THE SEPARATING VARIETY FOR THE BASIC REPRESENTATIONS OF THE ADDITIVE GROUP

EMILIE DUFRESNE AND MARTIN KOHLS

Abstract. For a group G acting on an affine variety X, the separating variety is the closed subvariety of $X \times X$ encoding which points of X are separated by invariants. We concentrate on the indecomposable rational linear representations V_n of dimension $n+1$ of the additive group of a field of characteristic zero, and decompose the separating variety into the union of irreducible components. We show that if n is odd, divisible by four, or equal to two, the closure of the graph of the action, which has dimension $n+2$, is the only component of the separating variety. In the remaining cases, there is a second irreducible component of dimension $n+1$. We conclude that in these cases, there are no polynomial separating algebras.

1. Introduction

Let $\Bbbk$ be an algebraically closed field and let G be an algebraic group acting rationally on an irreducible affine variety X. This action induces an action on $\Bbbk[X]$, the ring of regular functions on X, via $(\sigma * f)(u) = f(\sigma^{-1} * u)$. The *ring of invariants* is the subalgebra $\Bbbk[X]^G \subseteq \Bbbk[X]$ formed by the elements fixed by G, or equivalently, the subalgebra formed by the elements of $\Bbbk[X]$ which are constant on the orbits. Thus, for $x, y \in X$ and $f \in \Bbbk[X]^G$, having $f(x) \neq f(y)$ implies that x and y belong to distinct orbits. In this situation, we say that the invariant f *separates* x and y. A *separating set* is a set of invariants which separate any two points which are separated by some invariant (see [5, Definition 2.3.8]).

The *separating variety*

$$\mathcal{S}_G := \{(x, y) \in X \times X \mid f(x) = f(y) \text{ for all } f \in \Bbbk[X]^G\}$$

provides an alternate characterization of separating sets. Namely, if $\delta : \Bbbk[X] \to \Bbbk[X] \times \Bbbk[X]$ is the map defined by $\delta(f) := f \otimes 1 - 1 \otimes f$, then $E \subseteq \Bbbk[X]^G$ is a separating set if and only if $\mathcal{V}_{X\times X}(\delta(E)) = \mathcal{S}_G = \mathcal{V}_{X\times X}(\delta(\Bbbk[X]^G))$, where $\mathcal{V}$ denotes the common zero set of a set

Date: December 21, 2011.

1991 *Mathematics Subject Classification.* 13A50,14L30.

Key words and phrases. Invariant Theory, separating invariants, locally nilpotent derivations, basic actions, Weitzenböck derivation.

of polynomials. The separating variety encodes which points can be separated using invariants. In the case of finite groups, the invariants separate the orbits, and so the separating variety is in fact equal to the *graph* of the G-action:

$$\Gamma_G := \{(x, \sigma \cdot x)) \in X \times X \mid x \in X,\ \sigma \in G\}.$$

This played a central role in the first author's proof that, when X is a vector space on which a finite group G acts linearly, if there exists a polynomial separating algebra, then the action of G on X must be generated by reflections (see [7, Theorem 1.1]).

The graph consists of those pairs of points which belong to the same orbit, while the separating variety consists of the pairs of points which can not be separated by invariants. Thus, we always have $\Gamma_G \subseteq \mathcal{S}_G$. Moreover, as $\mathcal{S}_G$ is Zariski-closed, we also have $\overline{\Gamma_G} \subseteq \mathcal{S}_G$. Even for reductive groups, however, this inclusion can be strict (see [15, Example 2.1]). The invariants may not always separate orbits (as for the natural action of the multiplicative group of an infinite field on a vector space), but in the case of reductive groups, they do separate disjoint orbit closures (see [17, Corollary 3.5.2]). Exploiting this, Kemper gives an algorithm to compute the separating variety and then a separating set (see [15, Algorithm 2.9]), which is the first step in his algorithm to compute the invariants of reductive groups in arbitrary characteristic (see [15, Algorithm 1.9]).

The motivation for this paper is to better understand the separating variety in the case of non-reductive groups. We concentrate on what is perhaps the simplest situation: algebraic actions of the additive group $\mathbb{G}_a = (\Bbbk, +)$ on an irreducible affine variety X (we will concentrate on vector spaces), where $\Bbbk$ is a field of characteristic zero.

Actions of the additive group on X are in one to one correspondence with locally nilpotent derivations (abbreviated LND) on $\Bbbk[X]$. Recall that a *locally nilpotent derivation* D is a linear map $\Bbbk[X] \to \Bbbk[X]$ such that $D(ab) = aD(b) + bD(a)$ for all $a, b \in \Bbbk[X]$ and, for all $a \in \Bbbk[X]$, there exists an $m \geq 1$ such that $D^m(a) = 0$. A locally nilpotent derivation D on $\Bbbk[X]$ induces an action $* : \mathbb{G}_a \times \Bbbk[X] \to \Bbbk[X]$ via

$$(-t) * f := \exp(tD)f = \sum_{k=0}^{\infty} \frac{t^k}{k!} D^k(f) \text{ for } t \in \mathbb{G}_a,\ f \in \Bbbk[X].$$

The invariant ring $\Bbbk[X]^{\mathbb{G}_a}$ coincides with the kernel of D and is denoted by $\Bbbk[X]^D$. We write $\mathcal{S}_D = \mathcal{S}_{\mathbb{G}_a}$ to denote the separating variety corresponding to the action induced by the locally nilpotent derivation D, and Γ_D to denote the graph of the corresponding $\mathbb{G}_a$-action.

An important contribution of the LND approach is van den Essen's algorithm to compute the kernel of a LND, and thus the invariants of a $\mathbb{G}_a$-action (see [19]). An element $s \in \Bbbk[X]$ such that $Ds \neq 0$ and $D^2 s = 0$ is a *local slice*. By the Slice Theorem (which is in fact the first step of the algorithm, see [19, Section 3]), for a local slice s and any $f \in \Bbbk[X]$, the element $\pi(f) := \exp(tD)f|_{t:=-s/Ds}$ is in $\Bbbk[X]^D_{Ds}$, and the algebra homomorphism π maps $\Bbbk[X]$ onto $\Bbbk[X]^D_{Ds}$. We are particularly interested in the *plinth ideal* $\mathrm{pl}(D)$, that is, the ideal of $\Bbbk[X]^D$ formed by the images Ds of all local slices s together with zero.

In Section 2, we first observe that outside the zero set of any subset of $\mathrm{pl}(D)$, the invariants separate the orbits (Proposition 2.1). This leads to a rather rough description of the separating variety (Proposition 2.2): apart from the graph, the separating variety is determined by the restrictions of the invariants on the zero set of elements of $\mathrm{pl}(D)$. The last of our results on arbitrary $\mathbb{G}_a$-actions is that if there is a polynomial separating algebra, then the separating variety has no irreducible component of dimension less than $\dim X + 1 = \dim \overline{\Gamma_G}$ (Proposition 2.6).

In Section 3, we focus further on the basic actions of the additive group, that is, the finite dimensional indecomposable rational linear representations of $\mathbb{G}_a$. We use the separating set constructed in [11] to compute the separating variety and write it as the union of irreducible components (Theorem 3.2). We find that for n odd, divisible by four, or equal to two, there is exactly one irreducible component: the closure of the graph. On the other hand, for $n > 2$ even, but not divisible by four, we find a second component. This component has smaller dimension than the graph, which leads us to the conclusion that there can not be polynomial separating algebras (Corollary 3.3).

Section 4 contains the technical details for the proof of the key result of Section 3.

Acknowledgements. We thank Hanspeter Kraft and Gregor Kemper for their hospitality during academic visits between the two authors.

2. Separation properties of invariants

Before we specialize to the basic actions of the additive group, we present some general results on separating properties of invariants of additive group actions.

Proposition 2.1. *If $S \subseteq \sqrt{\mathrm{pl}(D)\Bbbk[X]}$, then the invariants separate orbits outside $\mathcal{V}_X(S)$, that is,*

$$\mathcal{S}_D \setminus (\mathcal{V}_X(S) \times \mathcal{V}_X(S)) \subseteq \Gamma_D.$$

Proof. We may assume that $S \subseteq \mathrm{pl}(D)$. Suppose $x, y \in X \setminus \mathcal{V}_X(S)$ are not separated by any invariant, that is, $f(x) = f(y)$ for all $f \in \Bbbk[X]^D$. By our assumptions, there exist $f \in S$ and $s \in \Bbbk[X]$ such that $f = D(s)$ and $f(x) = f(y) \neq 0$. Set $t_x = s(x)/f(x) \in \mathbb{G}_a$ and $t_y = s(y)/f(y) \in \mathbb{G}_a$. Suppose $\Bbbk[X] = \Bbbk[a_1, \dots, a_n]$. For each a_i, we have

$$\begin{aligned} a_i((-t_x)*x) &= (t_x * a_i)(x) = \left(\sum_{k=0}^{\infty} \tfrac{(-t_x)^k}{k!} D^k(a_i)\right)(x) \\ &= \left(\sum_{k=0}^{\infty} \tfrac{(-1)^k s(x)^k}{(f(x))^k k!} D^k(a_i)\right)(x) = \left(\sum_{k=0}^{\infty} \tfrac{(-1)^k s^k}{(Ds)^k k!} D^k(a_i)\right)(x). \end{aligned}$$

By the Slice Theorem (see [19, Proposition 2.1]), $\left(\sum_{k=0}^{\infty} \frac{(-1)^k s^k}{(Ds)^k k!} D^k(a_i)\right)$ is in $\Bbbk[X]_f^D$, and as x and y are not separated by invariants (including f), it follows that

$$a_i((-t_x)*x) = a_i((-t_y)*y) \quad \text{for } i = 1, \ldots, n,$$

that is, $(-t_x)*x = (-t_y)*y$, and so x and y are in the same orbit. □

Note that if $S \subseteq \Bbbk[X]$ consists of $\mathbb{G}_a$-invariants, then the zero set $\mathcal{V}_X(S)$ of S in X is $\mathbb{G}_a$-stable. In particular, the following Proposition is a first step of the decomposition of the separating variety in $\mathbb{G}_a \times \mathbb{G}_a$-stable subsets:

Proposition 2.2. *Let $I \subseteq \sqrt{\mathrm{pl}(D)\Bbbk[X]}$ be an ideal of $\Bbbk[X]$, and consider the canonical projection $\tau : \Bbbk[X] \to \Bbbk[X]/I$, given by $f \mapsto f + I$. Let $A \subseteq \Bbbk[X]^D$ be a separating algebra. If $h_1, \ldots, h_r$ are elements of $\Bbbk[X]$ such that $\Bbbk[\tau(h_1), \ldots, \tau(h_r)] = \tau(A)$, then the separating variety decomposes as*

$$\mathcal{S}_D = \Big(\mathcal{V}_{X\times X}(\delta(h_1), \ldots, \delta(h_r)) \cap (\mathcal{V}_X(I) \times \mathcal{V}_X(I))\Big) \cup \Gamma_D.$$

Proof.
"$\supseteq$": We have already seen that $\mathcal{S}_D \supseteq \Gamma_D$. Take a pair $(x, y) \in \mathcal{V}_{X\times X}(\delta(h_1), \ldots, \delta(h_r)) \cap (\mathcal{V}_X(I) \times \mathcal{V}_X(I))$. We have to show $(x, y) \in \mathcal{S}_D$, that is, $f(x) = f(y)$ for all $f \in \Bbbk[X]^D$. As A is a separating algebra, it suffices to show that $f(x) = f(y)$ for all $f \in A$. Let f be an element of A. As $\tau(f)$ is in $\Bbbk[\tau(h_1), \ldots, \tau(h_r)]$, there exists a polynomial p in r variables such that $\tau(f) = p(\tau(h_1), \ldots, \tau(h_r))$. Therefore, $f - p(h_1, \ldots, h_r) \in I$. As (x, y) is an element of $\mathcal{V}_X(I) \times \mathcal{V}_X(I)$, we have $g(x) = g(y) = 0$ for all $g \in I$. Thus we have

$$f(x) - p(h_1(x), \ldots, h_r(x)) = 0 = f(y) - p(h_1(y), \ldots, h_r(y)).$$

As also $(x, y) \in \mathcal{V}_{X\times X}(\delta(h_1), \ldots, \delta(h_r))$, we have $h_i(x) = h_i(y)$ for $i = 1, \ldots, r$. It follows that $f(x) = f(y)$.
"$\subseteq$": It suffices to show that $\mathcal{S}_D \setminus \Gamma_D \subseteq \mathcal{V}_{X\times X}(\delta(h_1), \ldots, \delta(h_r)) \cap (\mathcal{V}_X(I) \times \mathcal{V}_X(I))$. Take $(x, y) \in \mathcal{S}_D \setminus \Gamma_D$. By Proposition 2.1, we have that $(x, y) \in \mathcal{V}_X(I) \times \mathcal{V}_X(I)$. It remains to show that $(x, y) \in \mathcal{V}_{X\times X}(\delta(h_1), \ldots, \delta(h_r))$. Take elements $g_i \in A$ such that $\tau(h_i) = \tau(g_i)$ for $i = 1, \ldots, r$. There then exist elements $q_i \in I$ such that $h_i = g_i + q_i$ for $i = 1, \ldots, r$. As $x, y \in \mathcal{V}_X(I)$, we have $q_i(x) = 0 = q_i(y)$ for all i. As $(x, y) \in \mathcal{S}_D$, we have $g_i(x) = g_i(y)$ for all i. Hence,

$$h_i(x) = g_i(x) + q_i(x) = g_i(y) + q_i(y) = h_i(y) \quad \text{for all } i = 1, \ldots, r.$$

This shows that $\delta(h_i)(x, y) = 0$ for $i = 1, \ldots, r$, and so we are done. □

Example 2.3. We consider Daigle and Freudenburg's 5-dimensional counterexample to Hilbert's fourteenth problem (see [3]). Let $X := \Bbbk^5$ and let $R := \Bbbk[x, s, t, u, v]$ be the ring of regular functions on X. Define a LND on R via

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

In [9], we constructed the following separating algebra for R^Δ:

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

We have $x^3 = \Delta(s) \in R^\Delta$ and $f_2 = 2x^3t - s^2 = \Delta(3x^3u - st) \in R^\Delta$, thus, x and s are in $\sqrt{\mathrm{pl}(\Delta)R}$. By [9, Proposition 3.2], we have $R^\Delta \subseteq \Bbbk \oplus (x, s)R$. Thus, if $\tau : R \to R/(x, s)R$ is the canonical projection, for any separating algebra $A \subseteq R^\Delta$, we have $\Bbbk[\tau(1)] = \tau(A)$. By Proposition 2.2, it follows that

$$\mathcal{S}_\Delta = \big(\mathcal{V}_X(x, s) \times \mathcal{V}_X(x, s)\big) \cup \overline{\Gamma_\Delta}. \tag{1}$$

Both the sets on the right hand side are irreducible and of dimension 6, and one can check (using Magma [1], for example) that neither contains the other. Therefore Equation (1) gives $\mathcal{S}_\Delta$ as the union of irreducible components. $\triangleleft$

Remark 2.4. One can compute the separating variety in a similar manner for Roberts' counterexample [18] and the derivation investigated in [8, section 5]. Indeed, in both cases there is $S \subseteq \sqrt{\mathrm{pl}(D)}$ such that $\Bbbk[X]^D \subseteq \Bbbk + S\Bbbk[X]$.

As the separating variety contains the graph, its dimension is at least that of the graph. It can be bigger, as in [15, Example 2.1] and Example 2.5 below, and as we can see from Theorem 3.2, it can have components of smaller dimension. In characteristic zero, the additive group has no non-trivial closed subgroups. Points are thus either fixed or have trivial stabilizer. When the $\mathbb{G}_a$-action is non-trivial, the Zariski-closure of the graph therefore has dimension $\dim(X) + \dim(\mathbb{G}_a) = \dim(X) + 1$ (see for example [16, Section 10.3]).

Example 2.5. We now consider Freudenburg's 6-dimensional counterexample to Hilbert's fourteenth problem (see [12]). Let $X := \Bbbk^6$ and let $B := \Bbbk[x, y, s, t, u, v]$ be the ring of regular functions on X. Define a LND on B via:

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

We have $D(s) = x^3 \in B^D$ and $D(3x^3u - y^3st) = 2x^3y^3t - y^6s^2 \in B^D$, that is, $(x, ys) \subseteq \sqrt{\mathrm{pl}(D)B}$. As $B^D \subseteq \Bbbk \oplus (x, y)B$ (see [12, Lemma 1]) and $B^D \subseteq \Bbbk[y] \oplus (x, s)B$ (see [8, Example 4.4]), if $\tau : B \to B/(x, ys)$

is the canonical projection, then for any separating algebra A, $\tau(A) \subseteq \Bbbk[\tau(y)]$. By Proposition 2.2, we have

$$\begin{aligned}\mathcal{S}_D = &\ \overline{\Gamma_G} \cup \big((\mathcal{V}_X(x, ys) \times \mathcal{V}_X(x, ys)) \cap \mathcal{V}_{X\times X}(y \otimes 1 - 1 \otimes y)\big) \\ = &\ \overline{\Gamma_G} \cup \mathcal{V}_{X\times X}(x \otimes 1, 1 \otimes x, y \otimes 1, 1 \otimes y) \cup \\ &\qquad \mathcal{V}_{X\times X}(x \otimes 1, 1 \otimes x, s \otimes 1, 1 \otimes s, y \otimes 1 - 1 \otimes y).\end{aligned}$$

One can verify (again with Magma [1]) that this gives us the separating variety as the union of three irreducible components of dimension 7, 8, and 7, respectively. This example also shows that in general, the dimension of the separating variety is not $2 \dim X - \dim(\Bbbk[X]^D)$). $\triangleleft$

Proposition 2.6. *If D is nonzero and $\Bbbk[X]^D$ admits a polynomial separating algebra, then every irreducible component of $\mathcal{S}_D$ has dimension at least* $\dim X + 1$.

Proof. As $\Bbbk$ has characteristic zero, any separating algebra A has field of fractions $Q(A) = Q(\Bbbk[X]^D)$ (see [6, Theorem 3.2.3], or [5, Proposition 2.3.10] when $\Bbbk[X]^D$ is finitely generated). Thus a finitely generated separating algebra A has dimension $n := \operatorname{trdeg}_{\Bbbk}(Q(\Bbbk[X]^D)) = \dim X - 1$ (see [13, Principle 11(e)]). If A is a polynomial ring, then A is generated by n elements, say $f_1, \ldots, f_n$. It follows that $\mathcal{S}_D = \mathcal{V}_{X\times X}(\delta(A)) = \mathcal{V}_{X\times X}(\delta(f_1), \ldots, \delta(f_n))$ is cut out by n elements. By Krull's Principal Ideal Theorem (see for example, [10, Theorem 10.2]), every irreducible component of $\mathcal{S}_D$ has codimension at most n, that is, dimension at least $\dim X + 1$. $\square$

3. The basic actions

We now concentrate on the basic actions of the additive group. They are induced by the Weitzenböck derivations $D_n = x_0 \frac{\partial}{\partial x_1} + \ldots + x_{n-1} \frac{\partial}{\partial x_n}$ on the polynomial rings $\Bbbk[x_0, \ldots, x_n] = \Bbbk[V_n]$. We recall some results and notation from [11], where separating sets for the basic actions were first constructed. Define the invariants

$$f_m := \sum_{k=0}^{m-1} (-1)^k x_k x_{2m-k} + \frac{1}{2}(-1)^m x_m^2 \in \ker D_n \quad \text{for } m = 1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor,$$

and $f_0 := x_0$. For $m = 0, \ldots, \lfloor \frac{n-1}{2} \rfloor$, [11, Equation (3)] also gives polynomials s_m such that $D_n s_m = f_m$. It follows that

$$I_n := (x_0, \ldots, x_{\lfloor \frac{n-1}{2} \rfloor}) = \sqrt{(f_0, \ldots, f_{\lfloor \frac{n-1}{2} \rfloor})} \subseteq \sqrt{\operatorname{pl}(D_n)\Bbbk[V_n]}. \tag{2}$$

Consider the projection $\tau : \Bbbk[V_n] \to \Bbbk[V_n]/I_n$. We can reformulate [11, Proposition 3.1] as:

$$\tau(\Bbbk[V_n]^{D_n}) = \begin{cases} \Bbbk & \text{for } 2 \nmid n, \\ \Bbbk[\tau(x_m^2)] & \text{for } n = 2m,\ 2 \nmid m, \\ \Bbbk[\tau(x_m^2), \tau(x_m^3)] & \text{for } n = 2m,\ 2 \mid m. \end{cases} \tag{3}$$

Proposition 2.2 then implies that the separating variety $\mathcal{S}_{D_n}$ is

(4)
$$\begin{array}{ll} \big(\mathcal{V}_{V_n}(I_n)\times\mathcal{V}_{V_n}(I_n)\big)\cup\overline{\Gamma_{D_n}}, & \text{for } 2\nmid n,\\ \big(\mathcal{V}_{V_n\times V_n}(\delta(x_m^2))\cap(\mathcal{V}_{V_n}(I_n)\times\mathcal{V}_{V_n}(I_n))\big)\cup\overline{\Gamma_{D_n}}, & \text{for } n=2m,\ 2\nmid m,\\ \big(\mathcal{V}_{V_n\times V_n}(\delta(x_m))\cap(\mathcal{V}_{V_n}(I_n)\times\mathcal{V}_{V_n}(I_n))\big)\cup\overline{\Gamma_{D_n}}, & \text{for } n=2m,\ 2\mid m. \end{array}$$

We formulate the technical part of our main result as a proposition whose proof is postponed to Section 4:

Proposition 3.1.

(a) *If $n=2m+1$ is odd, then*
$$\mathcal{V}_{V_n}(I_n)\times\mathcal{V}_{V_n}(I_n)\subseteq\overline{\Gamma_{D_n}}.$$
(b) *If $n=2m$ is even, then*
  (i) $(\mathcal{V}_{V_n}(I_n)\times\mathcal{V}_{V_n}(I_n))\cap\mathcal{V}_{V_n\times V_n}((x_m\otimes 1)-(-1)^m(1\otimes x_m))\subseteq\overline{\Gamma_{D_n}}$,
  (ii) *and if furthermore $\Bbbk=\mathbb{C}$, then*

$$\overline{\Gamma_{D_n}}\setminus\Gamma_{D_n}\subseteq(\mathcal{V}_{V_n}(I_n)\times\mathcal{V}_{V_n}(I_n))\cap\mathcal{V}_{V_n\times V_n}((x_m\otimes 1)-(-1)^m(1\otimes x_m)).$$

Theorem 3.2.

(a) *If n is odd, divisible by four, or equal to 2, then the separating variety is equal to the Zariski closure of the graph of the $\mathbb{G}_a$-action, that is, $\mathcal{S}_{D_n}=\overline{\Gamma_{D_n}}$.*
(b) *If $n=2m$ and $m\geq 3$ is odd, then the separating variety has two irreducible components:*
  – *$\overline{\Gamma_{D_n}}$, which has dimension $n+2$,*
  – *and a second of dimension $n+1$:*
$$\mathcal{V}_{V_n\times V_n}\big(x_m\otimes 1-1\otimes x_m\big)\cap\big(\mathcal{V}_{V_n}(I_n)\times\mathcal{V}_{V_n}(I_n)\big).$$

Proof. (a) If n is odd or divisible by 4, the claim follows immediately from Equation (4) and Proposition 3.1 (a) and (b)(i), respectively.

When $n=2$, Equation (4) gives $\mathcal{S}_{D_2}=M\cup\overline{\Gamma_{D_2}}$, where
$$M=\{((0,a_1,a_2),(0,b_1,b_2))\in V_2\times V_2:\quad a_i,b_i\in\Bbbk,\ a_1^2=b_1^2\}.$$
Take $(a,b)\in M$. If $a_1=b_1\neq 0$, then setting $t=\frac{b_2-a_2}{a_1}$, we obtain
$$t*a=(0,a_1,a_2+ta_1)=(0,b_1,b_2)=b,$$
and so $(a,b)\in\Gamma_{D_2}$. On the other hand, if $a_1=-b_1$, then Proposition 3.1(b)(i) implies $(a,b)\in\overline{\Gamma_{D_2}}$.

(b) Assume $n=2m$ with $m\geq 3$ odd. Equation (4) yields $\mathcal{S}_{D_n}=\overline{\Gamma_{D_n}}\cup M_{n,1}\cup M_{n,2}$, where $M_{n,i}$ is the set of points of $V_n\times V_n$ of the form
$$((0,\ldots,0,a_m,a_{m+1},\ldots,a_{2m}),(0,\ldots,0,(-1)^i a_m,b_{m+1},\ldots,b_{2m}))$$
for $i=1,2$ and $a_k,b_k\in\Bbbk$. By Proposition 3.1 (b)(i), we have $M_{n,1}\subseteq\overline{\Gamma_{D_n}}$, and so $\mathcal{S}_{D_n}=\overline{\Gamma_{D_n}}\cup M_{n,2}$. We clearly have $\Gamma_{D_n}\not\subseteq M_{n,2}$. It

remains to show that $M_{n,2} \not\subseteq \overline{\Gamma_{D_n}}$. Suppose, for the sake of a proof by contradiction, that $M_{n,2} \subseteq \overline{\Gamma_{D_n}}$.

The $\mathbb{G}_a$-actions we consider are in fact defined over $\mathbb{Q}$. Thus, $\overline{\Gamma_{D_n}}$ is the zero set of an ideal generated by polynomials with coefficients in $\mathbb{Q}$ (often called the Derksen-ideal, see [4, 15]). Clearly, this also holds for $M_{n,2}$. Note that ideal inclusion can be decided using Gröbner Basis methods. Hence, the question of the inclusion of $M_{n,2}$ in $\overline{\Gamma_{D_n}}$ will have the same answer over any field of characteristic zero, and we may assume $\Bbbk = \mathbb{C}$. Proposition 3.1(b)(ii) then implies that $M_{n,2} \setminus \Gamma_{D_n} \subseteq \overline{\Gamma_{D_n}} \setminus \Gamma_{D_n} \subseteq M_{n,1}$. As $m \geq 3$, this is a contradiction. Indeed, if $a = e_m$ and $b = e_m + e_{m+1}$ (where $e_0, \dots, e_n$ are the standard basis vectors), then $(a, b) \in M_{n,2} \setminus \Gamma_{D_n}$, but $(a, b) \notin M_{n,1}$. $\square$

Corollary 3.3. *If $n = 2m$ and $m \geq 3$ is odd, then $\Bbbk[V_n]^{D_n}$ does not admit a polynomial separating algebra.*

Proof. Immediate from Theorem 3.2(b) and Proposition 2.6. $\square$

4. Proof of Propostion 3.1

We first prove a technical lemma, which in turn uses the following well-known formula (see, for example [14, Satz 1.25]):

$$\sum_{j=0}^{r} (-1)^j \binom{r}{j} \binom{p-j}{q} = \binom{p-r}{p-q} \qquad \text{for all } p \geq q \geq 0,\ r \geq 0. \tag{5}$$

Lemma 4.1.

(a) *If $2m \leq n$ are natural numbers, then $M_{m,n} = \left(\frac{1}{(n-i-j)!}\right)_{i,j=0,\dots,m} \in \mathbb{Q}^{(m+1)\times(m+1)}$ is an invertible matrix.*

(b) *For any m, if $A := M_{m-1,2m} = \left(\frac{1}{(2m-i-j)!}\right)_{i,j=0,\dots,m-1} \in \mathbb{Q}^{m\times m}$ and $v := (\frac{1}{m!}, \frac{1}{(m-1)!} \dots, \frac{1}{1!})^T \in \mathbb{Q}^m$, then $v^T A^{-1} v = 1 - (-1)^m$.*

Proof.
(a) For each $i = 0, \dots, m$, multiply the ith line of $M_{m,n}$ by $(n-i)!$ to obtain the matrix $\left(\frac{(n-i)!}{(n-i-j)!}\right)_{i,j=0,\dots,m}$ having the same rank as $M_{m,n}$. This is the evaluation matrix $(f_j(a_i))_{i,j=0,\dots,m}$ of the polynomials $f_j = X(X-1)\cdots(X-j+1)$ of degree j at the points $a_i = n-i$, and thus, it is invertible.
(b) Set

$$x = \left(\frac{(-1)^{m+j}(2m-j+1)!}{(j-1)!(m-j+1)!}\right)_{j=1,\dots,m} \in \mathbb{Q}^m.$$

We first show that $Ax = v$. For $i = 1, \dots, m$, we have to show that

$$\sum_{j=1}^{m} \frac{(-1)^{m+j}(2m-j+1)!}{(2m-i-j+2)!(j-1)!(m-j+1)!} = \frac{1}{(m-i+1)!},$$

which is equivalent to

$$\sum_{j=1}^{m+1} \frac{(-1)^{m+j}(2m-j+1)!}{(2m-i-j+2)!(j-1)!(m-j+1)!} = 0.$$

The left-hand side is equal to

$$\begin{aligned} & (-1)^{m+1} \sum_{j=0}^{m} \frac{(-1)^j (2m-j)!}{(2m-i-j+1)!j!(m-j)!} \\ = \quad & (-1)^{m+1} \frac{(i-1)!}{m!} \underbrace{\sum_{j=0}^{m} (-1)^j \binom{2m-j}{i-1}\binom{m}{j}}_{(*)}. \end{aligned}$$

Formula (5) with $r := m$, $p := 2m$, $q := i-1$ implies that the sum $(*)$ is equal to $\binom{m}{2m-i+1}$, which is zero for $i = 1, \ldots, m$, and so $Ax = v$.

Next, we show that $v^T x = 1 - (-1)^m$, that is,

$$\sum_{j=1}^{m} \frac{(-1)^{m+j}(2m-j+1)!}{(j-1)!((m-j+1)!)^2} = 1 - (-1)^m,$$

or again

$$\sum_{j=0}^{m} \frac{(-1)^j (2m-j)!}{j!((m-j)!)^2} = \sum_{j=0}^{m} (-1)^j \binom{m}{j}\binom{2m-j}{m} = 1.$$

Since Formula (5) with $r = m$, $p = 2m$, and $q = m$ yields the last equality, we have shown that $v^T A^{-1} v = v^T x = 1 - (-1)^m$. □

Proof of Proposition 3.1. Set $m := \lfloor \frac{n}{2} \rfloor$. We start by reformulating the three statements:

(a) Suppose $n = 2m+1$ is odd. If

$$\begin{aligned} & a = (0, \ldots, 0, a_{m+1}, \ldots, a_n) \\ \text{and} \quad & b = (0, \ldots, 0, b_{m+1}, \ldots, b_n), \end{aligned} \tag{6}$$

then $(a, b) \in \overline{\Gamma_{D_n}}$.

(b)(i) Suppose $n = 2m$ is even. If

$$\begin{aligned} & a = (0, \ldots, 0, a_m, a_{m+1}, \ldots, a_n) \\ \text{and} \quad & b = (0, \ldots, 0, (-1)^m a_m, b_{m+1}, \ldots, b_n), \end{aligned} \tag{7}$$

then $(a, b) \in \overline{\Gamma_{D_n}}$.

(b)(ii) If $\Bbbk = \mathbb{C}$, then every point $(a, b) \in \overline{\Gamma_{D_n}} \setminus \Gamma_{D_n}$ is of the form given in (7).

We prove (a) and (b)(i) simultaneously by constructing a morphism

$$\begin{array}{rccl} f: & \Bbbk & \longrightarrow & V \times V \\ & u & \longmapsto & (x(u), y(u)), \end{array}$$

such that

(1) $f(0) = (a, b)$, as given in Equation (6) or (7), if n is odd or even, respectively,
(2) and for each $u \neq 0$, we have $y(u) = {}^1\!/\!_u * x(u)$.

As $\overline{\Gamma_{D_n}}$ is Zariski-closed, $f^{-1}(\overline{\Gamma_{D_n}})$ is also Zariski-closed and contains $\Bbbk \setminus \{0\}$. Thus, $f^{-1}(\overline{\Gamma_{D_n}})$ must contain $\Bbbk$, and in particular, $(a, b) = f(0) \in \overline{\Gamma_{D_n}}$.

Set $m' := \lfloor \frac{n-1}{2} \rfloor$, so that for n odd, we have $m' = m$, and for n even, $m' = m - 1$. Note that $n = (m + 1) + m'$ in both cases. We impose the following restrictions:

$$\begin{aligned} x(u) &:= \underbrace{(x_0(u), \ldots, x_{m'}(u)}_{:=\tilde{x}(u)}, a_{m'+1}, \ldots, a_n), \\ y(u) &:= \underbrace{(y_0(u), \ldots, y_m(u)}_{:=\tilde{y}(u)}, b_{m+1}, \ldots, b_n). \end{aligned}$$

For $z = (z_i)_{i=0,\ldots,n} \in V_n$ and $t \in \mathbb{G}_a$, the group action is given by

$$t * z = \left(\sum_{i=0}^{k} \frac{t^{k-i}}{(k-i)!} z_i \right)_{k=0,\ldots,n}.$$

If $x(u)$ and $y(u)$ define a morphism as desired, for $u \neq 0$, we must have $({}^1\!/\!_u * x(u))_{k=m+1,\ldots,n} = (b_k)_{k=m+1,\ldots,n}$, or equivalently

$$\sum_{i=0}^{m'} \frac{1}{u^{k-i}(k-i)!} x_i + \sum_{i=m'+1}^{k} \frac{1}{u^{k-i}(k-i)!} a_i = b_k \quad \text{ for } k = n, \ldots, m+1.$$

Set $\delta := m - m'$, so that $\delta = 0$ for n odd, and $\delta = 1$ for n even, then $\tilde{x}(u)$ must be a solution of the following system of linear equations:

(8)
$$\underbrace{\begin{pmatrix} \frac{1}{u^n n!} & \frac{1}{u^{n-1}(n-1)!} & \cdots & \frac{1}{u^{m+1}(m+1)!} \\ \frac{1}{u^{n-1}(n-1)!} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \frac{1}{u^{m+1}(m+1)!} & \frac{1}{u^m m!} & \cdots & \frac{1}{u^{\delta+1}(\delta+1)!} \end{pmatrix}}_{=:C(u)} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{m'} \end{pmatrix} = \begin{pmatrix} p_m \\ p_{m-1} \\ \vdots \\ p_\delta \end{pmatrix},$$

where $p_{k-m'-1}(u) := b_k - \sum_{i=m'+1}^{k} \frac{({}^1\!/\!_u)^{k-i}}{(k-i)!} a_i$ for $k = n, \ldots, m + 1$.

Observe that

$$C(u) = u^{\delta-1} \cdot \operatorname{diag}(u^{-m}, u^{1-m}, \ldots, u^{-\delta}) \cdot A \cdot \operatorname{diag}(u^{-m}, u^{1-m}, \ldots, u^{-\delta}),$$

where $A := M_{m',n}$ is the invertible matrix of Lemma 4.1 (a). Thus, for nonzero u, we must have

$$\tilde{x}(u) = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{m'} \end{pmatrix} = u^{1-\delta} \operatorname{diag}(u^m, u^{m-1}, \ldots, u^\delta) A^{-1} \underbrace{\begin{pmatrix} u^m p_m \\ u^{m-1} p_{m-1} \\ \vdots \\ u^\delta p_\delta \end{pmatrix}}_{=:q(u)}.$$

Note that above, $q_k(u) = u^k p_k(u)$ is a polynomial in u, thus for this choice of $\tilde{x}(u)$, we obtain a morphism satisfying $x(0) = a$ as desired. For $u \neq 0$ and $k = 0, \ldots, m'$, we must then have

$$\begin{aligned} y_k(u) &:= \sum_{i=0}^{k} \frac{(1/u)^{k-i}}{(k-i)!} x_i(u) = \left(\frac{u^{-k}}{k!}, \frac{u^{-k+1}}{(k-1)!}, \ldots, \frac{1}{0!}, 0, \ldots, 0 \right) \tilde{x}(u) \\ &= u^{1-\delta} \left(\frac{u^{m-k}}{k!}, \frac{u^{m-k}}{(k-1)!}, \ldots, \frac{u^{m-k}}{0!}, 0, \ldots, 0 \right) A^{-1} q(u). \end{aligned}$$

This gives an expression of $y_k(u)$ as a polynomial in u. For $k = 0, \ldots, m'$, we have $y_k(0) = 0$. For n odd, it already follows that $y(0) = b$, and we are done. If n is even, then

$$y_m(u) = a_m + \left(\frac{1}{m!}, \frac{1}{(m-1)!}, \ldots, \frac{1}{2!}, \frac{1}{1!} \right) A^{-1} q(u), \tag{9}$$

which is again polynomial in u. It remains to show that $y_m(0) = (-1)^m a_m$ for $n = 2m$. As $q_k(0)$ is $-\frac{a_m}{k!}$ for $k = \delta, \delta+1, \ldots, m$, formula (9) yields

$$\begin{aligned} y_m(0) &= a_m + \left(\frac{1}{m!}, \frac{1}{(m-1)!}, \ldots, \frac{1}{2!}, \frac{1}{1!} \right) A^{-1} \begin{pmatrix} -\frac{a_m}{m!} \\ -\frac{a_m}{(m-1)!} \\ \vdots \\ -\frac{a_m}{1!} \end{pmatrix} \\ &= a_m (1 - v^T A^{-1} v) = (-1)^m a_m, \end{aligned}$$

where $v = (\frac{1}{m!}, \frac{1}{(m-1)!} \ldots, \frac{1}{1!})^T \in \Bbbk^m$, and the last equality follows from Lemma 4.1 (b).

We now prove (b)(ii). Recall that for a constructible subset U in an affine complex variety, the Zariski-closure coincides with the closure taken in the Euclidean topology (see [2, Satz 11.23]). In particular, as images of morphisms are constructible, this result holds for the image Γ_{D_n} of the graph morphism $\phi : \mathbb{G}_a \times V_n \to V_n \times V_n$ defined by $\phi(t, x) = (x, t * x)$. Let $(a, b) \in \overline{\Gamma_{D_n}} \setminus \Gamma_{D_n}$. We must show that (a, b) is of the form described in (7). By Proposition 2.1, $(a, b) \in \mathcal{S}_{D_n} \setminus \Gamma_{D_n}$ implies that $(a, b) \in \mathcal{V}_{V_n}(I_n) \times \mathcal{V}_{V_n}(I_n)$, that is, $a = (0, \ldots, 0, a_m, a_{m+1}, \ldots, a_n)$ and $b = (0, \ldots, 0, b_m, b_{m+1}, \ldots, b_n)$. Thus, it remains to show that

$b_m = (-1)^m a_m$. As $(a,b) \in \overline{\Gamma_{D_n}}$, there exists a sequence $(t_l, x^l)_{l\in\mathbb{N}} \in (\mathbb{G}_a \times V_n)^{\mathbb{N}}$ such that

$$\lim_{l\to\infty}(x^l, t_l * x^l) = (a,b).$$

If the sequence $(t_l)_{l\in\mathbb{N}}$ was bounded, there would be a convergent subsequence with limit t', and as the group action is a continuous map, we would have $(a,b) = (a, t' * a) \in \Gamma_{D_n}$, a contradiction. Thus, the sequence $(t_l)_{l\in\mathbb{N}}$ is unbounded, and we can assume

$$\lim_{l\to\infty} t_l = \infty \qquad \text{and } t_l \neq 0 \text{ for all } l \in \mathbb{N}.$$

Set $y^l := t_l * x^l$, and write $x^l = (x_0^l, x_1^l, \ldots, x_n^l)$ and $y^l = (y_0^l, y_1^l, \ldots, y_n^l)$. We then have the following equations:

$$y_k^l = \sum_{i=0}^{k} \frac{t_l^{k-i}}{(k-i)!} x_i^l \qquad \text{for } k = 0, \ldots, n.$$

For each $k = m+1, \ldots, 2m$, these equations can be written as

$$\sum_{i=0}^{m-1} \frac{t_l^{k-i}}{(k-i)!} x_i^l = \underbrace{y_k^l - \sum_{i=m}^{k} \frac{t_l^{k-i}}{(k-i)!} x_i^l}_{=:p_{k-m}^l}.$$

Similarly as in Equation (8), we may write these equations in matrix form:

$$(10) \quad \underbrace{\begin{pmatrix} \frac{t_l^{2m}}{2m!} & \frac{t_l^{2m-1}}{(2m-1)!} & \cdots & \frac{t_l^{m+1}}{(m+1)!} \\ \frac{t_l^{2m-1}}{(2m-1)!} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \frac{t_l^{m+1}}{(m+1)!} & \frac{t_l^{m}}{m!} & \cdots & \frac{t_l^{2}}{2!} \end{pmatrix}}_{=:C_l} \begin{pmatrix} x_0^l \\ x_1^l \\ \vdots \\ x_{m-1}^l \end{pmatrix} = \begin{pmatrix} p_m^l \\ p_{m-1}^l \\ \vdots \\ p_1^l \end{pmatrix}.$$

If $A := M_{m-1,2m} = \left(\frac{1}{(2m-i-j)!}\right)_{i,j=0,\ldots,m-1} \in \mathbb{Q}^{m\times m}$ is the invertible matrix of Lemma 4.1(a), then

$$C_l = \operatorname{diag}(t_l^m, t_l^{m-1}, \ldots, t_l) \cdot A \cdot \operatorname{diag}(t_l^m, t_l^{m-1}, \ldots, t_l),$$

and thus,

$$\begin{pmatrix} x_0^l \\ x_1^l \\ \vdots \\ x_{m-1}^l \end{pmatrix} = \operatorname{diag}(t_l^{-m}, t_l^{-m+1}, \ldots, t_l^{-1}) A^{-1} \begin{pmatrix} t_l^{-m} p_m \\ t_l^{-m+1} p_{m-1} \\ \vdots \\ t_l^{-1} p_1 \end{pmatrix}.$$

We define $q_k^l := t_l^{-k} p_k$ for $k = 1, \ldots, m$ and all l. We have

$$\begin{aligned} y_m^l &= x_m^l + \sum_{i=0}^{m-1} \frac{t_l^{m-i}}{(m-i)!} x_i^l \\ &= x_m^l + \left(\frac{t_l^m}{m!}, \frac{t_l^{m-1}}{(m-1)!}, \ldots, \frac{t_l}{1!} \right) \begin{pmatrix} x_0^l \\ x_1^l \\ \vdots \\ x_{m-1}^l \end{pmatrix} \\ &= x_m^l + \left(\frac{1}{m!}, \frac{1}{(m-1)!}, \ldots, \frac{1}{1!} \right) A^{-1} \begin{pmatrix} q_m^l \\ q_{m-1}^l \\ \vdots \\ q_1^l \end{pmatrix}. \end{aligned} \tag{11}$$

For $k = 1, \ldots, m$, we have

$$\begin{aligned} \lim_{l \to \infty} q_k^l &= \lim_{l \to \infty} t_l^{-k} \left(y_{k+m}^l - \sum_{i=m}^{k+m} \frac{t_l^{k+m-i}}{(k+m-i)!} x_i^l \right) \\ &= \lim_{l \to \infty} \left(-\frac{1}{k!} x_m^l \right) = -\frac{a_m}{k!}. \end{aligned}$$

Therefore, by Lemma 4.1(b),

$$\begin{aligned} b_m &= \lim_{l \to \infty} y_m^l = a_m - a_m \cdot v^T A^{-1} v \\ &= a_m - a_m \cdot (1 - (-1)^m) = (-1)^m a_m, \end{aligned}$$

as desired. □

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Markus Brodmann. *Algebraische Geometrie. Eine Einführung. (Algebraic geometry. An introduction).* Basler Lehrbücher, 1. Basel etc.: Birkhäuser Verlag. xv, 470 S., 1989.

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

[4] Harm Derksen. Computation of invariants for reductive groups. *Adv. Math.*, 141(2):366–384, 1999.

[5] Harm Derksen and Gregor Kemper. *Computational Invariant Theory.* Number 130 in Encyclopædia of Mathematical Sciences. Springer-Verlag, Berlin, Heidelberg, New York, 2002.

[6] Emilie Dufresne. *Separating Invariants.* PhD thesis, Queen's University, Kingston, Ontario, Canada, 2008. `http://hdl.handle.net/1974/1407`.

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

[8] Emilie Dufresne. Separating invariants and quasi-affine quotients. arXiv:1102.2132, 2011.

[9] Emilie Dufresne and Martin Kohls. A finite separating set for Daigle and Freudenburg's counterexample to Hilbert's fourteenth problem. *Comm. Algebra*, 38(11):3987–3992, 2010.

[10] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Number 150 in Graduate Texts in mathematics. Springer-Verlag, New York, 1995.

[11] Jonathan Elmer and Martin Kohls. Separating invariants for the basic $\mathbb{G}_a$-actions. *Proc. Amer. Math. Soc.*, 140(1):135–146, 2012.

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

[13] 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.

[14] Heinz-Richard Halder and Werner Heise. *Einführung in die Kombinatorik*. Carl Hanser Verlag, Munich, 1976. Mathematische Grundlagen für Mathematiker, Physiker und Ingenieure.

[15] Gregor Kemper. Computing invariants of reductive groups in positive characteristic. *Transform. Groups*, 8(2):158–176, 2003.

[16] Gregor Kemper. *A course in commutative algebra*, volume 256 of *Graduate Texts in Mathematics*. Springer, Heidelberg, 2011.

[17] P. E. Newstead. *Introduction to moduli problems and orbit spaces*, volume 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Tata Institute of Fundamental Research, Bombay, 1978.

[18] 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.

[19] 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.

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

E-mail address: emilie.dufresne@unibas.ch

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

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