear combination of "monomials" of the form $(-t_1)^l u_1^m$ such that $2l+3m = n$, that is, such that $m \in \left[0, \lfloor \frac{n}{3} \rfloor\right]$, $m \equiv n \mod 2$, and $l = \frac{n-3m}{2}$. Thus, for n odd, we have $m = 2m'+1$, where $0 \leq m' \leq \lfloor \frac{n-3}{6} \rfloor$, and for n even, we have $m = 2m'$ where $0 \leq m' \leq \lfloor \frac{n}{6} \rfloor$. The coefficient of $s^i u^k$ in $(-t_1)^l u_1^m = (s^2-t)^l (u - 3st + 2s^3)^m$ is $\binom{m}{k} 2^{m-k}$.

Thus, if $n \equiv 2, 3, 4$ or $5 \mod 6$, the number of admissible "monomials" in h is $d+1$. Therefore, the coefficient vector $(x_0, \ldots, x_d)^T$ of h is the solution of the system of linear equations $Mx = \alpha$, where $\alpha = (\alpha_{n,0,0}, \ldots, \alpha_{n-3d,0,d})^T$, and $M = (a_{k,m'})_{0 \leq k,m' \leq d}$ is the matrix given by $a_{k,m'} = \binom{2m'+1}{k} 2^{2m'+1-k}$, if n is odd, and by $a_{k,m'} = \binom{2m'}{k} 2^{2m'-k}$, if n is even.

By Lemma 4.3, M is invertible over $\mathbb{Z}[\frac{1}{2}]$ in both cases. Thus, the system of equations has a unique solution, and the primes which might occur in the denominators of the coefficients of h are 2 and the primes occuring in the denominators of the coefficients of some h_j $(0 \leq j \leq n-1)$. For $n = 2$, an explicit computation gives $h_2 = t_1$.

If $n \equiv 1 \mod 6$, the number of coefficients of h is less than d, which might lead to an unsolvable linear equation. Hence, we cannot use the exact same argument. We construct h_{n-1} and h_n in one step. Again by induction,

we may assume that the denominators of the coefficients of $h_0, \dots, h_{n-2}$ are only divisible by primes less than $n-1$.

We want $h_{n-1} = \sum_{m'=0}^{d} x_{m'}(-t_1)^l u_1^{2m'}$ and $h_n = \sum_{m'=0}^{d-1} y_{m'}(-t_1)^l u_1^{2m'+1}$ such that adding h_{n-1} to $\sum_{i=2}^{n} \binom{n-1}{i-1} h_{n-i} s^{i-1}$ cancels out the coefficient vector α of $\{s^{n-1}, s^{n-4}u, \dots, s^{n-3d+2}u^{d-1}\}$, and such that adding $h_n + n h_{n-1} s$ to $\sum_{i=2}^{n} \binom{n}{i} h_{n-i} s^i$ cancels out the coefficient vector β of $\{s^n, s^{n-3}u, \dots, s^{n-3d}u^d\}$. Thus, we must solve $Mx = -\alpha$ and $Ny + nLx = -\beta$, where

$$
\begin{aligned}
&M \in \mathrm{Mat}(d \times (d+1)), && M_{k,m'} = \binom{2m'}{k} 2^{2m'-k},\\
&N \in \mathrm{Mat}((d+1) \times d), && N_{k,m'} = \binom{2m'+1}{k} 2^{2m'+1-k},\\
&L \in \mathrm{Mat}((d+1) \times (d+1)), && L_{k,m'} = \binom{2m'}{k} 2^{2m'-k}.
\end{aligned}
$$

Since L is invertible (Lemma 4.3), the two equations are equivalent to

$$
x = -\frac{1}{n} L^{-1}(\beta + Ny) \quad \text{and} \quad ML^{-1}Ny = -ML^{-1}\beta + n\alpha.
$$

As $ML^{-1}N$ is the $d \times d$ matrix with entries $\binom{2m'+1}{k} 2^{2m'+1-k}$, by Lemma 4.3, it is invertible.

Therefore, we can find unique vectors x and y. From the equations giving x and y, we deduce that the denominators of the entries of y are only divisible by primes less than $n-1$, and if n is prime, the denominators of the entries of x may have the additional prime factor n. □

Lemma 4.3. *Let $d \in \mathbb{N}$. If $M_e, M_o \in \mathrm{Mat}((d+1) \times (d+1), \mathbb{Z})$ are given by*

$$
(M_e)_{k,m} := \binom{2m}{k} 2^{2m-k} \quad \textit{and} \quad (M_o)_{k,m} := \binom{2m+1}{k} 2^{2m+1-k}
$$

for all $k, m = 0, \dots, d$, then $\det(M_e) = 2^{d(d+1)}$, and $\det(M_o) = 2^{(d+1)^2}$.

Proof. If $x_0, \dots, x_d$ are indeterminates, denote by $V(x_0, \dots, x_d)$ the Vandermonde matrix

$$
V(x_0, \dots, x_d) = \begin{pmatrix} 1 & x_0 & \dots & x_0^d \\ 1 & x_1 & \dots & x_1^d \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_d & \dots & x_d^d \end{pmatrix}.
$$

By definition of the binomial coefficients, we have

$$
V(x_0, \dots, x_d) \cdot M_e \equiv V((2+x_0)^2, \dots, (2+x_d)^2) \mod (x_0^{d+1}, \dots, x_d^{d+1}),
$$

and therefore their determinants are also congruent modulo $(x_0^{d+1}, \ldots, x_d^{d+1})$. Since $\det\left(V(x_0, \ldots, x_d)\right) = \prod_{j>i}(x_j - x_i)$, and

$$\begin{aligned}\det\left(V((2+x_0)^2, \ldots, (2+x_d)^2)\right) &= \prod_{j>i}\left((2+x_j)^2 - (2+x_i)^2\right) \\ &= \prod_{j>i}(x_j - x_i)\prod_{j>i}(4 + x_j + x_i),\end{aligned}$$

we obtain

$$\prod_{j>i}(x_j - x_i) \cdot \left[\det(M_e) - \prod_{j>i}(4 + x_j + x_i)\right] \equiv 0 \mod (x_0^{d+1}, \ldots, x_d^{d+1}).$$

This implies that the coefficient of $x_1 x_2^2 \cdots x_d^d$ of the left hand side, namely $\det(M_e) - \prod_{j>i} 4$, has to vanish. Hence, $\det(M_e) = 2^{d(d+1)}$.

A similar argument proves the statement about M_o. The key is to recognize that $V(x_0, \ldots, x_d) \cdot M_o$ is congruent to

$$\begin{pmatrix} 2+x_0 & (2+x_0)^3 & \ldots & (2+x_0)^{2d+1} \\ 2+x_1 & (2+x_1)^3 & \ldots & (2+x_1)^{2d+1} \\ \vdots & \vdots & \ddots & \vdots \\ 2+x_d & (2+x_d)^3 & \ldots & (2+x_d)^{2d+1} \end{pmatrix}$$

modulo $(x_0^{d+1}, \ldots, x_d^{d+1})$, and that this matrix has determinant equal to $\prod_{l=0}^{d}(2+x_l) \cdot \det\left(V((2+x_0)^2, \ldots, (2+x_d)^2)\right)$. □

We are now prepared to prove the existence of the special invariant.

Theorem 4.4. *Let $\Bbbk$ be of positive characteristic p, and let (B_5, θ) be as in Example (DF5) over $\Bbbk$.*
There exists a w_5-homogeneous invariant in B_5 of the form $v^p + vb' - b$, where $b', b \in \Bbbk[x, s, t, u] \subset B_5$ have w_4-degree $w_4(b) = p$ and $w_4(b') = p - 1$.

Proof. If suffices to find $b, b' \in \Bbbk[x, s, t, u]$ such that $\theta(b) = b + x^2 b' U + x^{2p} U^p$. Indeed, this implies $\theta(b') = b'$, and

$$\begin{aligned}\theta(v^p + vb' - b) &= \theta(v)^p + \theta(v)\theta(b') - \theta(b) \\ &= (v + x^2 U)^p + (v + x^2 U)b' - (b + x^2 b' U + x^{2p} U^p) = v^p + vb' - b.\end{aligned}$$

Let $\mathcal{O} := \mathbb{W}(\Bbbk)$ be the Witt ring of $\Bbbk$, and let $\mathbb{K}$ be the field of fractions of $\mathcal{O}$. Hence $\mathbb{K}$ is a discrete valued field of unequal characteristic with valuation ring $\mathcal{O}$, valuation ideal (p) and residue class field $\Bbbk$. Example (DF5) over $\mathbb{K}$ has a lfihd which restricts to $\mathcal{O}[x, s, t, u, v]$. Reduction modulo p then leads to Example (DF5) over $\Bbbk$. Thus, to obtain $b, b' \in \Bbbk[x, s, t, u]$ such that $\theta(b) = b + x^2 b' U + x^{2p} U^p$, it suffices to find $\tilde{b}, \tilde{b}' \in \mathcal{O}[x, s, t, u] \subseteq \mathbb{K}[x, s, t, u]$ such that $\theta(\tilde{b}) \equiv \tilde{b} + x^2 \tilde{b}' U + x^{2p} U^p \mod p$.

Let $(c_n)_{n\in\mathbb{N}} \subset \mathbb{Q}[s,t,u] \subseteq \mathbb{K}[s,t,u]$ be the sequence constructed in Proposition 4.1. Set

$$b_n := x^{2p} c_n(\frac{s}{x^3}, \frac{t}{x^3}, \frac{u}{x^3}) \text{ for } 0 \leq n \leq p,$$

that is, b_n is the homogenization of c_n of degree $2p$ with respect to the grading w_5. By construction of c_n, the elements b_n are indeed in $\mathbb{K}[x,s,t,u]$ and have coefficients in $\mathbb{Z}_{(p)} \subseteq \mathcal{O}$ resp. $\frac{1}{p}\mathbb{Z}_{(p)}$ for $n = p-1$. Moreover, we have $b_0 = x^{2p}$, and if $p > 2$, x^2 divides b_{p-1}. A similar calculation as in Remark 4.2 shows that $\theta^{(k)}(b_p) = \binom{p}{k} b_{p-k}$ for all $0 \leq k \leq p$, and $\theta^{(k)}(b_p) = 0$ for $k > p$. Hence, if $p = 2$, $\theta(b_2) = b_2 + x^4U^2 \mod 2$, and otherwise, $\theta(b_p) \equiv b_p + x^2\left(\frac{pb_{p-1}}{x^2}\right)U + x^{2p}U^p \mod p$, as desired. □

5. Generalized Form of the Examples

In this section we explain how the arguments of Sections 3 and 4 can be adapted to generalized forms of examples (R7), (F6), and (DF5). We start by writing down these general forms. In characteristic zero, these generalizations are discussed in Section 7.2.3 of Freudenburg's book (c.f. [5]). Note that the version of (R7) presented here is the original version. Let $m \geq 2$ be an integer.

Generalized Daigle-Freudenburg's example (DF5-m):
$B_5 := \Bbbk[x,s,t,u,v]$,

$$\theta(x) = x, \qquad \theta(s) = s + x^{m+1}U,$$
$$\theta(t) = t + 2sU + x^{m+1}U^2, \qquad \theta(u) = u + 3tU + 3sU^2 + x^{m+1}U^3,$$
$$\theta(v) = v + x^mU.$$

Generalized Freudenburg's example (F6-m):
$B_6 := \Bbbk[x,y,s,t,u,v]$,

$$\theta(x) = x, \qquad \theta(t) = t + 2y^{m+1}sU + x^{m+1}y^{m+1}U^2,$$
$$\theta(y) = y, \qquad \theta(u) = u + 3y^{m+1}tU + 3y^{2(m+1)}sU^2 + x^{m+1}y^{2(m+1)}U^3,$$
$$\theta(s) = s + x^{m+1}U, \quad \theta(v) = v + x^my^mU.$$

Generalized Roberts's example (R7-m):
$B_7 := \Bbbk[x_1,x_2,x_3,y_1,y_2,y_3,v]$,

$$\theta(x_i) = x_i, \qquad \theta(y_i) = y_i + x_i^{m+1}U \quad (i = 1,2,3),$$
$$\theta(v) = v + x_1^mx_2^mx_3^mU.$$

On the $\Bbbk$-algebras B_5, B_6, B_7, we define gradings w_5, w_6, w_7 by assigning the following degrees:

$$w_5(x) = 1,\ w_5(s) = w_5(t) = w_5(u) = m+1,\ w_5(v) = m;$$
$$w_6(x) = w_6(y) = 1,\ w_6(s) = m+1,\ w_6(t) = 2(m+1),$$
$$w_6(u) = 3(m+1), w_6(v) = 2m;$$
$$w_7(x_i) = 1,\ w_7(y_i) = m+1,\ (i = 1,2,3),\ w_7(v) = 3m.$$

With respect to these gradings, the lfihd and the corresponding $\mathbb{G}_a$-actions are homogeneous, and so the rings of invariants are graded subalgebras. We will also use an additional grading w_4 on B_5 which is given by:

$$w_4(x) = 0,\ w_4(s) = 1,\ w_4(t) = 2,\ w_4(u) = 3,\ w_4(v) = 1.$$

Proposition 5.1. *In each of B_5, B_6, and B_7, there exists a homogeneous invariant of the form $v^p + vb' - b$ such that v does not appear in b and b'.*

Proof. A short computation verifies that there exists similar relationship between the generalized examples as establish in Lemma 3.1. Namely, the ring B_5 is isomorphic to $B_6/(y-1)$ and the lfihd on B_5 is the lfihd induced by this isomorphism from the lfihd on B_6, and a homomorphism $\alpha_m : B_6 \to B_7$ respecting the lfihd is given by:

$$\begin{aligned}
&\alpha(x) = x_1, \quad \alpha(y) = x_2x_3, && \alpha(s) = y_1,\\
&\alpha(t) = (x_3^{m+1}y_2 + x_2^{m+1}y_3)y_1 - x_1^{m+1}y_2y_3, && \alpha(v) = v,\\
&\alpha(u) = (x_2^{2(m+1)}y_3^2 + x_2^{m+1}x_3^{m+1}y_2y_3 + x_3^{2(m+1)}y_2^2)y_1 - (x_3^{m+1}y_2 + x_2^{m+1}y_3)x_1^{m+1}y_2y_3
\end{aligned}$$

As in Proposition 3.2, we construct the special invariant for Example (DF5-m), and then the relationships described above yields the special invariants for the two other examples.

To construct the special invariant for (DF5-m), it suffices as in Theorem 4.4 to find $b, b' \in \Bbbk[x, s, t, u]$ such that $\theta(b) = b + x^m b'U + x^{mp}U^p$. Similarly, it suffices to find $\tilde{b}, \tilde{b}' \in \mathcal{O}[x, s, t, u] \subseteq \mathbb{K}[x, s, t, u]$ such that $\theta(\tilde{b}) \equiv \tilde{b} + x^m\tilde{b}'U + x^{mp}U^p \mod p$. Let $(c_n)_{n\in\mathbb{N}} \subset \mathbb{Q}[s, t, u] \subseteq \mathbb{K}[s, t, u]$ be the sequence constructed in Proposition 4.1. Set

$$b_n := x^{mp}c_n(\frac{s}{x^{m+1}}, \frac{t}{x^{m+1}}, \frac{u}{x^{m+1}}) \text{ for } 0 \le n \le p,$$

that is, b_n is the homogenization of c_n of degree mp with respect to the grading w_5. By construction of c_n, the elements b_n are indeed in $\mathbb{K}[x, s, t, u]$ and have coefficients in $\mathbb{Z}_{(p)} \subseteq \mathcal{O}$ resp. $\frac{1}{p}\mathbb{Z}_{(p)}$ for $n = p - 1$. Moreover, we have $b_0 = x^{mp}$, and if $p > 2$, x^m divides b_{p-1}. A similar calculation as in Remark 4.2 shows that $\theta^{(k)}(b_p) = \binom{p}{k}b_{p-k}$ for all $0 \le k \le p$, and $\theta^{(k)}(b_p) = 0$ for $k > p$. Hence, if $p = 2$, $\theta(b_2) = b_2 + x^{2m}U^2 \mod 2$, and otherwise, $\theta(b_p) \equiv b_p + x^m\left(\frac{pb_{p-1}}{x^m}\right)U + x^{mp}U^p \mod p$, as desired.

□

This finally leads to the generalized version of our main theorem:

Theorem 5.2. *In every positive characteristic, the rings of invariants B_5^θ, B_6^θ, and B_7^θ, are finitely generated.*

Proof. The argument is as in the proof of Theorem 2.1. Again, the $\Bbbk$-algebra A (that is, A_5, A_6 and A_7) is finitely generated, and the finite generation of B^θ then follows from the special invariant established by Proposition 5.1. □

Remark 5.3.

(1) For (R7-m), our argument has the additional advantage of providing a somewhat simpler proof than Kurano's, admittedly more general, argument (c.f. [6]). Moreover, our proof constructs an invariant which is monic of degree p as a polynomial in v, where Kurano proves only the existence of some invariant monic as a polynomial in v.

(2) In Section 7.2.3 of his book (c.f. [5]), Freudenburg explains how (DF5-m) is really (R7-m) with all the symmetries removed. Precisely he proves that B_5^θ is equal to the ring of invariants of B_7^θ under the action of a reductive group. In characteristic zero, this automatically implies that B_5^θ is not finitely generated. Freudenburg's argument concerning the relationship between B_7^θ and B_5^θ remains valid in positive characteristic, and so the finite generation of B_7^θ implies the finite generation of B_5^θ. In characteristic zero, since B_6^θ surjects onto B_5^θ, it follows that B_6^θ is also not finitely generated. It appears that, in positive characteristic, the use of our constructive argument is unavoidable to prove the finite generation of B_6^θ.

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. Computing Invariants of Algebraic Groups in Arbitrary Characteristic. *Adv. Math.*, 217(5):2089–2129, 2008.

[3] James K. Deveney and David R. Finston. G_a actions on $\mathbf{C}^3$ and $\mathbf{C}^7$. *Comm. Algebra*, 22(15):6295–6302, 1994.

[4] Gene Freudenburg. A counterexample to Hilbert's fourteenth problem in dimension six. *Transform. Groups*, 5(1):61–71, 2000.

[5] Gene Freudenburg. *Algebraic Theory of Locally Nilpotent Derivations*. Encyclopaedia of Mathematical Sciences. Springer, Berlin Heidelberg, 2006.

[6] Kazuhiko Kurano. Positive characteristic finite generation of symbolic Rees algebras and Roberts' counterexamples to the fourteenth problem of Hilbert. *Tokyo J. Math.*, 16(2):473–496, 1993.

[7] Masayoshi Miyanishi. A remark on an iterative infinite higher derivation. *J. Math. Kyoto Univ.*, 8:411–415, 1968.

[8] Masayoshi Miyanishi. G_a-action of the affine plane. *Nagoya Math. J.*, 41:97–100, 1971.

[9] Masayoshi Nagata. Invariants of a group in an affine ring. *J. Math. Kyoto Univ.*, 3:369–377, 1963/1964.

[10] Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77(1):89–92, 1916.

[11] Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Chracteristic p. *Nachr. Gött. Ges. Wissensch.*, pages 28–35, 1926.

[12] V. L. Popov. On Hilbert's theorem on invariants. *Dokl. Akad. Nauk SSSR*, 249(3):551–555, 1979.

[13] 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):461–473, 1990.

[14] C. S. Seshadri. On a theorem of Weitzenböck in invariant theory. *J. Math. Kyoto Univ.*, 1:403–409, 1961/1962.

[15] Ryuji Tanimoto. On the polynomiality of invariant rings for codimension one $\mathbb{G}_a$-modules. *J. Algebra*, 305(2):1084–1092, 2006.
[16] Ryuji Tanimoto. An algorithm for computing the kernel of a locally finite iterative higher derivation. *J. Pure Appl. Algebra*, 212(10):2284–2297, 2008.
[17] A. van den Essen and T. Janssen. Kernels of elementary derivations. Technical Report 9548, Dept. of Mathematics, Univ. Nijmegen, The Netherlands, 1995.
[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):551–555, 1993.
[19] Arno van den Essen. A simple solution of Hilbert's fourteenth problem in dimension five. *Colloq. Math.*, 105(1):167–170, 2006.
[20] R. Weitzenböck. Über die Invarianten von linearen Gruppen. *Acta Math.*, 58(1):231–293, 1932.
[21] O. Zariski. Interprétations algébrico-géométriques du quatorzième problème de Hilbert. *Bull. Sci. Math. (2)*, 78:155–168, 1954.

Emilie Dufresne, Mathematics Center of Heidelberg (MATCH), Heidelberg University, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail address: emilie.dufresne@iwr.uni-heidelberg.de

Andreas Maurischat, Interdisciplinary Center for Scientific Computing (IWR), Heidelberg University, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail address: andreas.maurischat@iwr.uni-heidelberg.de