

# SEPARATING INVARIANTS AND FINITE REFLECTION GROUPS

EMILIE DUFRESNE

ABSTRACT. A separating algebra is, roughly speaking, a subalgebra of the ring of invariants whose elements distinguish between any two orbits that can be distinguished using invariants. In this paper, we introduce a geometric notion of separating algebra. This allows us to prove that only groups generated by reflections may have polynomial separating algebras, and only groups generated by bireflections may have complete intersection separating algebras.

## 1. INTRODUCTION

The study of separating invariants is a new trend in Invariant Theory initiated by Derksen and Kemper [4, 17]. It returns to the roots of Invariant Theory: using invariants to distinguish between the orbits of a group action on some geometric or algebraic space. Roughly speaking, a separating algebra is a subalgebra of the ring of invariants whose elements distinguish between any two orbits that can be distinguished using invariants. A separating set need not generate the ring of invariants. Separating algebras are often much better behaved than the ring of invariants. In contrast with the ring of invariants, a finitely generated separating algebra always exists, with no restrictions on the group (Theorem 2.3.15 in [4]); the polarization of separating invariants yields a separating set (Theorem 1.4 in [6]); for finite groups, the Noether bound holds for separating invariants (Corollary 3.9.14 in [4]).

In this paper, we introduce the notion of geometric separating algebra, a notion of separating algebra stable under extensions of the base field. But more importantly, we give two geometric formulations of this notion. These provide the keys to relating the structure of geometric separating algebras to the geometry of the representation.

Let  $G$  be a group, and let  $V$  be a finite dimensional representation of  $G$  over a field  $\mathbb{k}$ . Our first two results link the existence of polynomial geometric separating algebras to the presence of *reflections*, elements of  $G$  fixing a subspace of codimension 1 in  $V$ :

**Theorem 1.1.** *Let  $G$  be a finite group. If there exists a geometric separating algebra which is a polynomial ring, then the action of  $G$  on  $V$  is generated by reflections.*

Our method provides a new proof for the result of Serre [20] which established that only reflection groups may have polynomial rings of invariants. In Example 3.1 the ring of invariants is not polynomial, but we give a polynomial geometric separating algebra. Thus, Theorem 1.1 is a strict generalization of Serre's result.

An interesting consequence is a characterization, when the order of the group is invertible in the base field, of the existence of polynomial geometric separating algebras. It generalizes the well-known result of Shephard and Todd [21], Chevalley [2], Serre, and Clark and Ewing [3] which states that when the order of the group is invertible in the base field, the ring of invariants is polynomial if and only if the group is generated by reflections.

**Corollary 1.2.** *Let  $G$  be a finite group. If the characteristic of  $\mathbb{k}$  does not divide the order of  $G$ , then there exists a geometric separating algebra which is a polynomial ring if and only if the action of  $G$  on  $V$  is generated by reflections.*

Corollary 1.2 is new, even in characteristic zero. A version of it is an easy consequence of Theorem 1.6 of [17] (or Theorem 2.3.12 of [4]), but it requires the additional assumption that the polynomial separating algebra be graded and the base field algebraically closed.

Our third result generalizes a result of Gordeev [15], and Kac and Watanabe [15]. They proved that when the ring of invariants is a complete intersection, the group must be generated by *bireflections*, that is, elements of  $G$  fixing a subspace of codimension 2 in  $V$ .

**Theorem 1.3.** *Let  $G$  be a finite group. If there exists a graded geometric separating algebra which is a complete intersection, then the action of  $G$  on  $V$  is generated by bireflections.*

Examples where there is a geometric separating algebra which is a complete intersection abound. For example, for every 2-dimensional representations of finite abelian groups over  $\mathbb{C}$ , there is a geometric separating algebra which is a hypersurface (see [7]). The abundance of similarly well-behaved examples led to the question of whether there always existed such nice separating algebras (see the introduction of [18]). Example 4.1, due to Harm Derksen, shows that, in general, we can not expect an hypersurface geometric separating algebra to exist. His example, however, is of a representation of  $\mathbb{C}^*$ , and the technique he uses does not appear to be adaptable to finite groups.

Thus, the question remained open for finite groups. With Theorem 1.3, we provide some answers: if  $G$  is not generated by bireflections, no graded geometric separating algebra is a complete intersection, and in particular, no graded geometric separating algebra is a hypersurface.

Section 2 of this paper introduces the notion of geometric separating algebra, and more importantly, its two geometric formulations. In Section 3, we prove Theorems 1.1 and 1.2, and then discuss briefly some interesting examples, and questions arising from them. In Section 4, we prove Theorem 1.3, and end with Harm Derksen's example.

**Acknowledgements** I thank Harm Derksen for giving permission to include his example (Example 4.1). I also thank David Wehlau for his supervision during my graduate studies, and Mike Roth and Greg Smith for helpful conversations.

## 2. GEOMETRIC SEPARATING INVARIANTS

This section establishes the definitions and results needed throughout this text. It introduces the notion of geometric separating algebra and its two geometric formulations. Consider a linear algebraic group  $G$ , and a  $n$ -dimensional representation  $V$  of  $G$  over a field  $\mathbb{k}$ . We write  $\mathbb{k}[V]$  for the symmetric algebra on the vector space dual of  $V$ . The polynomial ring  $\mathbb{k}[V]$  has the standard grading. The action of the group  $G$  on  $V$  induces an action on  $\mathbb{k}[V]$ . Specifically, for a polynomial  $f$ , the action of an element  $\sigma$  of  $G$ , is given by  $(\sigma \cdot f)(u) = f(\sigma^{-1} \cdot u)$ , for  $u$  in  $V$ . We let  $\mathbb{k}[V]^G$  denote the ring formed by the elements of  $\mathbb{k}[V]$  fixed by the  $G$ -action. Since the group action preserves degree,  $\mathbb{k}[V]^G$  is a graded subalgebra of  $\mathbb{k}[V]$ .

By definition, elements of  $\mathbb{k}[V]^G$  are constant on  $G$ -orbits. Thus, if an invariant  $f$  takes distinct values on elements  $u$  and  $v$  of  $V$ , then we know that these elements belong to distinct orbits, that is,  $f$  separates  $u$  and  $v$ . A naive definition for a separating set would be to require that it separates elements  $u$  and  $v$  whenever they belong to distinct orbits. The ring of invariants, however, often does not distinguish the orbits (see, for example, Section 2.3.1 in [4]). Derksen and Kemper [4] and [17] define a *separating set* as a subset  $E$  of  $\mathbb{k}[V]^G$  such that for all  $u, v$  in  $V$ , if there exists  $f$  in  $\mathbb{k}[V]^G$  with  $f(u) \neq f(v)$ , then there exists  $h$  in  $E$  with  $h(u) \neq h(v)$ .

This definition yields interesting results: [17] uses the computation of a separating set as an intermediate step in the computation of a generating set for the invariants of reductive groups in positive characteristic; [5, 6] show the polarization of separating sets yields separating sets; [18] offers a generalization of separating sets to more general rings

of functions. Many of these results, however, require the base field to be algebraically closed; this notion of separating algebra behaves rather differently over non algebraically closed fields, and its behaviour over finite fields diverges even more from the situation over algebraically closed fields. The definition we suggest in the present paper is stable under extensions of the base field.

Let  $\bar{\mathbb{k}}$  be an algebraic closure of the field  $\mathbb{k}$ , and let  $\bar{V} = V \otimes_{\mathbb{k}} \bar{\mathbb{k}}$ , then  $\mathbb{k}[V] \subset \bar{\mathbb{k}}[\bar{V}]$ , and so any  $f$  in  $\mathbb{k}[V]$  can be considered as a function  $\bar{V} \rightarrow \bar{\mathbb{k}}$ . Moreover, we can extend the action of  $G$  on  $V$  to an action of  $G$  on  $\bar{V}$ . Thus, we can view  $\mathbb{k}[V]^G \subset \bar{\mathbb{k}}[\bar{V}]^G$ .

**Definition 2.1.** A subset  $E$  of  $\mathbb{k}[V]^G$  is a *geometric separating set* if, for all  $u$  and  $v$  in  $\bar{V}$ , the two following equivalent statements hold:

- if there exists  $f$  in  $\mathbb{k}[V]^G$  such that  $f(u) \neq f(v)$ , then there exists  $h$  in  $E$  such that  $h(u) \neq h(v)$ ;
- $f(u) = f(v)$ , for all  $f$  in  $\mathbb{k}[V]^G$  if and only if  $h(u) = h(v)$  for all  $h$  in  $E$ .

A subalgebra  $A \subset \mathbb{k}[V]^G$  satisfying these conditions is called a *geometric separating algebra*. If a subalgebra of  $\mathbb{k}[V]^G$  is generated by a geometric separating set, then it is a geometric separating algebra.

The adjective ‘‘Geometric’’ is often used to describe similar constructions. The strength of this new definition lies in the two geometric formulations presented below. In fact, for most of the results concerning separating invariants found in the literature, a geometric separating invariants version holds, often removing the requirement on  $\mathbb{k}$  to be algebraically closed (see [7]).

Our first geometric formulation of the definition of geometric separating algebra is a generalization to general groups and fields of some ideas of Kemper for reductive groups over algebraically closed fields (Section 2 of [17]). We write  $V$  for the affine scheme corresponding to  $\mathbb{k}[V]$ ,  $V//G$  for the affine scheme corresponding to  $\mathbb{k}[V]^G$ , and  $\pi$  for the morphism from  $V$  to  $V//G$  corresponding to the inclusion  $\mathbb{k}[V]^G \subset \mathbb{k}[V]$ .

**Definition 2.2.** The separating scheme  $\mathcal{S}_G$  is the unique reduced scheme having the same underlying topological space as the product  $V \times_{V//G} V$ , that is,  $\mathcal{S}_G := (V \times_{V//G} V)_{\text{red}}$ .

The separating scheme can be used to detect when a subalgebra  $A \subset \mathbb{k}[V]^G$  is a geometric separating algebra:

**Theorem 2.1.** *Let  $A \subset \mathbb{k}[V]^G$  be a subalgebra, then the following statements are equivalent:*

- (1)  *$A$  is a geometric separating algebra;*

- (2) if  $W = \text{Spec}(A)$ , then the natural morphism  $\mathcal{S}_G \rightarrow (V \times_W V)_{\text{red}}$  is an isomorphism;
- (3) if  $\delta$  denotes the map  $\delta : \mathbb{k}[V] \rightarrow \mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]$  sending an element  $f$  of  $\mathbb{k}[V]$  to  $f \otimes 1 - 1 \otimes f$ , then the ideals  $(\delta(A))$  and  $(\delta(\mathbb{k}[V]^G))$  have the same radical in the ring  $\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]$ , i.e.,

$$\sqrt{\delta(A)} = \sqrt{\delta(\mathbb{k}[V]^G)};$$

*Proof.* First, we prove (2) and (3) are equivalent. As  $V$ ,  $V//G$ , and  $W$  are affine schemes, we have  $V \times_{V//G} V = \text{Spec}(\mathbb{k}[V] \otimes_{\mathbb{k}[V]^G} \mathbb{k}[V])$ , and  $V \times_W V = \text{Spec}(\mathbb{k}[V] \otimes_A \mathbb{k}[V])$ . For any subalgebra  $B \subset \mathbb{k}[V]$ ,

$$\mathbb{k}[V] \otimes_B \mathbb{k}[V] = \frac{\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]}{(\delta(B))}.$$

Thus, (2) is equivalent to saying the  $\mathbb{k}$ -algebra homomorphism

$$\frac{\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]}{\sqrt{\delta(A)}} \rightarrow \frac{\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]}{\sqrt{\delta(\mathbb{k}[V]^G)}}$$

is an isomorphism, that is,  $\sqrt{\delta(A)} = \sqrt{\delta(\mathbb{k}[V]^G)}$ .

We now prove (1) and (3) are equivalent. If  $A$  is a geometric separating algebra, then for any  $u$  and  $v$  in  $\overline{V}$ ,  $f(u) = f(v)$  for all  $f$  in  $\mathbb{k}[V]^G$  if and only if  $h(u) = h(v)$  for all  $h$  in  $A$ . If  $\mathcal{I}_{\overline{V}^2}(u, v)$  denotes the maximal ideal of  $\overline{\mathbb{k}}[\overline{V}] \otimes_{\overline{\mathbb{k}}} \overline{\mathbb{k}}[\overline{V}]$  corresponding to the point  $(u, v)$  of  $\overline{V} \times \overline{V}$ , then we can rewrite this statement as:

$$\mathcal{I}_{\overline{V}^2}(u, v) \cap (\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]) \supset \delta(\mathbb{k}[V]^G)$$

if and only if

$$\mathcal{I}_{\overline{V}^2}(u, v) \cap (\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]) \supset \delta(A).$$

Since the maximal ideals of  $\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]$  are in bijection with Galois orbits of the maximal ideals of  $\overline{\mathbb{k}}[\overline{V}] \otimes_{\overline{\mathbb{k}}} \overline{\mathbb{k}}[\overline{V}]$ , the maximal ideals of  $\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]$  are exactly the primes of the form

$$\mathcal{I}_{\overline{V}^2}(u, v) \cap (\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]).$$

As  $\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]$  is a finitely generated  $\mathbb{k}$ -algebra, the radical of an ideal  $I$  is given by the intersection of all maximal ideals containing  $I$  (Theorem 5.5 of [19]). Therefore,  $\sqrt{\delta(\mathbb{k}[V]^G)} = \sqrt{\delta(A)}$ .  $\square$

*Remark 2.1.* The proof of Theorem 2.1 implies that a subset  $E \subset \mathbb{k}[V]^G$  is a geometric separating set if and only if  $\sqrt{\delta(\mathbb{k}[V]^G)} = \sqrt{\delta(E)}$ .

Under an additional hypothesis, we obtain another geometric formulation of geometric separation which involves the notion of radical morphism (Definition 3.5.4 in [8]). A map of schemes  $f : X \rightarrow Y$  is *radicial* if for any field  $\mathbb{F}$ , the corresponding map of  $\mathbb{F}$ -points is injective.

**Theorem 2.2.** *If  $G$  is reductive, then a subalgebra  $A \subset \mathbb{k}[V]^G$  is a geometric separating algebra if and only if the morphism of schemes  $\theta : V//G \rightarrow W = \text{Spec}(A)$  corresponding to the inclusion  $A \subset \mathbb{k}[V]^G$  is a radicial morphism.*

*Proof.* We write  $\gamma$  for the morphism of schemes corresponding to the inclusion  $\mathbb{k}[V] \subset \overline{\mathbb{k}}[\overline{V}]$ . By definition, a subalgebra  $A \subset \mathbb{k}[V]^G$  is a geometric separating algebra if and only if for  $u$  and  $v$  in  $\overline{V}$ , having  $\theta(\pi(\gamma(u))) = \theta(\pi(\gamma(v)))$  implies that  $\pi(\gamma(u)) = \pi(\gamma(v))$ . In other words,  $A$  is a geometric separating algebra if and only if  $\theta$  is injective on  $\overline{\mathbb{k}}$ -points in the image of  $\overline{V}$ .

On the other hand, since  $G$  is reductive,  $\pi$  is surjective (Lemma 1.3 in [16]), and any map  $\text{Spec}(\overline{\mathbb{k}}) \rightarrow V//G$  factors through  $V$ . Since  $\overline{V} \rightarrow V$  is also surjective,  $\text{Spec}(\overline{\mathbb{k}}) \rightarrow V$  factors through  $\overline{V}$ . Thus, all  $\overline{\mathbb{k}}$ -points of  $V//G$  are in the image of  $\overline{V}$ . Therefore,  $A$  is a geometric separating algebra if and only if  $\theta$  is injective on all  $\overline{\mathbb{k}}$ -points. But since  $V$  and  $W$  are of finite type over  $\overline{\mathbb{k}}$ , by Propositions 1.8.4 and 1.8.7.1 of [11] injectivity on  $\overline{\mathbb{k}}$ -points is equivalent to injectivity on any  $\mathbb{F}$ -points. It follows that  $A$  is a geometric separating algebra if and only if  $\theta$  is radicial.  $\square$

*Remark 2.2.* It follows from Theorem 2.2 that if we assume  $G$  is reductive, then finitely generated geometric separating algebras have the same dimension as the ring of invariants.

### 3. POLYNOMIAL GEOMETRIC SEPARATING ALGEBRAS

In this section, we prove Theorem 1.1 and Corollary 1.2, and then we provide non-trivial examples where there is a geometric separating algebra which is a polynomial ring. The following concrete description of the separating scheme for finite groups is a key element in our proof:

**Proposition 3.1.** *If  $G$  is a finite group, then the separating scheme is a union of  $|G|$  linear subspaces, each of dimension  $n$ . There is a natural correspondence between these linear spaces and the elements of  $G$ . Moreover, if  $H_\sigma$  and  $H_\tau$  denote the subspaces corresponding to the elements  $\sigma$  and  $\tau$  of  $G$ , respectively, then the dimension of the intersection  $H_\sigma \cap H_\tau$  is equal to the dimension of the subspace fixed by  $\tau^{-1}\sigma$  in  $V$ .*

*Proof.* For each  $\sigma \in G$ , let  $H_\sigma$  be the graph of  $\sigma$ , that is

$$H_\sigma = \{(u, \sigma \cdot u) \in V \times V \mid u \in V\}.$$

The linear space  $H_\sigma$  has dimension  $n$ . For elements  $\sigma$  and  $\tau$  of  $G$ , the intersection  $H_\sigma \cap H_\tau$  is  $\{(u, v) \in V \times V \mid u \in V \text{ and } v = \sigma \cdot u = \tau \cdot u\}$ .

Hence,  $H_\sigma \cap H_\tau$  is isomorphic to the fixed space of  $\tau^{-1}\sigma$ . Next, we show that

$$\mathcal{S}_G = \bigcup_{\sigma \in G} H_\sigma.$$

For each  $\sigma \in G$ ,  $H_\sigma$  is given as a closed subscheme of  $V \times V$  by the ideal  $(f \otimes 1 - 1 \otimes \sigma^{-1}f \mid f \in \mathbb{k}[V])$ . Thus, in algebraic terms, we want to show that

$$\frac{\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]}{\sqrt{(\delta(\mathbb{k}[V]^G))}} = \frac{\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]}{\bigcap_{\sigma \in G} (f \otimes 1 - 1 \otimes \sigma^{-1}f \mid f \in \mathbb{k}[V])}.$$

As  $G$  is finite, the ring of invariants separates orbits in  $\bar{V}$  (Lemma 2.1 in [6]), thus for  $u$  and  $v$  in  $\bar{V}$ ,  $f(u) = f(v)$ , for all  $f$  in  $\mathbb{k}[V]^G$ , if and only if there exists  $\sigma$  in  $G$  such that  $u = \sigma v$ . In other words,  $\delta(\mathbb{k}[V]^G) \subset \mathcal{I}_{\bar{V}^2}(u, v) \cap (\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V])$ , if and only if

$$\bigcap_{\sigma \in G} (f \otimes 1 - 1 \otimes \sigma^{-1}f \mid f \in \mathbb{k}[V]) \subset \mathcal{I}_{\bar{V}^2}(u, v) \cap (\mathbb{k}[V] \otimes_{\mathbb{k}} \mathbb{k}[V]).$$

Therefore,  $\sqrt{(\delta(\mathbb{k}[V]^G))} = \bigcap_{\sigma \in G} (f \otimes 1 - 1 \otimes \sigma^{-1}f \mid f \in \mathbb{k}[V])$ .  $\square$

We may now prove the two main results of this section.

*Proof of Theorem 1.1.* Suppose a separating algebra  $A$  is a polynomial ring. By Remark 2.2,  $A$  is  $n$ -dimensional, thus  $A$  is generated by  $n$  elements. It follows that the ideal  $(\delta(A))$  is also generated by  $n$  elements. Therefore,  $V \times_W V$  is a complete intersection, and in particular, it is Cohen-Macaulay. As  $V \times_W V$  is Noetherian, Hartshorne's Connectedness Theorem (Corollary 2.4 in [12]) implies that  $V \times_W V$  is connected in codimension 1, and thus, so is  $\mathcal{S}_G = (V \times_W V)_{\text{red}}$ .

Consider the irreducible components  $H_1$  and  $H_\sigma$  of  $\mathcal{S}_G$  corresponding to the identity and an arbitrary element  $\sigma$  of  $G$ , respectively. As  $\mathcal{S}_G$  is connected in codimension 1, there is a sequence of irreducible components

$$H_1 = H_{\sigma_0}, \dots, H_{\sigma_r} = H_\sigma,$$

such that  $H_{\sigma_i} \cap H_{\sigma_{i+1}}$  has codimension 1. By Proposition 3.1,  $\sigma_i^{-1}\sigma_{i+1}$  fixes a subspace of codimension 1, and so it acts as a reflection on  $V$ . Thus,  $\sigma = 1^{-1}\sigma = \sigma_0^{-1}\sigma_r = (\sigma_0^{-1}\sigma_1)(\sigma_1^{-1}\sigma_2) \cdots (\sigma_{r-1}^{-1}\sigma_r)$  is a product of reflections on  $V$ . Therefore, the action of  $G$  on  $V$  is generated by reflections.  $\square$

*Proof of Theorem 1.2.* One direction is given by Theorem 1.1, and as the ring of invariants is a geometric separating algebra, the other is an immediate consequence of the part of the result of Shephard and Todd

[21], Chevalley [2], Serre, and Clark and Ewing [3] which establishes that reflection groups have polynomial ring of invariants.  $\square$

The following example shows that it is possible for a geometric separating algebra to be polynomial even if the ring of invariants is not, showing that Theorem 1.1 is stronger than Serre's result.

*Example 3.1.* Let  $\mathbb{k}$  be a field of characteristic  $p$ , containing a root  $z$  of the irreducible polynomial  $Z^p - Z - 1$ . Let

$$G = \left\langle \left( \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ z & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

Let  $\{x_1, y_1, x_2, y_2\}$  be the dual basis for  $V^*$ . Using Proposition 3.1 of [1] (see [7] for details) we obtain that the ring of invariants of  $G$  is generated minimally by  $x_1, x_2, M_1, M_2$ , and  $h$ , where

$$\begin{aligned} M_1 &= (y_1^p - x_1^{p-1}y_1)^p - (x_1^p)^{p-1}(y_1^p - x_1^{p-1}y_1), \\ M_2 &= (y_2^p - x_2^{p-1}y_2)^p - (x_1^p - x_2^{p-1}x_1)^{p-1}(y_2^p - x_2^{p-1}y_2), \\ h &= (x_1^{p-1} - x_2^{p-1})(y_1^p - x_1^{p-1}y_1) - x_1^{p-1}(y_2^p - x_2^{p-1}y_2). \end{aligned}$$

Thus, the ring of invariants  $\mathbb{k}[V]^G$  is a hypersurface, and a generating relation is given by

$$h^p - (x_1^{p-1} - x_2^{p-1})^p M_1 + x_1^{p^2-p} M_2 - (x_1^p(x_1^{p-1} - x_2^{p-1}))^{p-1} h = 0.$$

We can rewrite this relation as

$$h^p = (x_1^{p-1} - x_2^{p-1})^p M_1 - x_1^{p^2-p} (M_2 - (x_1^{p-1} - x_2^{p-1})^{p-1} h).$$

As  $h$  and  $h^p$  separate the same points,

$$S = \{x_1, x_2, M_1, M_2 - (x_1^{p-1} - x_2^{p-1})^{p-1} h\}$$

is a geometric separating set which generates a polynomial geometric separating algebra.  $\triangleleft$

In [7] more examples are discussed, including another similar infinite family. As required by Theorem 1.1, all the group actions involved are generated by reflections. But they have more in common: they act as rigid groups, i.e., the actions of all their isotropy subgroups are generated by reflections. We do not expect polynomial geometric separating algebras to exist for all rigid groups. On the other hand, we suspect that rigid groups are the only ones for which polynomial separating algebras can exist.

## 4. COMPLETE INTERSECTION GEOMETRIC SEPARATING ALGEBRAS

In this section, we prove Theorem 1.3, and then present an example. Our proof extends the argument used by Kac and Watanabe to prove their Theorem A in [15], and it exploits the second geometric formulation of the notion of geometric separating algebra. The statement of Theorem 1.3 concerns graded separating algebras. Assuming that a geometric separating algebra  $A$  is graded imposes a very close relationship with the ring of invariants  $\mathbb{k}[V]^G$ :

**Proposition 4.1.** *Let  $A \subset \mathbb{k}[V]^G$  be a graded subalgebra. If the map of schemes  $\theta : V//G \rightarrow W = \text{Spec}(A)$  is injective, then the extension  $A \subset \mathbb{k}[V]^G$  is integral.*

*Proof.* Let  $A_+$  and  $\mathbb{k}[V]_+^G$  denote the maximal graded ideals of  $A$  and  $\mathbb{k}[V]^G$ , respectively. If  $\mathfrak{p}$  is a proper prime ideal of  $\mathbb{k}[V]^G$  containing  $A_+\mathbb{k}[V]^G$ , then

$$A_+ \subset A_+\mathbb{k}[V]^G \cap A \subset \mathfrak{p} \cap A \subset A.$$

As  $A_+$  is a maximal ideal,  $\mathfrak{p} \cap A = A_+$ .

On the other hand,  $A_+ = \mathbb{k}[V]_+^G \cap A$ . Thus, the injectivity of  $\theta$  implies  $\mathfrak{p} = \mathbb{k}[V]_+^G$ , and the radical of  $A_+\mathbb{k}[V]^G$  in  $\mathbb{k}[V]^G$  is  $\mathbb{k}[V]_+^G$ . It follows that  $\mathbb{k}[V]^G/A_+\mathbb{k}[V]^G$  has Krull dimension 0, i.e., it is a finite dimensional  $\mathbb{k}$ -vector space. By the graded version of Nakayama's Lemma (Lemma 3.5.1 in [4]),  $\mathbb{k}[V]^G$  is a finite  $A$ -module, and so the extension  $A \subset \mathbb{k}[V]^G$  is integral.  $\square$

**Corollary 4.2.** *If the action of  $G$  on  $V$  is reductive, and if  $A \subset \mathbb{k}[V]^G$  is a graded geometric separating algebra, then the extension  $A \subset \mathbb{k}[V]^G$  is integral.*

*Proof.* By Theorem 2.2, the morphism of schemes  $\theta : V//G \rightarrow W$  is radicial. As radicial morphism of schemes are injective (Proposition 3.5.8 in [8]), and as  $A$  is assumed to be graded, the corollary follows directly from Proposition 4.1.  $\square$

We can now prove the main result of this section:

*Proof of Theorem 1.3.* Without loss of generality, we may assume that the base field is algebraically closed. Indeed, if  $A$  is a complete intersection graded geometric separating algebra inside of  $\mathbb{k}[V]^G$ , then  $A \otimes_{\mathbb{k}} \bar{\mathbb{k}}$  is a complete intersection and a graded geometric separating algebra inside of  $\mathbb{k}[\bar{V}]^G$ . Assuming the theorem holds over algebraically closed fields, it follows that  $G$  is generated by bireflection on  $\bar{V}$ . Thus, the action of  $G$  on  $V$  is also generated by bireflections.

Since  $G$  is finite, it is reductive, and so Theorem 2.2 implies that  $\theta$  is a radicial morphism. As  $A$  is graded, Corollary 4.2 implies  $\theta$  is finite. Finally, since  $\theta$  is dominant and finite it is also surjective.

Now, let  $\widehat{\mathbb{k}[V]}$ ,  $\widehat{\mathbb{k}[V]^G}$ , and  $\widehat{A}$  be the completions of  $\mathbb{k}[V]$ ,  $\mathbb{k}[V]^G$ , and  $A$  at their maximal graded ideal  $\mathbb{k}[V]_+$ ,  $\mathbb{k}[V]^G_+$ , and  $A_+$ , respectively. A scheme is *simply connected* if and only if there are no nontrivial étale coverings ([13], Example 2.5.3). As complete local rings satisfy Hensel's Lemma, by Theorem 5.2 in [14], the affine schemes corresponding to the completions are simply connected. The  $G$ -action on  $\mathbb{k}[V]$  extends to a  $G$ -action on  $\widehat{\mathbb{k}[V]}$ , and  $\widehat{\mathbb{k}[V]^G} = (\widehat{\mathbb{k}[V]})^G$ . Thus  $\text{Spec}(\widehat{\mathbb{k}[V]^G}) = \widehat{V} // G$ , and the finite morphism  $\pi$  lifts to the quotient morphism  $\widehat{\pi} : \widehat{V} \rightarrow \widehat{V} // G$ , which remains finite. Since  $\widehat{\mathbb{k}[V]^G} = \mathbb{k}[V]^G \otimes_A \widehat{A}$  (Theorem 9.3A in [13]), taking the completion corresponds to doing a base change. Hence,  $\theta$  lifts to a morphism  $\widehat{\theta}$  which is surjective, radicial, and finite, since all three properties are preserved by base changes: see Propositions 3.5.2 and 3.5.7 in [8], and 6.1.5 in [9], respectively.

For  $\sigma$  in  $G$  we let  $\widehat{V}^\sigma$  denote the subscheme of fixed points of  $\sigma$  on  $\widehat{V}$ . Let  $L$  be the union of all the  $\widehat{V}^\sigma$ 's with codimension at least 3, and put  $M = \widehat{\pi}(L)$ , and  $N = \widehat{\theta}(M)$ . Since  $W$  is a complete intersection, Proposition 3.2 of [12] implies  $\widehat{W} = \text{Spec}(\widehat{A})$  is also a complete intersection. Since  $\widehat{\pi}$  and  $\widehat{\theta}$  are finite,  $N$  has codimension 3 in  $\widehat{W}$ . Hence, by Lemma 1 from [15],  $\widehat{W} \setminus N$  is simply connected. As the restriction of  $\widehat{\theta}$  to  $\widehat{V} // G \setminus M$  is radicial, surjective, and finite, by Theorem 4.10 of [10], it follows that  $(\widehat{V} // G) \setminus M$  is also simply connected.

Furthermore,  $X = \widehat{V} \setminus L$  is an integral scheme with the induced  $G$ -action, and  $(\widehat{V} // G) \setminus N = X // G$ . Since  $X // G$  is simply connected, Lemma 2 from [15] implies that the group  $G$  is generated by the set  $\{G_x \mid x \in X = \widehat{V} \setminus L\}$ . But by the definition of  $\widehat{V} \setminus L$ , an element  $\sigma$  belongs to  $G_x$  for some  $x \in \widehat{V} \setminus L$  if and only if  $\text{codim}(\widehat{V}^\sigma) \leq 2$ . Hence,  $G$  is generated by bireflections.  $\square$

Derksen's example of a representation for which no geometric separating algebra is a hypersurface follows:

*Example 4.1* (Harm Derksen). Let  $t$  in  $G = \mathbb{C}^*$  act on the polynomial ring  $\mathbb{C}[x_1, x_2, x_3, y_1, y_2]$ , as

$$\begin{pmatrix} t & 0 & 0 & 0 & 0 \\ 0 & t & 0 & 0 & 0 \\ 0 & 0 & t & 0 & 0 \\ 0 & 0 & 0 & t^{-1} & 0 \\ 0 & 0 & 0 & 0 & t^{-1} \end{pmatrix}.$$

Monomials are sent to scalar multiples of themselves, and so the ring of invariants is generated by monomials. In fact,

$$\mathbb{C}[V]^{\mathbb{C}^*} = \mathbb{C}[x_1y_1, x_2y_1, x_3y_1, x_1y_2, x_2y_2, x_3y_2].$$

The dimension of  $\mathbb{C}[V]^{\mathbb{C}^*}$  is equal to its transcendence degree (i.e., the maximal number of algebraically independent elements). The set  $\{x_1y_1, x_3y_1, x_1y_2, x_2y_2\}$  forms a transcendence basis for  $\mathbb{C}[V]^{\mathbb{C}^*}$ . Indeed, they are clearly algebraically independent, and the relations  $(x_1y_1)(x_3y_2) = (x_3y_1)(x_1y_2)$  and  $(x_2y_2)(x_1y_1) = (x_2y_1)(x_1y_2)$  give  $x_3y_2$  and  $x_2y_2$  as roots of polynomials in the other generators. Thus,  $\mathbb{C}[V]^{\mathbb{C}^*}$  has dimension 4.

As the group is reductive, by Remark 2.2, geometric separating algebras have dimension 4. Thus, a geometric separating algebra is a hypersurface if it is generated by 5 elements. We will prove that there are no geometric separating sets of 5 elements.

Suppose, by way of contradiction, that  $f_1, f_2, f_3, f_4, f_5$  is a geometric separating set. As the  $f_i$ 's are invariant, we can write:

$$f_i = F_i(x_1y_1, x_2y_1, x_3y_1, x_1y_2, x_2y_2, x_3y_2),$$

where each  $F_i$  is a polynomial in  $\mathbb{C}[z_1, z_2, z_3, z_4, z_5, z_6]$ . The ideal generated by the 5 polynomials  $F_i(z_1, z_2, z_3, 0, 0, 0) - F_i(0, 0, 0, z_4, z_5, z_6)$ , for  $i = 1, \dots, 5$ , corresponds to a subvariety of  $\mathbb{C}^6$  which is either empty or has dimension at least 1. As the point  $(0, 0, 0, 0, 0, 0)$  is a common zero, there are infinitely many solutions, in particular there is a non-zero solution  $(a, b, c, d, e, f)$ . If  $u = (a, b, c, 1, 0)$ , and  $v = (d, e, f, 0, 1)$ , then for all  $i = 1, \dots, 5$

$$f_i(u) = F_i(a, b, c, 0, 0, 0) = F_i(0, 0, 0, d, e, f) = f_i(v),$$

that is, the  $f_i$ 's do not separate  $u$  and  $v$ . We have, however,

$$\begin{aligned} x_1y_1(u) &= a, & x_1y_1(v) &= 0, \\ x_2y_1(u) &= b, & x_2y_1(v) &= 0, \\ x_3y_1(u) &= c, & x_3y_1(v) &= 0, \\ x_1y_2(u) &= 0, & x_1y_2(v) &= d, \\ x_2y_2(u) &= 0, & x_2y_2(v) &= e, \\ x_3y_2(u) &= 0, & x_3y_2(v) &= f, \end{aligned}$$

and as  $(a, b, c, d, e, f)$  is nonzero, this is a contradiction. We conclude that no geometric separating algebra is a hypersurface.  $\triangleleft$

## REFERENCES

- [1] H. E. A. Campbell and I.P. Hughes. Rings of Invariants of Certain  $p$ -Groups over the Field  $\mathbb{F}_p$ . *J. Algebra*, 211:549–561, 1998.
- [2] Claude Chevalley. Invariants of Finite Groups Generated by Reflections. *Amer. J. Math.*, 77:778–782, 1955.

- [3] Allan Clark and John Ewing. The Realization of Polynomial Algebras as Co-homology Rings. *Pacific J. Math.*, 50:425–434, 1974.
- [4] Harm Derksen and Gregor Kemper. *Computational Invariant Theory*. Number 130 in Encyclopædia of Mathematical Sciences. Springer-Verlag, Berlin, Heidelberg, New York, 2002.
- [5] Mátyás Domokos. Typical separating invariants. *Transform. Groups*, 12(1):49–63, 2007.
- [6] Jan Draisma, Gregor Kemper, and David Wehlau. Polarization of Separating Invariants. *Can. J. Math.*, 2008.
- [7] Emilie Dufresne. *Separating Invariants*. PhD thesis, Queen’s University, Kingston, Ontario, Canada, in preparation.
- [8] Alexander Grothendieck. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.
- [9] Alexander Grothendieck. Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes. *Inst. Hautes Études Sci. Publ. Math.*, (8):222, 1961.
- [10] Alexander Grothendieck. *Revêtements étales et groupe fondamental. Fasc. II: Exposés 6, 8 à 11*, volume 1960/61 of *Séminaire de Géométrie Algébrique*. Institut des Hautes Études Scientifiques, Paris, 1963.
- [11] Alexander Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I. *Inst. Hautes Études Sci. Publ. Math.*, (20):259, 1964.
- [12] Robin Hartshorne. Complete Intersection and Connectedness. *Amer. J. Math.*, 84.
- [13] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.
- [14] Birger Iversen. *Generic Local Structure of the Morphisms in Commutative Algebra*. Lecture Notes in Mathematics, Vol. 310. Springer-Verlag, Berlin, 1973.
- [15] Victor Kac and Kei-Ichi Watanabe. Finite Linear Groups whose Ring of Invariants is a Complete Intersection. *Bull. (New Series) of the AMS*, 6(2).
- [16] Gregor Kemper. A Characterization of Linear Reductive Groups by their Invariants. *Transformation Groups*, 5(1):1–8, 2000.
- [17] Gregor Kemper. Computing Invariants of Reductive Groups in Positive characteristic. *Transformation Groups*, 8(2):158–176, 2003.
- [18] Gregor Kemper. Separating Invariants. *J. Symbolic Computation*, to appear.
- [19] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.
- [20] Jean-Pierre Serre. Groupes finis d’automorphismes d’anneaux locaux réguliers. In *Colloque d’Algèbre (Paris, 1967)*, Exp. 8, page 11. Secrétariat mathématique, Paris, 1968.
- [21] G. C. Shephard and J. A. Todd. Finite Unitary Reflection Groups. *Canadian J. Math.*, 6:274–304, 1954.

DEPARTMENT OF MATHEMATICS AND STATISTICS, QUEEN’S UNIVERSITY, JEFFERY HALL, UNIVERSITY AVENUE, KINGSTON, ON, CANADA, K7L 3N6  
*E-mail address:* emilie@mast.queensu.ca