SEPARATING INVARIANTS FOR ARBITRARY LINEAR ACTIONS OF THE ADDITIVE GROUP

EMILIE DUFRESNE, JONATHAN ELMER, AND MÜFİT SEZER

ABSTRACT. We consider an arbitrary representation of the additive group $\mathbb{G}_a$ over a field of characteristic zero and give an explicit description of a finite separating set in the corresponding ring of invariants.

1. INTRODUCTION

The problem of distinguishing the orbits of an action of a group G on a vector space V is one of the most fundamental in mathematics, and some of the most widely studied questions in mathematics are merely special cases of this problem. For example, if we take G to be the group $GL_n(\mathbb{k})$ acting by conjugation on the vector space of $n \times n$ matrices over a field $\mathbb{k}$, then this is the problem of classifying square matrices up to conjugacy. If we take G to be the group $SL_2(\mathbb{k})$ and V to be the nth symmetric power, $S^n(W)$ of the natural representation W, then this is the problem of classifying binary forms of degree n over $\mathbb{k}$ up to equivalence.

The classical approach to solving these problems is to construct "invariant polynomials". These are polynomial functions $V \to \mathbb{k}$ which are constant on the G-orbits. One can also view these as the G-fixed points $\mathbb{k}[V]^G$ of the $\mathbb{k}$-algebra $\mathbb{k}[V]$ of polynomial functions from V to $\mathbb{k}$, where G acts on $\mathbb{k}[V]$ via

$$g \cdot f(v) = f(g^{-1} \cdot v)$$

for $v \in V$, $g \in G$ and $f \in \mathbb{k}[V]$. From this point of view it is clear that $\mathbb{k}[V]^G$ is a subalgebra of $\mathbb{k}[V]$. A natural approach to the orbit problem is then to try to find algebra generators.

Invariant theory can be considered to be the study of the subalgebras $\mathbb{k}[V]^G \subseteq \mathbb{k}[V]$. The problem of finding algebra generators has been studied rather extensively over the past 200 years, but we are still a very long way from being able to write down algebra generators in the general case. For example, in the case of $SL_2(\mathbb{k})$ acting on $S^n(W)$, a complete set of algebra generators is known only for $n \leq 10$, and the number of generators required appears to grow very quickly with n. While the list of groups and representations for which a complete set of generating invariants is known is very small, the problem has been solved algorithmically for reductive algebraic groups acting on an algebraic variety ([10, 11, 2]) and for certain non-reductive algebraic groups ([18], [4]). Many of these algorithms rely on Gröbner basis calculations, which have a tendency to explode in higher dimensions. For this

reason, using full sets of generating invariants to separate orbits is rarely a realistic proposition.

It has been known for a number of years that one can sometimes obtain as much information about the orbits of a group using a smaller subset of $\Bbbk[V]^G$; for a very simple example, see [3, Example 2.3.9]. With this in mind, a new trend in invariant theory has emerged, based around the following definition:

Definition 1 (Derksen and Kemper [3, Definition 2.3.8]). A *separating set* for the ring of invariants $\Bbbk[V]^G$ is a subset $S \subset \Bbbk[V]^G$ with the following property: given $v, w \in V$, if there exists an invariant f such that $f(v) \neq f(w)$, then there also exists $s \in S$ such that $s(v) \neq s(w)$.

Separating sets have, in many respects, "nicer" properties than generating sets. As a first example, it is well known that if G is finite and the characteristic of $\Bbbk$ does not divide $|G|$, then $\Bbbk[V]^G$ is generated by elements of degree $\leq |G|$ [7, 8], but this is not necessarily true in the modular case [16]. On the other hand, the analogue for separating invariants holds in arbitrary characteristic [3, Theorem 3.9.13]. Second, Nagata famously showed that if G is not reductive, then $\Bbbk[V]^G$ is not always finitely generated [13]. On the other hand, regardless of whether $\Bbbk[V]^G$ is finitely generated, it must contain a finite separating set [3, Theorem 2.3.15]. Unfortunately, this existence proof is non-constructive. No algorithm is known for computing finite separating sets of invariants for non-reductive groups.

In this paper, we describe a finite separating set for any finite dimensional representation of the additive group $\mathbb{G}_a$ over a field $\Bbbk$ of characteristic zero, extending the results of Elmer and Kohls for the indecomposable representations (see [6]). Accordingly, from now on, $\Bbbk$ denotes a field of characteristic zero and $\mathbb{G}_a$ its additive group. The group $\mathbb{G}_a$ is in some sense the simplest of all non-reductive groups. We describe briefly its representation theory. In each dimension there is exactly one indecomposable representation. Following the classical convention, we let V_n denote the indecomposable representation of dimension $n + 1$. We have $V_n \cong V_n^*$. There is a basis $x_0, \ldots, x_n$ for V_n^* such that the action of $\mathbb{G}_a$ on V_n^* is given by

$$\alpha \cdot x_i = \sum_{j=0}^{i} \frac{\alpha^j}{j!} x_{i-j} \text{ for } \alpha \in \mathbb{G}_a, \ \ 0 \leq i \leq n.$$

In this case, we say that $\mathbb{G}_a$ acts *basically* with respect to the basis $\{x_0, \ldots, x_n\}$. Note that $\mathbb{G}_a$ acts on V_n^* via upper triangular and on V_n via lower triangular matrices. We note that V_n^* is isomorphic to the nth symmetric power $S^n(V_1^*)$ of V_1^*; if $\mathbb{G}_a$ acts basically on V_1^* with respect to the basis $\{x_0, x_1\}$, then it acts basically on $S^n(V_1^*)$ with respect to the basis $\{\frac{1}{j!}x_0^{n-j}x_1^j \ 0 \leq j \leq n\}$.

For any finite dimensional representation W of $\mathbb{G}_a$, there is a multiset of non-negative integers $\boldsymbol{n} := \{n_1, n_2, \ldots, n_k\}$ such that $W \cong V_{n_1} \oplus V_{n_2} \oplus \ldots \oplus V_{n_k}$ as representations of $\mathbb{G}_a$. For shorthand, we let $V_{(\boldsymbol{n})}$ denote the latter and identify $\Bbbk[V_{(\boldsymbol{n})}]$ with $\Bbbk[x_{i,j} \mid 0 \leq i \leq n_j, \ 1 \leq j \leq k]$. For convenience, we will assume that $n_1, n_2, \ldots, n_k$ are ordered so that n_j is even for $1 \leq j \leq l$ and odd for $l+1 \leq j \leq k$, and further assume that $n_j \equiv 2 \mod 4$ for $1 \leq j \leq l'$ and $n_j \equiv 0 \mod 4$ for $l' + 1 \leq j \leq l$. As the problem of computing separating sets for indecomposable linear $\mathbb{G}_a$-actions was considered in [6], we assume throughout that $k \geq 2$.

The main result of this paper is as follows:

Theorem 1. *Let V be a finite dimensional representation of $\mathbb{G}_a$, with $\dim(V) = n$. Then there exists a separating set $S \subset \Bbbk[V]^{\mathbb{G}_a}$ with the following properties:*

(1) *S consists of invariants of degree at most $2n - 1$.*
(2) *The size of S is quadratic in n.*
(3) *S consists of invariants which involve variables coming from at most 2 indecomposable summands.*

This result will be proved in section 2. We also discuss and compare the number and degrees of elements in S with those of generating invariants in known cases. It should be noted that, while we can describe explicitly a separating set for any ring of invariants of a linear $\mathbb{G}_a$-action, generating sets are known only in small dimensions. Section 3 explains the interest in the third property.

2. Separating sets

Let V_n be the indecomposable representation of $\mathbb{G}_a$ of dimension $n + 1$ and suppose $\mathbb{G}_a$ acts basically with respect to the basis $\{x_0, \dots, x_n\}$ of V_n^*. The action of $\mathbb{G}_a$ is given by the formula

$$\alpha \cdot f = \exp(\alpha D_n)f \text{ for } \alpha \in \mathbb{G}_a, \ f \in \Bbbk[V_n],$$

where D_n is the Weitzenböck derivation

$$D_n = x_0 \frac{\partial}{\partial x_1} + \cdots + x_{n-1} \frac{\partial}{\partial x_n}.$$

The algebra of invariants $\Bbbk[V_n]^{\mathbb{G}_a}$ is precisely the kernel of the derivation D_n. More generally, the ring of invariants $\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$ coincides with the kernel of the derivation

$$D_{(\boldsymbol{n})} := \sum_{j=1}^{k} x_{0,j} \frac{\partial}{\partial x_{1,j}} + \cdots + x_{n_j-1,j} \frac{\partial}{\partial x_{n_j,j}}.$$

Let $\boldsymbol{n} = (n_1, n_2, \dots, n_k)$ and $\boldsymbol{n'} = (n_1', n_2', \dots, n_k')$ be two vectors in $\mathbb{N}^k$ with $n_j \geq n_j'$ for $1 \leq j \leq k$. Define the linear map $\Pi_{\boldsymbol{n'},\boldsymbol{n}} : V_{(\boldsymbol{n'})} \to V_{(\boldsymbol{n})}$ to be the map induced by the linear maps $V_{n_j'} \to V_{n_j}$,

$$(a_{0,j}, \dots, a_{n_j',j}) \mapsto (0, \dots, 0, a_{0,j}, \dots, a_{n_j',j}).$$

The map $\Pi_{\boldsymbol{n'},\boldsymbol{n}}$ is $\mathbb{G}_a$-equivariant, and so we have $\Pi_{\boldsymbol{n},\boldsymbol{n'}}^*(\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}) \subseteq \Bbbk[V_{(\boldsymbol{n'})}]^{\mathbb{G}_a}$, where $\Pi_{\boldsymbol{n},\boldsymbol{n'}}^*$ is the corresponding algebra map. For a vector $\boldsymbol{n} = (n_1, n_2, \dots, n_k)$ set $\lfloor \boldsymbol{n}/2 \rfloor = (\lfloor n_1/2 \rfloor, \lfloor n_2/2 \rfloor, \dots, \lfloor n_k/2 \rfloor)$, where the symbol $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. We let n denote the dimension of $V_{(\boldsymbol{n})}$. Note that $n = \sum_{j=1}^{k}(n_j + 1)$.

Proposition 2. *Assume the convention of section 1. Then we have*

$$\Pi_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}^*(\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}) \subseteq \Bbbk[x_{0,j} \mid 1 \leq j \leq l].$$

Moreover, $\Pi_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}^*(\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a})$ is contained in the ring of invariants of the cyclic group of order two acting on $\Bbbk[x_{0,j} \mid 1 \leq j \leq l]$ as multiplication by -1 on $x_{0,j}$ for $1 \leq j \leq l'$ and trivially on the remaining variables.

Proof. The proof essentially carries over from the indecomposable case (see [6, Proposition 3.1]). The isomorphisms $V_{n_j}^* \cong S^{n_j}(V_1^*)$ extend the $\mathbb{G}_a$-action on $\mathbb{k}[V]$ to a $SL_2(\mathbb{k})$-action when we identify V_1^* with the natural representation of $SL_2(\mathbb{k})$. A well known theorem of Roberts [17] states that the $\mathbb{G}_a$-equivariant linear map

$$\Phi: \quad \begin{array}{ccc} V_{(\boldsymbol{n})} & \longrightarrow & V_{(\boldsymbol{n})} \oplus V_1 \\ v & \longmapsto & (v, (0, 1)) \end{array}$$

induces an isomorphism $\Phi^* : \mathbb{k}[V_{(\boldsymbol{n})} \oplus V_1]^{SL_2(\mathbb{k})} \to \mathbb{k}[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$. The elements μ_α and τ of $SL_2(\mathbb{k})$ acting on V_1^* via

$$\mu_\alpha = \left(\begin{array}{cc} \alpha & 0 \\ 0 & \alpha^{-1} \end{array} \right) \text{ for } \alpha \in \mathbb{k} \setminus \{0\}, \text{ and } \tau = \left(\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right)$$

act on $V_{(\boldsymbol{n})} \oplus V_1$ as follows:

$$\mu_\alpha \cdot (\ldots, a_{i,j}, \ldots, b_0, b_1) = (\ldots, \alpha^{2i-n_j} a_{i,j}, \ldots, \alpha^{-1} b_0, \alpha b_1)$$
$$\tau \cdot (\ldots, a_{i,j}, \ldots, b_0, b_1) = (\ldots, (-1)^i \tfrac{i!}{(n_j-i)!} a_{n_j-i,j}, \ldots, b_1, -b_0).$$

Let $f \in \mathbb{k}[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$ and pick $h \in \mathbb{k}[V_{(\boldsymbol{n})} \oplus V_1]^{SL_2(\mathbb{k})}$ such that $\Phi^*(h) = f$. Then h is fixed by μ_α and so, for all $\alpha \in \mathbb{k} \setminus \{0\}$,

$$f(\ldots, a_{i,j}, \ldots) = h(\ldots, a_{i,j}, \ldots, 0, 1) = h(\ldots, \alpha^{2i-n_j} a_{i,j}, \ldots, 0, \alpha).$$

Thus, for all $\alpha \in \mathbb{k} \setminus \{0\}$, we have

$$(\Pi_{\boldsymbol{n}, \lfloor \boldsymbol{n}/2 \rfloor}^* f)(\ldots, a_{i,j}, \ldots) = f(\ldots, 0, \ldots, a_{0,j}, \ldots, a_{\lfloor n_j/2 \rfloor, j}, \ldots)$$
$$= h(\ldots, 0, \ldots, \alpha^{n_j - 2\lfloor n_j/2 \rfloor} a_{0,j}, \ldots, \alpha^{n_j} a_{\lfloor n_j/2 \rfloor, j}, \ldots, 0, \alpha).$$

Since this is a polynomial equation in α and $\mathbb{k}$ is an infinite field, the equality must also hold for $\alpha = 0$, in which case we have:

$$(\Pi_{\boldsymbol{n}, \lfloor \boldsymbol{n}/2 \rfloor}^* f)(\ldots, a_{i,j}, \ldots) = h(\ldots, 0, \ldots, a_{0,j}, 0, \ldots, 0, 0),$$

where $2 | n_j$, proving the first statement.

To prove the second assertion, we use that h is also fixed by τ. We then have

$$(\Pi_{\boldsymbol{n}, \lfloor \boldsymbol{n}/2 \rfloor}^* f)(\ldots, a_{i,j}, \ldots) = h(\ldots, 0, \ldots, a_{0,j}, 0, \ldots, 0, 0)$$
$$= h(\ldots, 0, (-1)^{n_j/2} a_{0,j}, 0, \ldots, 0, 0),$$

ending the proof. $\qquad \square$

Let f, g be two polynomials in $\mathbb{k}[V_{(\boldsymbol{n})} \oplus V_1]^{SL_2(\mathbb{k})}$. Assume that the total degrees of these polynomials in the variables y_0, y_1 are d_1 and d_2, respectively, where we identify $\mathbb{k}[V_1]$ with $\mathbb{k}[y_0, y_1]$. Then for $r \leq \min(d_1, d_2)$, the polynomial

$$\sum_{q=0}^{r} (-1)^q \binom{r}{q} \frac{\partial^r f}{\partial y_0^{r-q} \partial y_1^q} \frac{\partial^r g}{\partial y_0^q \partial y_1^{r-q}}$$

also lies in $\mathbb{k}[V_{(\boldsymbol{n})} \oplus V_1]^{SL_2(\mathbb{k})}$ (see, for example, [15, p. 88]). This polynomial is called the *rth transvectant of f and g* and is denoted by $\langle f, g \rangle^r$. Together with Roberts' isomorphism this process produces a new invariant in $\mathbb{k}[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$ from a given pair as follows. Let $f_1, f_2 \in \mathbb{k}[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$, and let d_1 and d_2 denote the total degrees in y_0, y_1 of $\Phi^{*-1}(f_1)$ and $\Phi^{*-1}(f_2)$, respectively. For $r \leq \min(d_1, d_2)$ the *rth semitransvectant of f_1 and f_2* is defined by

$$[f_1, f_2]^r := \Phi^*(\langle \Phi^{*-1}(f_1), \Phi^{*-1}(f_2) \rangle^r).$$

A crucial part of our separating set consists of semitransvectants of two polynomials each depending on only one summand. For these invariants, the inverse of Roberts' isomorphism is given in terms of a derivation. For $1 \leq j \leq k$, set

$$\Delta_j = \sum_{i=0}^{n_j} (n_j - i)(i+1)x_{i+1,j} \frac{\partial}{\partial x_{i,j}}.$$

Let f be in $\Bbbk[x_{0,j}, x_{1,j}, \ldots, x_{n_j,j}]^{\mathbb{G}_a}$ for some $1 \leq j \leq k$. Then f is called *isobaric of weight m*, if all of the monomials $x_{0,j}^{e_0} x_{1,j}^{e_1} \cdots x_{n_j,j}^{e_{n_j}}$ in f satisfy $m = \sum_{i=0}^{n_j} (n_j - 2i)e_i$. For an isobaric $f \in \Bbbk[x_{0,j}, x_{1,j}, \ldots, x_{n_j,j}]^{\mathbb{G}_a}$ of weight m, the inverse of Roberts' isomorphism is given by

$$\Phi^{*-1}(f) = \sum_{i=0}^{m} (-1)^i \frac{\Delta_j^i(f)}{i!} y_0^i y_1^{m-i},$$

see [9, p. 43]. For $1 \leq j_1 \neq j_2 \leq l'$, let N denote the least common multiple of n_{j_1} and n_{j_2}. We define $w_{j_1,j_2} := [x_{0,j_1}^{N/n_{j_1}}, x_{0,j_2}^{N/n_{j_2}}]^N$.

Proposition 3. *Let $1 \leq j_1 \neq j_2 \leq l'$. There exists a non-zero scalar d such that*

$$\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(w_{j_1,j_2}) = d x_{0,j_1}^{N/n_{j_1}} x_{0,j_2}^{N/n_{j_2}}.$$

Proof. Let $0 \leq q \leq N$ be an integer. Since the weight of the invariant $x_{0,j_1}^{N/n_{j_1}}$ is N, the formula for Φ^{*-1} in the previous paragraph yields

$$\frac{\partial^N \Phi^{*-1}(x_{0,j_1}^{N/n_{j_1}})}{\partial y_0^{N-q} \partial y_1^q} = \sum_{i=N-q}^{N-q} (-1)^i \frac{\Delta_{j_1}^i(x_{0,j_1}^{N/n_{j_1}})}{i!} \frac{i!}{(i-N+q)!} \frac{(N-i)!}{(N-i-q)!} y_0^{i-N+q} y_1^{N-i-q}$$

$$= (-1)^{N-q} q! \Delta_{j_1}^{N-q}(x_{0,j_1}^{N/n_{j_1}}).$$

Similarly, we have

$$\frac{\partial^N \Phi^{*-1}(x_{0,j_2}^{N/n_{j_2}})}{\partial y_0^q \partial y_1^{N-q}} = \sum_{i=q}^{q} (-1)^i \frac{\Delta_{j_2}^i(x_{0,j_2}^{N/n_{j_2}})}{i!} \frac{i!}{(i-q)!} \frac{(N-i)!}{(q-i)!} y_0^{i-q} y_1^{q-i}$$

$$= (-1)^q (N-q)! \Delta_{j_2}^q(x_{0,j_2}^{N/n_{j_2}}).$$

Using that Φ^* is an algebra homomorphism, we get

$$w_{j_1,j_2} = \sum_{q=0}^{N} (-1)^q N! \Delta_{j_1}^{N-q}(x_{0,j_1}^{N/n_{j_1}}) \Delta_{j_2}^q(x_{0,j_2}^{N/n_{j_2}}).$$

Since both j_1 and j_2 are congruent to two modulo four, we have $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(x_{i,j}) = 0$ if $i < n_j/2$, and $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(x_{i,j}) = x_{i-n_j/2,j}$ if $i - n_j/2 \geq 0$ for $j = j_1, j_2$. Therefore to compute $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(w_{j_1,j_2})$, it suffices to consider w_{j_1,j_2} modulo the ideal of $\Bbbk[V_{(\boldsymbol{n})}]$ generated by $x_{0,j_1}, \ldots, x_{n_{j_1}/2-1,j_1}, x_{0,j_2}, \ldots, x_{n_{j_2}/2-1,j_2}$. Call this ideal I.

A monomial $x_{0,j_1}^{e_0} x_{1,j_1}^{e_1} \cdots x_{n_{j_1},j_1}^{e_{n_{j_1}}}$ in $\Bbbk[x_{0,j_1}, \ldots, x_{n_{j_1},j_1}]$ is said to have j_1-weight p if $p = \sum_{i=0}^{n_{j_1}} i e_i$. Let m be a monomial with j_1-weight p and m' be any other monomial appearing in $\Delta_{j_1}(m)$. Then m and m' have the same degree and the j_1-weight of m' is $p+1$. It follows that the j_1-weight of any monomial appearing in $\Delta_{j_1}^i(x_{0,j_1}^{N/n_{j_1}})$ is i. But the smallest possible j_1-weight of a monomial of degree N/n_{j_1} in $\Bbbk[x_{n_{j_1}/2,j_1}, \ldots, x_{n_{j_1},j_1}]$ is $N/2$. Hence all monomials of degree N/n_{j_1} of

j_1-weight less than $N/2$ lie in I. It follows that $\Delta_{j_1}^i(x_{0,j_1}^{N/n_{j_1}}) \in I$ for $i < N/2$. Similarly, $\Delta_{j_2}^i(x_{0,j_2}^{N/n_{j_2}}) \in I$ for $i < N/2$. Therefore we have

$$w_{j_1,j_2} \equiv (-1)N!\Delta_{j_1}^{N/2}(x_{0,j_1}^{N/n_{j_1}})\Delta_{j_2}^{N/2}(x_{0,j_2}^{N/n_{j_2}}) \mod I.$$

Furthermore, we claim that $\Delta_{j_1}^{N/2}(x_{0,j_1}^{N/n_{j_1}})$ is equivalent to a non-zero multiple of $x_{n_{j_1}/2,j_1}^{N/n_{j_1}}$ modulo I. To see this, first note that the j_1-weight of monomials appearing in $\Delta_{j_1}^{N/2}(x_{0,j_1}^{N/n_{j_1}})$ is $\frac{N}{2}$. But $x_{n_{j_1}/2,j_1}^{N/n_{j_1}}$ is the only monomial of degree N/n_{j_1} in $\Bbbk[x_{n_{j_1}/2,j_1},\ldots,x_{n_{j_1},j_1}]$ with j_1-weight $N/2$. Thus it suffices to show that $x_{n_{j_1}/2,j_1}^{N/n_{j_1}}$ appears with a non-zero coefficient in $\Delta_{j_1}^{N/2}(x_{0,j_1}^{N/n_{j_1}})$. This follows because for an arbitrary monomial $m \in \Bbbk[x_{0,j_1},\ldots,x_{n_{j_1},j_1}]$, any monomial that appears in $\Delta_{j_1}(m)$ has positive coefficients, and $x_{n_{j_1}/2,j_1}^{N/n_{j_1}}$ can be obtained from $x_{0,j_1}^{N/n_{j_1}}$ in $N/2$ steps by replacing a variable u with another variable appearing in $\Delta_{j_1}(u)$ at each step. This establishes the claim. A similar argument shows that $\Delta_{j_2}^{N/2}(x_{0,j_2}^{N/n_{j_2}})$ is equivalent to a non-zero multiple of $x_{n_{j_2}/2,j_2}^{N/n_{j_2}}$ modulo I. The assertion of the proposition now follows because $\Pi_{\boldsymbol{n},\lfloor\boldsymbol{n}/2\rfloor}^*$ is an algebra homomorphism and $\Pi_{\boldsymbol{n},\lfloor\boldsymbol{n}/2\rfloor}^*(x_{n_j/2,j}^{N/n_j}) = x_{0,j}^{N/n_j}$ for $j = j_1, j_2$. $\qquad\square$

We introduce some invariants which will play a key role in the construction of our separating set, as they did in the construction of separating sets for the indecomposable representations, see [6]. For $1 \leq j \leq k$ and $1 \leq i \leq \lfloor n_j/2 \rfloor$ define

$$f_{i,j} := \sum_{q=0}^{i-1}(-1)^q x_{q,j}x_{2i-q,j} + \frac{1}{2}(-1)^i x_{i,j}^2$$

and $f_{0,j} = x_{0,j}$. Also, for $1 \leq i \leq \lfloor \frac{n_j-1}{2} \rfloor$ set

$$s_{i,j} := \sum_{q=0}^{i}(-1)^q \frac{2i+1-2q}{2} x_{q,j}x_{2i+1-q,j}$$

and $s_{0,j} = x_{1,j}$. Note that we have $D_{(\boldsymbol{n})}(s_{i,j}) = f_{i,j}$ for $0 \leq i \leq \lfloor \frac{n_j-1}{2} \rfloor$. An element f in $\Bbbk[V_{(\boldsymbol{n})}]$ is called a local slice if $D_{(\boldsymbol{n})}(f) \in \Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$. For a non-zero element $f \in \Bbbk[V_{(\boldsymbol{n})}]$, let $\nu(f)$ denote the maximum integer d such that $D_{(\boldsymbol{n})}^d(f) \neq 0$. For a local slice s and an arbitrary polynomial f define

$$\epsilon_s(f) := \sum_{q=0}^{\nu(f)} \frac{(-1)^q}{q!}(D_{(\boldsymbol{n})}^q f)s^q(D_{(\boldsymbol{n})}s)^{\nu(f)-q}.$$

We remark that $\epsilon_s(f) \in \Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$. Furthermore, for $l'+1 \leq j \leq l$, we define $z_j := [x_{0,j}, f_{n_j/4,j}]^{n_j}$. We can now make our main result precise:

Theorem 4. *Let T denote the union of the following set of polynomials in $\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$.*

(1) $f_{i,j}$ for $1 \leq j \leq k$ and $0 \leq i \leq \lfloor n_j/2 \rfloor$.

(2) $\epsilon_{s_{i_2,j_2}}(x_{i_1,j_1})$ for $1 \leq j_1 < j_2 \leq k$, $\left\lfloor \frac{n_{j_1}-1}{2} \right\rfloor < i_1 \leq n_{j_1}$ and $0 \leq i_2 \leq \left\lfloor \frac{n_{j_2}-1}{2} \right\rfloor$.

(3) $\epsilon_{s_{i_2,j}}(x_{i_1,j})$ for $1 \le j \le k$, $0 \le i_2 \le \left\lfloor \frac{n_j-1}{2} \right\rfloor$, $i_2 \le i_1 \le n_j$.

(4) $\epsilon_{s_{i_2,j_2}}(x_{i_1,j_1})$ for $1 \le j_2 < j_1 \le k$, $0 \le i_1 \le n_{j_1}$, $0 \le i_2 \le \left\lfloor \frac{n_{j_2}-1}{2} \right\rfloor$.

(5) w_{j_1,j_2} for $1 \le j_1 \ne j_2 \le l'$.

(6) z_j for $l' + 1 \le j \le l$.

Then T is a separating set for $\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$.

Proof. We first show that the invariants labelled (1)-(4) above separate any pair of vectors that do not simultaneously lie in $\mathcal{V}_{V_{(\boldsymbol{n})}}(x_{i_2,j_2} \mid 1 \le j_2 \le k,\ 0 \le i_2 \le \left\lfloor \frac{n_{j_2}-1}{2} \right\rfloor)$. If $v_1 = (a_{i,j})$ and $v_2 = (b_{i,j})$ are any two such vectors, then there exists $1 \le j' \le k$ such that, for some $0 \le i' \le \left\lfloor \frac{n_{j'}-1}{2} \right\rfloor$, $a_{i',j'}$ and $b_{i',j'}$ are not simultaneously zero. We assume that i' and j' are minimal among such indices, that is, that we have

(1) $a_{i,j'} = b_{i,j'} = 0$ for $i < i'$.

(2) $a_{i,j} = b_{i,j} = 0$ for $j < j'$ and $0 \le i \le \left\lfloor \frac{n_j-1}{2} \right\rfloor$.

If exactly one of $a_{i',j'}$ and $b_{i',j'}$ is zero, then $f_{i',j'}$ separates v_1 and v_2. Otherwise the value of any invariant at v_1 and v_2 is determined by the set $\{f_{i',j'}, \epsilon_{s_{i',j'}}(x_{i_1,j_1}) \mid 0 \le i_1 \le n_{j_1},\ 1 \le j_1 \le k\}$. Indeed, as $D_{(\boldsymbol{n})} s_{i',j'} = f_{i',j'}$, the "Slice Theorem" [18, 2.1] implies that

$$\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}_{f_{i',j'}} = \Bbbk[\epsilon_{s_{i',j'}}(x_{i_1,j_1}) \mid 0 \le i_1 \le n_{j_1},\ 1 \le j_1 \le k]_{f_{i',j'}}.$$

On the other hand, if $i_1 < i'$ and $j_1 = j'$ or if $0 \le i_1 \le \left\lfloor \frac{n_{j_1}-1}{2} \right\rfloor$ and $j_1 < j'$, then $\epsilon_{s_{i',j'}}(x_{i_1,j_1})$ vanishes at v_1 and v_2. It follows that the set

$$f_{i',j'} \cup \{\epsilon_{s_{i',j'}}(x_{i_1,j_1}) \mid \left\lfloor \frac{n_{j_1}-1}{2} \right\rfloor < i_1 \le n_{j_1},\ j_1 < j'\} \cup \{\epsilon_{s_{i',j'}}(x_{i_1,j'}) \mid i' \le i_1 \le n_{j'}\}$$

$$\cup \{\epsilon_{s_{i',j'}}(x_{i_1,j_1}) \mid j' < j_1,\ 0 \le i_1 \le n_{j_1}\}$$

separates v_1 and v_2 whenever they are separated by some invariant.

It remains to show that T is a separating set on the zero set of the ideal $I := (x_{i_2,j_2} \mid 1 \le j_2 \le k,\ 0 \le i_2 \le \left\lfloor \frac{n_{j_2}-1}{2} \right\rfloor)$. Note that $\Bbbk[V_{(\boldsymbol{n})}]/I \cong \Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(\Bbbk[V_{(\boldsymbol{n})}]) = \Bbbk[V_{(\lfloor \boldsymbol{n}/2 \rfloor)}]$. Thus, finding a set which separates on $\mathcal{V}_{V_{(\boldsymbol{n})}}(I)$ is equivalent to finding a subset $E \subseteq \Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$ such that $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(E)$ separates the same points of $V_{(\lfloor \boldsymbol{n}/2 \rfloor)}$ as $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a})$. By Proposition 2, $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(\Bbbk[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}) \subseteq \Bbbk[x_{0,j} \mid 1 \le j \le l]^{C_2}$, where the cyclic group of order two C_2 acts as multiplication by -1 on the first l' variables and trivially on the remaining variables.

Consider the subset $B \subseteq \Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(T)$ formed by the following:

- $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(f_{\lfloor \boldsymbol{n}_j/2 \rfloor,j}) = x_{0,j}^2$, for $1 \le j \le l$,
- $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(w_{j_1,j_2}) = d x_{0,j_1}^{N/n_{j_1}} x_{0,j_2}^{N/n_{j_2}}$ for $1 \le j_1 \ne j_2 \le l'$, where $d \ne 0$ and N is the least common multiple of n_{j_1} and n_{j_1}.
- $\Pi^*_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}(z_j) = x_{0,j}^3$ for $l' + 1 \le j \le l$, see [6, Lemma 5.4].

Showing that B is a separating set for $\Bbbk[x_{0,j} \mid 1 \le j \le l]^{C_2}$ will end the proof. More precisely, we show that value of the generators of $\Bbbk[x_{0,j} \mid 1 \le j \le l]^{C_2}$ is entirely determined by the value of the elements of B. The ring of invariants is given by

$$\Bbbk[x_{0,j} \mid 1 \le j \le l]^{C_2} = \Bbbk[x_{0,j_1} x_{0,j_2}, x_{0,j} \mid 1 \le j_1 \le j_2 \le l',\ l' + 1 \le j \le l].$$

Suppose $1 \leq j_1 \neq j_2 \leq l'$. Note that N/n_{j_1} and N/n_{j_2} are odd integers. On points where either x_{0,j_1}^2 or x_{0,j_2}^2 is zero, so is $x_{0,j_1} x_{0,j_2}$. Otherwise, we have

$$x_{0,j_1} x_{0,j_2} = \frac{d x_{0,j_1}^{N/n_{j_1}} x_{0,j_2}^{N/n_{j_2}}}{d(x_{0,j_1}^2)^{1/2(N/n_{j_1}-1)}(x_{0,j_2}^2)^{1/2(N/n_{j_2}-1)}}.$$

Now suppose $l'+1 \leq j \leq l$. On points where $x_{0,j}^2$ is zero, so is $x_{0,j}$, and otherwise, $x_{0,j} = x_{0,j}^3/x_{0,j}^2$. Therefore $B \subseteq \Pi_{\boldsymbol{n},\lfloor \boldsymbol{n}/2 \rfloor}^*(T)$ is a separating set. $\qquad \square$

Theorem 1 is an easy consequence of Theorem 4:

Proof of Theorem 1 . The degree of the each invariant $f_{i,j}$ is two, and the invariants z_j all have degree three. The degree of w_{j_1,j_2} is $N/n_{j_1} + N/n_{j_2}$, where $N = \mathrm{lcm}(n_{j_1}, n_{j_2})$. Since $1 \leq j_1, j_2 \leq l'$, we have $N \leq (n_{j_1} n_{j_2})/2$ and so the degree of w_{j_1,j_2} is at most $(n_{j_1}+n_{j_2})/2$. Finally, the degree of $\varepsilon_{s_{i_2,j_2}}(x_{i_1,j_1})$ is $\deg(s_{i_2,j_2})i_1+1$ which is less than or equal to $2n_{j_1}+1$ which is in turn at most $2n-1$, since $n_j \leq n-1$ for all $1 \leq j \leq k$. It then follows that the degree of each invariant in T is at most $2n-1$, as claimed.

The number of invariants of the form $f_{i,j}$ in our separating set is

$$\sum_{j=1}^{k} \left\lfloor \frac{n_j}{2} \right\rfloor + 1 \leq \frac{n+k}{2}.$$

Since $1 \leq k \leq n$, this is linear in n. Note at this point that for each j_1, j_2, i_2 we have $\epsilon_{s_{i_2,j_2}}(x_{0,j_1}) = f_{0,j_1}$, so we have already counted these elements. The number of further invariants in T of the form $\varepsilon_{s_{i_2,j_2}}(x_{i_1,j_1})$ is

$$\sum_{j_2=1}^{k} \sum_{j_1=j_2+1}^{k} n_{j_1} \left\lfloor \frac{n_{j_2}+1}{2} \right\rfloor + \sum_{j=1}^{k} \sum_{i_2=0}^{\left\lfloor \frac{n_j-1}{2} \right\rfloor}(n_j - i_2 + 1) - 1 + \sum_{j_2=1}^{k} \sum_{j_1=1}^{j_2-1} \left\lfloor \frac{n_{j_1}+2}{2} \right\rfloor \left\lfloor \frac{n_{j_2}+1}{2} \right\rfloor.$$

Here the three terms correspond to the invariants labeled (4),(3), and (2) in our definition of T. Using that for any half-integer x we have $x - {}^1\!/{}_2 \leq \lfloor x \rfloor \leq x$ (which we also used to derive the third term above), the first term is bounded above by

$$\frac{1}{2} \sum_{j_2=1}^{k} \sum_{j_1=j_2+1}^{k} n_{j_1}(n_{j_2}+1)$$

$$\leq \frac{1}{4}\left(\left(\sum_{j_1=1}^{k} n_{j_1}\right)\left(\sum_{j_2=1}^{k} n_{j_2}\right) - \sum_{j=1}^{k} n_j^2\right) + \frac{k-1}{2} \sum_{j=1}^{k} n_j$$

$$= \frac{1}{4}(n-k)(n+k-2) - \frac{1}{4} \sum_{j=1}^{k} n_j^2.$$

For the same reason, the second term is bounded above by

$$\sum_{j=1}^{k} \frac{1}{2}(n_j+1)^2 - \sum_{j=1}^{k} \frac{1}{2} \frac{(n_j-2)}{2} \frac{n_j}{2} = \frac{3}{8} \sum_{j=1}^{k} n_j^2 + \text{ linear terms.}$$

The third term is bounded above by

$$\sum_{j_2=1}^{k} \sum_{j_1=1}^{j_2-1} \frac{(n_{j_1}+2)(n_{j_2}+1)}{4}$$

$$= \sum_{j_2=1}^{k} \sum_{j_1=1}^{j_2-1} \frac{(n_{j_1}+1)(n_{j_2}+1)}{4} + \sum_{j_2=1}^{k} \sum_{j_1=1}^{j_2-1} \frac{n_{j_2}+1}{4}$$

$$\leq \frac{1}{8}\sum_{j_1=1}^{k}\sum_{j_2=1}^{k}(n_{j_1}+1)(n_{j_2}+1) - \frac{1}{8}\sum_{j=1}^{k}(n_j+1)^2 + \frac{1}{4}\sum_{j_1=1}^{k}\sum_{j_2=1}^{k}(n_{j_2}+1) - \frac{1}{4}\sum_{j=1}^{k}(n_{j_2}+1)$$

$$= \frac{1}{8}n^2 - \frac{1}{8}\sum_{j=1}^{k}n_j^2 + \frac{1}{4}nk + \text{linear terms.}$$

Moreover, there are $\frac{1}{2}l'(l'-1)$ invariants of the form w_{j_1,j_2}, and $l-l'$ of the form z_j. Ignoring linear terms, the size of T is therefore bounded above by

$$\frac{1}{4}nk + \frac{3}{8}n^2 - \frac{1}{4}k^2 + \frac{1}{2}l'^2$$

which is indeed quadratic in n as claimed, since $l' \leq k$ and $k \leq n$. Note that when $k=1$ we get a separating set of size approximately $\frac{3}{8}n^2$, which coincides with the size of the separating set found in [6]. Indeed, our separating set specializes to the separating set found in [6] when $k=1$.

The following tables show the exact size of T for certain representations V of $\mathbb{G}_a$. It also shows the size of a minimal generating set $c_{\boldsymbol{n}}$ of $\mathbb{k}[V_{(\boldsymbol{n})}]^{\mathbb{G}_a}$, when this is known. The data for the numbers $c_{\boldsymbol{n}}$ was taken from Andries Brouwer's website [1]. Note that nV_k is taken to mean the direct sum of n copies of V_k. The generators of nV_1 which coincide with our separating set T were first conjectured by Nowicki [14], and first proved by Khoury [12]. The case nV_2 was recently solved by Wehlau [19].

V	$2V_2$	$3V_2$	$4V_2$	nV_2	V_3	$2V_3$	$3V_3$	$4V_3$	$5V_3$	nV_3
$\|T\|$	10	21	36	$2n^2+n$	7	24	51	108	135	$5n^2+2n$
$\|c_{\boldsymbol{n}}\|$	6	13	24	$\frac{1}{6}n(n^2+3n+8)$	4	26	97	280	689	?

V	V_4	$2V_4$	$3V_4$	$4V_4$	$5V_4$	nV_4	V_5	$2V_5$	nV_5	nV_6
$\|T\|$	11	35	75	128	195	$7n^2+4n$	16	56	$12n^2+4n$	$\frac{1}{2}(31n^2+9n)$
$\|c_{\boldsymbol{n}}\|$	5	28	103	305	?	?	23	?	?	?

V	$V_1\oplus V_2$	$V_1\oplus V_3$	$V_1\oplus V_4$	$V_1\oplus V_5$	$V_2\oplus V_3$	$V_2\oplus V_4$	$V_2\oplus V_5$	$V_3\oplus V_4$	$V_3\oplus V_5$
$\|T\|$	7	12	17	23	15	21	29	30	39
$\|c_{\boldsymbol{n}}\|$	5	13	20	94	15	18	92	63	?

To prove that T contains only invariants depending on at most two summands, simply observe that the invariants $f_{i,j}$ and z_j are non-zero only on the summand V_{n_j} of $V_{(\boldsymbol{n})}$, while $\varepsilon_{s_{i_2,j_2}}(x_{i_1,j_1})$ and w_{j_1,j_2} are non-zero on only on $V_{n_{j_1}}$ and $V_{n_{j_2}}$. $\qquad\square$

3. A NOTE ON HELLY DIMENSION

In [5], the authors define the *Helly dimension* of an algebraic group as follows:

Definition 2 (see [5, Definition 1.1])**.** The *Helly dimension* $\kappa(G)$ of an algebraic group is the minimal natural number d such that any finite system of closed cosets in G with empty intersection, has a subsystem consisting of at most d cosets with empty intersection. We define $\kappa(G) := \infty$, if there are no such natural numbers.

They go on to show that if $\Bbbk$ is a field of characteristic zero, and G acts on the affine $\Bbbk$-variety $X := \Pi_{i=1}^k X_i$, then there exists a dense G-stable open subset U of X and a set $S \subset \Bbbk[X]^G$ of invariants each depending on at most $\kappa(G)$ indecomposable factors of X such that S is a separating set on U [5, Theorem 4.1]. It is easy to see that the Helly dimension of $\mathbb{G}_a$ is two: in characteristic zero, the additive group does not have any proper nontrivial closed subgroups. That is, its only proper subgroup is $\{0\}$, and the only possible cosets are singletons. In particular, it follows from their work that for any product of $\mathbb{G}_a$-varieties, we should be able to find an ideal I of $\Bbbk[X]^{\mathbb{G}_a}$ and a set $S \subset \Bbbk[X]^{\mathbb{G}_a}$ of invariants each depending on at most two factors, such that S is a separating set on the open set $X \setminus \mathcal{V}(I)$. We recover this result for representations of $\mathbb{G}_a$ in the first part of the proof of Theorem 4. In fact, one could easily prove the same result directly for a product of arbitrary $\mathbb{G}_a$-varieties by applying the "Slice Theorem" with a local slice depending on just one factor.

For X a product of G-varieties, Domokos and Szabo also consider the quantities

$$\sigma(G, X) := \min\{d \mid \exists S \subset \Bbbk[X]^G, \text{ a separating set depending on } d \text{ factors of } X\},$$

and $\delta(G, X)$, defined as the minimum natural number d such that given $x \in X$ with Gx closed in X, there exists a set $\{j_1, j_2, \ldots, j_d\}$ such that the projection y of x onto the subvariety $Y := \Pi_{i=1}^d X_{j_i}$ has Gy closed in Y with the same dimension as Gx. The supremum of these quantities over all possible product varieties are denoted by $\sigma(G)$ and $\delta(G)$, respectively. They remark that for any unipotent group G, $\delta(G) \leq \dim(G)$ [5, Section 5], and in particular $\delta(\mathbb{G}_a) = 1$. Finally, they show that for any reductive group G, we have [5, Lemma 5.9]

$$\sigma(G) \leq \kappa(G) + \delta(G).$$

We do not know whether this inequality holds for non-reductive groups. If it did, it would follow that, given any affine $\mathbb{G}_a$-variety X, we could find a separating subset of $\Bbbk[X]^G$ depending on at most 3 indecomposable factors of X. Theorem 4(3) shows that, provided $\mathbb{G}_a$ acts linearly, two factors suffices. It would be interesting to know whether this holds for products of arbitrary affine $\mathbb{G}_a$-varieties.

REFERENCES

[1] Andries Brouwer. http://www.win.tue.nl/~aeb/math/invar.html.

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

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

[4] Harm Derksen and Gregor Kemper. Computing invariants of algebraic groups in arbitrary characteristic. *Adv. Math.*, 217(5):2089–2129, 2008.

[5] Mátyás Domokos and Endre Szabó. Helly dimension of algebraic groups. *J. Lond. Math. Soc. (2)*, 84(1):19–34, 2011.

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

[7] Peter Fleischmann. The Noether bound in invariant theory of finite groups. *Adv. Math.*, 156(1):23–32, 2000.

[8] John Fogarty. On Noether's bound for polynomial invariants of a finite group. *Electron. Res. Announc. Amer. Math. Soc.*, 7:5–7 (electronic), 2001.

[9] David Hilbert. *Theory of algebraic invariants*. Cambridge University Press, Cambridge, 1993. Translated from the German and with a preface by Reinhard C. Laubenbacher, Edited and with an introduction by Bernd Sturmfels.

[10] Gregor Kemper. Calculating invariant rings of finite groups over arbitrary fields. *J. Symbolic Comput.*, 21(3):351–366, 1996.

[11] Gregor Kemper. Computing invariants of reductive groups in positive characteristic. *Transform. Groups*, 8(2):159–176, 2003.

[12] Joseph Khoury. A Groebner basis approach to solve a conjecture of Nowicki. *J. Symbolic Comput.*, 43(12):908–922, 2008.

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

[14] Andrzej Nowicki. *Polynomial derivations and their rings of constants*. Uniwersytet Mikołaja Kopernika, Toruń, 1994.

[15] Peter J. Olver. *Classical invariant theory*, volume 44 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[16] David R. Richman. On vector invariants over finite fields. *Adv. Math.*, 81(1):30–65, 1990.

[17] Michael Roberts. On the Covariants of a Binary Quantic of the nth Degree. *The Quarterly Journal of Pure and Applied Mathematics*, 4:168–178, 1861.

[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] David Wehlau. Weitzenböck derivations of nilpotency 3. *Forum Math., to appear*, 2011.

MATHEMATISCHES INSTITUT, UNIVERSITÄT BASEL, RHEINSPRUNG 21, 4051 BASEL, SWITZERLAND
E-mail address: `emilie.dufresne@unibas.ch`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ABERDEEN, KING'S COLLEGE, ABERDEEN AB24 3UE, SCOTLAND
E-mail address: `j.elmer@abdn.ac.uk`

DEPARTMENT OF MATHEMATICS, BILKENT UNIVERSITY, ANKARA 06800, TURKEY
E-mail address: `sezer@fen.bilkent.edu.tr`