THE COHEN-MACAULAY PROPERTY OF SEPARATING INVARIANTS OF FINITE GROUPS

EMILIE DUFRESNE, JONATHAN ELMER, AND MARTIN KOHLS

Abstract. In the case of finite groups, a separating algebra is a subalgebra of the ring of invariants which separates the orbits. Although separating algebras are often better behaved than the ring of invariants, we show that many of the criteria which imply the ring of invariants is non Cohen-Macaulay actually imply that no graded separating algebra is Cohen-Macaulay. For example, we show that, over a field of positive characteristic p, given sufficiently many copies of a faithful modular representation, no graded separating algebra is Cohen-Macaulay. Furthermore, we show that, for a p-group, the existence of a Cohen-Macaulay graded separating algebra implies the group is generated by bireflections. Additionally, we give an example which shows that Cohen-Macaulay separating algebras can occur when the ring of invariants is not Cohen-Macaulay.

1. Introduction

Let G be a finite group, and let V be a finite dimensional representation of G over a field $\Bbbk$ of characteristic $p \geq 0$. We say V is a modular representation if p divides $|G|$. We write $\Bbbk[V]$ for the symmetric algebra $S(V^*)$ on the vector space dual of V. It is a polynomial ring with the standard grading. The action of G on V induces an action on $\Bbbk[V]$: for $f \in V^*$ and $v \in V$, the action of $\sigma \in G$ is given by $(\sigma \cdot f)(v) = f(\sigma^{-1} \cdot v)$. The ring of invariants, denoted $\Bbbk[V]^G$, is the ring formed by the elements of $\Bbbk[V]$ fixed by G. Since the group action preserves degree, $\Bbbk[V]^G$ is a graded subalgebra of $\Bbbk[V]$.

Let $\overline{\Bbbk}$ be an algebraic closure of the field $\Bbbk$, and let $\overline{V} = \overline{\Bbbk} \otimes_{\Bbbk} V$. As $\Bbbk[V] \subseteq \overline{\Bbbk} \otimes_{\Bbbk} \Bbbk[V] \cong \overline{\Bbbk}[\overline{V}]$, any f in $\Bbbk[V]$ can be considered as a function $\overline{V} \to \overline{\Bbbk}$. The action of G on V extends to an action of G on $\overline{V}$, and so $\Bbbk[V]^G \subseteq \overline{\Bbbk}[\overline{V}]^G$.

By definition, elements of $\Bbbk[V]^G$ are constant on G-orbits. Accordingly, if an invariant f takes distinct values on elements $u, v \in \overline{V}$, then these elements belong to distinct orbits, and we say f *separates* u and v. A *geometric separating set* is then a set of invariants which separates exactly the same points of $\overline{V}$ as the whole ring of invariants. As G is finite, the ring of invariants separates orbits in $\overline{V}$ [11, Lemma 2.1].

Date: August 12, 2009.

Hence, a geometric separating set is a set of invariants which separates the orbits of the G-action on $\overline{V}$.

The study of separating invariants, which has become quite popular in recent years, was initiated by Derksen and Kemper ([8, Section 2.3] and [24]). They defined a *separating set* as a set separating the same orbits in V as the whole ring of invariants [8, Definition 2.3.8]. For $\Bbbk$ algebraically closed, geometric separating sets coincide with separating sets, but in general, a separating set is not always a geometric separating set (see Example 2.5). On the other hand, $A \subseteq \Bbbk[V]^G$ is a geometric separating algebra if and only if $\overline{\Bbbk} \otimes_{\Bbbk} A \subseteq \overline{\Bbbk}[\overline{V}]^G$ is a separating algebra. Moreover, if A is graded, so is $\overline{\Bbbk} \otimes_{\Bbbk} A$, and the two rings have the same dimension and depth. Furthermore, the extension $A \subseteq \Bbbk[V]^G$ is integral if and only if $\overline{\Bbbk} \otimes_{\Bbbk} A \subseteq \overline{\Bbbk}[\overline{V}]^G$ is integral. Thus, it often suffices to write proofs for separating sets over algebraically closed fields. Note that this works only because we are interested in geometric separating algebras.

Many defects of invariant rings disappear when one considers separating invariants. The ring of invariants is not always finitely generated (for non-reductive groups) [8, Example 2.1.4, due to Nagata], but there always exist finite geometric separating sets [8, Theorem 2.3.15]. Over algebraically closed fields, there is an upper bound on the size of minimal separating sets, depending only on the dimension of the representation [12, Proposition 5.1.1]. Polarization, a classical method for obtaining vector invariants in characteristic zero, extends, for separating invariants, to all characteristics [11, 10]. For G finite, the Noether bound holds for separating invariants in all characteristics: although they may not generate the ring of invariants, the invariants of degree at most $|G|$ always form a geometric separating set [8, Section 3.9].

Graded separating algebras are very closely related to the ring of invariants:

Proposition 1.1. *If $A \subseteq \Bbbk[V]^G$ is a graded geometric separating algebra, then $A \subseteq \Bbbk[V]^G$ is an integral extension, and A is a finitely generated $\Bbbk$-algebra.*

Proof. We may assume $\Bbbk$ is algebraically closed. By [24, Lemma 1.3], the extension $A \subseteq \Bbbk[V]^G$ is integral. The finite generation of A as a $\Bbbk$-algebra then follows from that of $\Bbbk[V]^G$ by Newstead [26, p. 52, (II)], or in the manner of [1, Proof of Theorem 1.3.1]. □

Proposition 1.2. *Suppose $p > 0$. If $A \subseteq \Bbbk[V]^G$ is a graded subalgebra, then A is a geometric separating algebra if and only if $\Bbbk[V]^G$ is the purely inseparable closure of A in $\Bbbk[V]$, that is,*

$$\Bbbk[V]^G = \{f \in \Bbbk[V] \mid \quad \textit{for some } m,\ f^{p^m} \in A\}.$$

Proof. For $\Bbbk$ algebraically closed, see [9, Remark 1.3]. The proof is an application of a result of van der Kallen [28, Sublemma A.5.1] (see the extended proof in [27]). A variation of the same argument first appeared in [19, Theorem 6]. For $f \in \Bbbk[V]^G$ and $\Bbbk$ arbitrary, we have that $f^{p^m} \in \overline{\Bbbk} \otimes_{\Bbbk} A$ for some m. The stability of the rank of matrices under field extensions implies $f^{p^m} \in A$. □

Remark 1.3. Propositions 1.1 and 1.2 hold for rational representations of reductive groups.

Kemper [24] exploited this close relationship to compute the invariants of reductive groups in positive characteristic. On the other hand, Dufresne [13] showed that the existence of polynomial or complete intersection separating algebras imposes strong conditions on the representation. The present paper is in the latter vein. We show that, in many instances, conditions which ensure that the ring of invariants is non Cohen-Macaulay, in fact imply that no graded geometric separating algebra is Cohen-Macaulay. We thus provide a (partial) negative answer to Kemper who asked if Cohen-Macaulay separating algebras should always exist [25]. Notably, we show:

Theorem 1.4. *If V is faithful and modular, then there exists $r \geq 1$ such that, for all k, every graded geometric separating algebra in $\Bbbk[V^{\oplus k}]^G$ has Cohen-Macaulay defect at least $k - r - 1$. In particular, for $k > r + 1$, no graded geometric separating algebra in $\Bbbk[V^{\oplus k}]^G$ is Cohen-Macaulay.*

An element σ of G acts as a *bireflection* on V if its fixed space is of codimension at most 2 in V.

Theorem 1.5. *Let G be a p-group. If there exists a graded geometric separating algebra in $\Bbbk[V]^G$ which is Cohen-Macaulay, then G is generated by elements acting as bireflections.*

Theorem 1.5 fits well with [13, Theorem 1.3]. In the important special case of p-groups, we obtain that G is generated by bireflections from a much weaker hypothesis: the existence of a Cohen-Macaulay rather than a complete intersection graded geometric separating algebra. This mirrors the situation for invariant rings ([22, Corollary 3.7] and [21, Theorem A]). Example 2.10 shows that not only the converse of Theorem 1.5, but also the converses of [13, Theorem 1.1 and Theorem 1.3], are not true.

In Section 2, we extend the methods introduced in [22] to prove our main results. Section 3 concentrates on the alternating group A_4. We conclude in Section 4 with a discussion of the general situation and examples which show that the depth of graded geometric separating algebras can be both larger and smaller than that of the corresponding invariant ring.

Acknowledgements. This paper was prepared during visits of the first and second authors to TU München, and of the second and third authors to Universität Heidelberg. We thank Gregor Kemper, B. Heinrich Matzat, and MATCH for making these visits possible. Finally, we thank the anonymous referees for helpful suggestions, in particular for pointing out an error in our original proof of Lemma 2.2.

2. The Cohen-Macaulay Defect of Separating Algebras

Let $A \subseteq \Bbbk[V]$ be a finitely generated graded subalgebra, and let A_+ denote its maximal homogeneous ideal. Homogeneous elements $a_1, \dots, a_k$ in A_+ form a *partial homogeneous system of parameters (phsop)* if they generate an ideal of height k in A. If additionally $k = \dim A$, then they form a *homogeneous system of parameters (hsop)*. Noether's normalization theorem guarantees that a hsop always exists. If, for $i = 1, \dots, k$, the element a_i is not a zero divisor in $A/(a_1, \dots, a_{i-1})A$, then the elements $a_1, \dots, a_k$ form a *regular sequence*. Every regular sequence is a phsop. We say A is *Cohen-Macaulay* when every phsop is a regular sequence. The depth of a homogeneous ideal $I \subseteq A_+$, written $\operatorname{depth}_A(I)$, is the maximal length of a regular sequence in I. Note that the height of I, $\operatorname{ht}(I)$, is equal to the maximal length of a phsop in I. We write $\operatorname{depth}(A) := \operatorname{depth}_A(A_+)$, and define the *Cohen-Macaulay defect* of A to be $\operatorname{cmdef}(A) := \dim A - \operatorname{depth}(A)$. Thus, A is Cohen-Macaulay precisely when $\operatorname{cmdef} A = 0$.

In Theorem 2.1, we relate the Cohen-Macaulay defect of graded geometric separating algebras to the n-th cohomology group $H^n(G, \overline{\Bbbk}[\overline{V}])$. For the theory of these groups for arbitrary n, we refer to [2, 29]. Since we have $n = 1$ in most applications of this theorem, we construct this group now.

Let W be a representation of the group G over the field $\Bbbk$. A *1-cocycle* is a map $g : G \to W$, $\sigma \mapsto g_\sigma$ such that $g_{\sigma\tau} = \sigma g_\tau + g_\sigma$, for all $\sigma, \tau \in G$. We write $Z^1(G, W)$ for the additive group of all 1-cocycles. For each $w \in W$, the map given by $\sigma \mapsto (\sigma - 1)w := \sigma w - w$ is a 1-cocycle, which is called a *1-coboundary*. The coboundaries form the subgroup $B^1(G, W)$ of $Z^1(G, W)$. The *first cohomology group of G with coefficients in W* is the quotient group $H^1(G, W) := Z^1(G, W)/B^1(G, W)$. A cocycle g is *nontrivial* if and only if its *cohomology class* $g + B^1(G, W)$ is nonzero in $H^1(G, W)$. Similar definitions hold for $H^n(G, W)$. We will sometimes abuse notation by using the same symbols for cocycles and cohomology classes.

The group $H^n(G, \Bbbk[V])$ has a natural graded $\Bbbk[V]^G$-module structure. For a homogeneous $g \in H^n(G, \Bbbk[V])$, its annihilator in $\Bbbk[V]^G$,

$$\operatorname{Ann}_{\Bbbk[V]^G}(g) := \{a \in \Bbbk[V]^G : ag = 0 \in H^n(G, \Bbbk[V])\},$$

is a homogeneous ideal. If $p > 0$, the m-fold Frobenius homomorphism $\Bbbk[V] \to \Bbbk[V]$, $f \mapsto f^{p^m}$, induces a map $H^n(G, \Bbbk[V]) \to H^n(G, \Bbbk[V])$. This map is a homomorphism of abelian groups, but not of $\Bbbk$-vector spaces. We write g^{p^m} for the image of an element $g \in H^n(G, \Bbbk[V])$

under this map. In particular, for $g \in H^1(G, \Bbbk[V])$, the cohomology class $g^{p^m} \in H^1(G, \Bbbk[V])$ is given by the cocycle $\sigma \mapsto (g_\sigma)^{p^m}$.

Over fields of characteristic zero, and in the non-modular case in general, the ring of invariants is always Cohen-Macaulay [20]. In particular, there will always be a Cohen-Macaulay geometric separating algebra. Accordingly, from now on we assume V is modular.

Our most general statement generalizes [22, Corollary 1.6] (see also [23, Proposition 6]) to the case of separating algebras:

Theorem 2.1. *Let $n \geq 1$ be the smallest integer such that there exists a homogeneous $g \in H^n(G, \overline{\Bbbk}[\overline{V}])$ such that g^{p^m} is nonzero for every $m \geq 0$. If A is a graded geometric separating algebra in $\Bbbk[V]^G$, then $I := \mathrm{Ann}_A(g)$, the annihilation ideal of g in A, has depth at most $n+1$. Furthermore, if $\mathrm{Ann}_{\overline{\Bbbk}[\overline{V}]^G}(g)$ has height k, then A has Cohen-Macaulay defect at least $k-n-1$.*

Since the case $n = 1$ suffices for most of our applications, we give an additional more elementary proof of the first part. Without loss of generality, we assume $\Bbbk = \overline{\Bbbk}$ in both arguments.

Proof of the case $n = 1$. By Proposition 1.2, there exists a p-power q such that $(\Bbbk[V]^G)^q \subseteq A$. Suppose, for a contradiction, that $\mathrm{depth}_A(I)$ is at least 3. Hence, there exists an A-regular sequence a_1, a_2, a_3 in I. Since $a_i g = 0$, there are $b_1, b_2, b_3 \in \Bbbk[V]$ such that

$$a_i g_\sigma = (\sigma - 1)b_i, \quad \text{for all } \sigma \in G,\ i = 1, 2, 3.$$

Set $u_{ij} := a_i b_j - a_j b_i$, for $1 \leq i < j \leq 3$. For all i, j, u_{ij} is invariant, and so u_{ij}^q belongs to A. Since a_1^q, a_2^q, a_3^q forms an A-regular sequence [14, Corollary 17.8 (a)], and since

$$a_1^q u_{23}^q - a_2^q u_{13}^q + a_3^q u_{12}^q = \begin{vmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}^q = 0,$$

it follows that $u_{12}^q \in (a_1^q, a_2^q)A$. Thus, there exist $f_1, f_2 \in A$ such that

$$u_{12}^q = a_1^q b_2^q - a_2^q b_1^q = f_1 a_1^q + f_2 a_2^q.$$

As a_1, a_2 is a phsop in A, it is also a phsop in its integral extension $\Bbbk[V]$, and thus a_1, a_2 are coprime in $\Bbbk[V]$. From $a_1^q(b_2^q - f_1) = a_2^q(f_2 + b_1^q)$, it follows that a_1^q divides $f_2 + b_1^q$ in $\Bbbk[V]$. Therefore, there exists $h \in \Bbbk[V]$ such that $a_1^q h = f_2 + b_1^q$. Hence, for every $\sigma \in G$, we have

$$a_1^q(\sigma - 1)h = ((\sigma - 1)b_1)^q = (a_1 g_\sigma)^q = a_1^q g_\sigma^q,$$

that is, $g_\sigma^q = (\sigma - 1)h$, a contradiction since g^q is nonzero. Thus, $\mathrm{depth}_A(I) \leq 2$. $\square$

Proof of the general case. For some $m \geq 0$, we have $(\Bbbk[V]^G)^{p^m} \subseteq A$. For each i, $H^i(G, \Bbbk[V])$ is finitely generated as a $\Bbbk[V]^G$-module. Therefore, for each $0 < i < n$, there exists some $m(i)$ such that $\alpha^{p^{m(i)}} = 0$ for all $\alpha \in H^i(G, \Bbbk[V])$. Set $q := p^{m'}$, where m' is the maximum of $m, m(1), m(2), \ldots, m(n-1)$. Assume, for a contradiction, that $\mathrm{depth}_A(I) \geq n+2$, and let $a_1, a_2, \ldots, a_{n+2}$ be an A-regular sequence in I. Consider the bar resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module:

$$\ldots \xrightarrow{\partial_{n+1}} X_n \xrightarrow{\partial_n} X_{n-1} \xrightarrow{\partial_{n-1}} \ldots \xrightarrow{\partial_1} X_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0,$$

where $X_0 = \mathbb{Z}G$, and ∂_0 is the augmentation map. The cohomology class g is represented by a $u_{\{1\}} \in \mathrm{Hom}_{\mathbb{Z}G}(X_n, \Bbbk[V])$ such that $u_{\{1\}}\partial_{n+1} = 0$, that is, $u_{\{1\}} \in Z^n(G, \Bbbk[V])$ (the notation will become clear later). For each i, $a_i g = 0$, so there is $h_{\{i\}} \in \mathrm{Hom}_{\mathbb{Z}G}(X_{n-1}, \Bbbk[V])$ such that $a_i u_{\{1\}} = h_{\{i\}}\partial_n$. We next define, for each $2 \leq r \leq n+1$, and for each ordered r-subset $J := \{j(1), j(2), \ldots, j(r)\}$ of $\{1, \ldots, n+2\}$, a homomorphism $u_J \in \mathrm{Hom}_{\mathbb{Z}G}(X_{n-r+1}, \Bbbk[V])$ such that $u_J\partial_{n-r+2} = 0$, that is, $u_J \in Z^{n-r+1}(G, \Bbbk[V])$. For $2 \leq r \leq n$, the definition of q implies $u_J^q \in B^{n-r+1}(G, \Bbbk[V])$, so there is a map $h_J \in \mathrm{Hom}_{\mathbb{Z}G}(X_{n-r}, \Bbbk[V])$ satisfying $u_J^q = h_J\partial_{n-r+1}$. We now define u_J, and thus h_J, by induction on r:

$$u_J := \sum_{i=1}^{r} (-1)^{i+1} a_{j(i)}^{q^{r-2}} h_{J\setminus\{j(i)\}}. \tag{1}$$

Next, we show that $u_J\partial_{n-r+2} = 0$ for $2 \leq r \leq n+1$. For $r = 2$, we get

$$\begin{aligned} u_{\{j(1),j(2)\}}\partial_n &= a_{j(1)}h_{\{j(2)\}}\partial_n - a_{j(2)}h_{\{j(1)\}}\partial_n \\ &= a_{j(1)}a_{j(2)}u_{\{1\}} - a_{j(2)}a_{j(1)}u_{\{1\}} = 0. \end{aligned}$$

For $2 < r \leq n+1$, we obtain similarly:

$$u_J\partial_{n-r+2} = \sum_{i=1}^{r} (-1)^{i+1} a_{j(i)}^{q^{r-2}} u_{J\setminus\{j(i)\}}^q = 0, \tag{2}$$

since the middle term is

$$\sum_{i=1}^{r} (-1)^{i+1} a_{j(i)}^{q^{r-2}} \left(\sum_{k=1}^{i-1} (-1)^{k+1} a_{j(k)}^{q^{r-2}} h_{J\setminus\{j(i),j(k)\}}^q + \sum_{k=i+1}^{r} (-1)^{k} a_{j(k)}^{q^{r-2}} h_{J\setminus\{j(i),j(k)\}}^q \right) =$$

$$\sum_{1\leq k<i\leq r} (-1)^{i+k} a_{j(i)}^{q^{r-2}} a_{j(k)}^{q^{r-2}} h_{J\setminus\{j(i),j(k)\}}^q + \sum_{1\leq i<k\leq r} (-1)^{i+k+1} a_{j(i)}^{q^{r-2}} a_{j(k)}^{q^{r-2}} h_{J\setminus\{j(i),j(k)\}}^q,$$

which equals zero. When $r = n+1$, $u_J \in Z^0(G, \Bbbk[V])$. It follows that $u_J(\iota) \in \Bbbk[V]^G$, which implies $u_J(\iota)^q \in A$ ($\iota \in G$ is the neutral element). Therefore, for each $1 \leq i \leq n+2$, we have $u_{\{1,2,\ldots n+2\}\setminus\{i\}}^q(\iota) \in A$. The second equality in (2) is also valid for $J = \{1, 2, \ldots, n+2\}$ ($r = n+2$), that is,

$$\sum_{i=1}^{n+2} (-1)^{i+1} a_i^{q^n} u_{\{1,2,\ldots,n+2\}\setminus\{i\}}^q(\iota) = 0.$$

As $a_1^{q^n}, \dots, a_{n+2}^{q^n}$ is A-regular, $u^q_{\{1,\dots,n+1\}}(\iota) \in (a_1^{q^n}, \dots, a_{n+1}^{q^n})A$. Thus there exist $f_1, f_2, \dots, f_{n+1} \in \mathrm{Hom}_{\mathbb{Z}G}(X_0, A)$ (in particular, $f_i\partial_1 = 0$) such that $u^q_{\{1,\dots,n+1\}} = \sum_{i=1}^{n+1} a_i^{q^n} f_i$. Substituting (1) for $u_{\{1,\dots,n+1\}}$ yields

$$\sum_{i=1}^{n+1} (a_i^{q^n})((-1)^{i+1} h^q_{\{1,\dots,n+1\}\setminus\{i\}} - f_i) = 0.$$

Since $a_1^{q^n}, \dots, a_{n+1}^{q^n}$ is a phsop in A, it is also a phsop in $\Bbbk[V]$, and so $((-1)^n h^q_{\{1,\dots,n\}} - f_{n+1})(\iota) \in (a_1^{q^n}, a_2^{q^n}, \dots, a_n^{q^n})\Bbbk[V]$. It follows that

$$h^q_{\{1,\dots,n\}} - (-1)^n f_{n+1} = \sum_{i=1}^{n} a_i^{q^n} l_i$$

for some $l_1, l_2, \dots, l_n \in \mathrm{Hom}_{\mathbb{Z}G}(X_0, \Bbbk[V]) \cong \Bbbk[V]$. We next apply ∂_1 to this expression. For $n = 1$, we have $a_1^q u^q_{\{1\}} = a_1^q l_1 \partial_1$, or alternatively $u^q_{\{1\}} = l_1\partial_1 \in B^1(G, \Bbbk[V])$, a contradiction to $g^q \neq 0$. Now assume that $n \geq 2$. Applying ∂_1 leads to

$$u^{q^2}_{\{1,\dots,n\}} = \sum_{i=1}^{n} a_i^{q^n} l_i \partial_1. \tag{3}$$

For $2 \leq r \leq n$, we prove by reverse induction that there exist elements $l_1, l_2, \dots, l_r \in \mathrm{Hom}_{\mathbb{Z}G}(X_{n-r}, \Bbbk[V])$ such that

$$u^{q^{n+2-r}}_{\{1,\dots,r\}} = \sum_{i=1}^{r} a_i^{q^n} l_i \partial_{n-r+1}. \tag{4}$$

The case $r = n$ is covered by (3). Suppose $u^{q^{n+1-r}}_{\{1,\dots,r+1\}} = \sum_{i=1}^{r+1} a_i^{q^n} l'_i \partial_{n-r}$ for some $l'_1, l'_2, \dots l'_{r+1} \in \mathrm{Hom}_{\mathbb{Z}G}(X_{n-r-1}, \Bbbk[V])$. Using (1), we obtain

$$\sum_{i=1}^{r+1} (-1)^{i+1} a_i^{q^n} h^{q^{n+1-r}}_{\{1,\dots,r+1\}\setminus\{i\}} = \sum_{i=1}^{r+1} a_i^{q^n} l'_i \partial_{n-r},$$

and rearranging yields

$$\sum_{i=1}^{r+1} a_i^{q^n} ((-1)^{i+1} h^{q^{n+1-r}}_{\{1,\dots,r+1\}\setminus\{i\}} - l'_i \partial_{n-r}) = 0.$$

Since $a_1^{q^n}, \dots, a_{r+1}^{q^n}$ is a phsop for $\Bbbk[V]$, we have

$$h^{q^{n+1-r}}_{\{1,\dots,r\}} - (-1)^r l'_{r+1} \partial_{n-r} = \sum_{i=1}^{r} a_i^{q^n} l_i$$

for some $l_1, l_2, \dots, l_r \in \mathrm{Hom}_{\mathbb{Z}G}(X_{n-r}, \Bbbk[V])$. Here we have used that X_{n-r} is a free $\mathbb{Z}G$-module. Applying ∂_{n-r+1} to this expression gives us

$$h^{q^{n+1-r}}_{\{1,\dots,r\}} \partial_{n-r+1} = \sum_{i=1}^{r} a_i^{q^n} l_i \partial_{n-r+1},$$

which implies (4), as required.

When $r=2$, Equation (4) reads $u_{\{1,2\}}^{q^n} = a_1^{q^n} l_1 \partial_{n-1} + a_2^{q^n} l_2 \partial_{n-1}$, where $l_1, l_2 \in \mathrm{Hom}_{\mathbb{Z}G}(X_{n-2}, \Bbbk[V])$. Substituting (1) for $u_{\{1,2\}}$, we obtain $a_1^{q^n}(h_{\{2\}}^{q^n} - l_1\partial_{n-1}) = a_2^{q^n}(h_{\{1\}}^{q^n} + l_2\partial_{n-1})$. For the same reasons as before, we have $h_{\{1\}}^{q^n} + l_2\partial_{n-1} = a_1^{q^n} l$ for some $l \in \mathrm{Hom}_{\mathbb{Z}G}(X_{n-1}, \Bbbk[V])$. Applying ∂_n gives us $a_1^{q^n} u_{\{1\}}^{q^n} = a_1^{q^n} l\partial_n$. Hence, $u_{\{1\}}^{q^n} = l\partial_n \in B^n(G, \Bbbk[V])$, a contradiction to $g^{q^n} \neq 0$. Therefore, $\mathrm{depth}_A(I) \leq n+1$.

Finally, if $c_1, \ldots, c_k \in \mathrm{Ann}_{\Bbbk[V]^G}(g)$ forms a phsop in $\Bbbk[V]^G$, then $c_1^q, \ldots, c_k^q \in I$ forms a phsop in A, and so I has height at least k. The graded analogue of [5, Exercise 1.2.23] implies the Cohen-Macaulay defect of A is at least $\mathrm{ht}_A(I) - \mathrm{depth}_A(I) \geq k-n-1$. □

Lemma 2.2. *If $g \in H^n(G, \Bbbk)$ is nonzero, then g^{p^m} is nonzero for all $m \geq 0$.*

Proof. For $n=1$, this is clear since elements of $H^1(G,\Bbbk)$ are group homomorphisms $G \to (\Bbbk, +)$. For arbitrary n, by the Universal Coefficient Theorem [18, page 30], $H^n(G,\Bbbk) \cong H^n(G, \mathbb{F}_p) \otimes_{\mathbb{F}_p} \Bbbk$. We have $g = \sum_{i \in I} g_i \otimes \lambda_i$ for some $g_i \in H^n(G, \mathbb{F}_p)$ and $\lambda_i \in \Bbbk$. Without loss of generality, we can assume that the set $\{\lambda_i : i \in I\}$ is $\mathbb{F}_p$-linearly independent and g_i is nonzero for all i. Then $g^{p^m} = \sum_{i\in I} g_i^{p^m} \otimes \lambda_i^{p^m} = \sum_{i \in I} g_i \otimes \lambda_i^{p^m}$, since the m-fold Frobenius homomorphism induces the identity map on $\mathbb{F}_p$, and thus also on $H^n(G, \mathbb{F}_p)$. Therefore, as $\{\lambda_i^{p^m} : i \in I\}$ is still $\mathbb{F}_p$-linearly independent, g^{p^m} is still nonzero. □

Remark 2.3. For $n>1$, Theorem 2.1 is new even in the case $A = \Bbbk[V]^G$.

Example 2.4. Let $G \subseteq (\Bbbk, +)$ be a finite nontrivial subgroup. Consider the threefold sum of the 2-dimensional representation V of G over $\Bbbk$ given by $\sigma \mapsto \left(\begin{smallmatrix} 1 & 0 \\ -\sigma & 1 \end{smallmatrix}\right)$. Write $\Bbbk[V^{\oplus 3}] = \Bbbk[x_1, y_1, x_2, y_2, x_3, y_3]$ and ρ for the induced G-action. The map $g : G \to \Bbbk$, $\sigma \mapsto \sigma$ yields a nonzero element in $H^1(G, \Bbbk)$. For all $\sigma \in G$, we have $x_i g_\sigma = (\rho(\sigma) - 1)y_i$, that is, $x_i g$ is trivial. Since x_1, x_2, x_3 form a phsop in $\Bbbk[V^{\oplus 3}]$, Theorem 2.1 implies that no graded geometric separating algebra in $\Bbbk[V^{\oplus 3}]^G$ is Cohen-Macaulay. ◁

The following example shows that Theorem 2.1 applies only to graded *geometric* separating algebras:

Example 2.5. Let V be the permutation representation of the cyclic group $C_4 = \langle \sigma \rangle$ of order 4 over the field $\mathbb{F}_2$. Consider the C_4-invariants $c_1 := x_1+x_2+x_3+x_4$, $c_2 := x_1x_3+x_2x_4$, $c_3 := x_1x_2+x_2x_3+x_3x_4+x_1x_4$, and $c_4 := x_1x_2x_3x_4$. The action of C_4 on V partitions its 16 elements into 6 orbits, which one can check are separated by c_1, c_2, c_3, and c_4. As c_1, c_2, c_3, c_4 form a hsop in $\mathbb{F}_2[V]$, the subalgebra $\mathbb{F}_2[c_1, c_2, c_3, c_4]$ is a polynomial graded (non geometric) separating algebra. In particular, it is Cohen-Macaulay.

On the other hand, if $g : C_4 \to \mathbb{F}_2$ is the nontrivial cocycle given by $\sigma^i \mapsto i \mod 2$, then $c_1 g_{\sigma^i} = (\sigma^i - 1)(x_1 + x_3)$, $c_2 g_{\sigma^i} = (\sigma^i - 1)(x_1 x_3)$, and $c_3 g_{\sigma^i} = (\sigma^i - 1)(x_1 x_4 + x_2 x_3)$, that is, $c_1, c_2, c_3 \in \mathrm{Ann}_{\mathbb{F}_2[\overline{V}]^{C_4}}(g)$. Since c_1, c_2, c_3, c_4 form a hsop in $\mathbb{F}_2[V]$, by Theorem 2.1, no graded geometric separating algebra in $\mathbb{F}_2[V]^{C_4}$ is Cohen-Macaulay. $\triangleleft$

Using Theorem 2.1, we can quickly generalize several results which were consequences of its analogue [22, Corollary 1.6]. A first consequence is the following generalization of [6, Corollary 21]:

Corollary 2.6. *Assume G contains a normal subgroup N of index p (for example, G is a p-group). Then for any faithful representation V, every graded geometric separating algebra in $\Bbbk[V^{\oplus k}]^G$ has Cohen-Macaulay defect at least $k - 2$.*

Proof. Since $G/N \cong (\mathbb{F}_p, +)$, there is a nonzero element in $H^1(G, \Bbbk)$. As V is faithful, the fixed subspaces of nonidentity elements in G have codimension at least k in $V^{\oplus k}$. The result follows from Lemma 2.7. □

Lemma 2.7. *Suppose V is faithful. If the fixed subspace of every element of order p in G has codimension at least k in V, then for any homogeneous $g \in H^n(G, \overline{\Bbbk}[\overline{V}])$, the ideal $\mathrm{Ann}_{\overline{\Bbbk}[\overline{V}]^G}(g)$ has height at least k.*

Therefore, if there exists a homogeneous $g \in H^n(G, \overline{\Bbbk}[\overline{V}])$ satisfying the hypotheses of Theorem 2.1, then every graded geometric separating algebra in $\Bbbk[V]^G$ has Cohen-Macaulay defect at least $k - n - 1$.

Proof. We may assume $\Bbbk = \overline{\Bbbk}$. By Kemper [22, Lemma 2.1] there exist (in general, non-homogeneous) elements $a_1, \ldots, a_k \in \Bbbk[V]^G_+$ such that $a_i H^n(G, \Bbbk[V]) = 0$, for all i, and $\mathrm{ht}(a_1, \ldots, a_k) = k$. It follows that $\mathrm{Ann}_{\Bbbk[V]^G}(g)$ has height at least k. □

Proof of Theorem 1.4. By [3, Theorem 4.1.3], there is a number r such that $H^r(G, \Bbbk) \neq 0$. Thus by Lemma 2.2, for any k, there is a minimal number $n \leq r$ such that the hypotheses of Theorem 2.1 are satisfied for $V^{\oplus k}$. The same argument as in Corollary 2.6 shows that A has Cohen-Macaulay defect at least $k - n - 1 \geq k - r - 1$. □

Next, we generalize three results of [22]. Note that since, for us, elements acting trivially are bireflections, we do not need to assume that V is faithful.

Corollary 2.8. *If G has a normal subgroup N of index p which contains all elements acting as bireflections on V, then no graded geometric separating algebra in $\Bbbk[V]^G$ is Cohen-Macaulay.*

Proof. The proof of [22, Theorem 3.6] shows that the hypotheses of Theorem 2.1 are fulfilled with $n = 1$ and $k = 3$. □

Proof of Theorem 1.5. For p-groups, if the elements acting as bireflections generate a proper subgroup, then this subgroup lies in a normal subgroup of index p. □

Proposition 2.9. *Suppose G has a normal subgroup N with factor group an elementary abelian p-group. If there exists $\sigma \in G \setminus N$ whose fixed space in V is not contained in the fixed space of any bireflection in $G \setminus N$, then no graded geometric separating algebra in $\mathbb{k}[V]^G$ is Cohen-Macaulay.*

Proof. Without loss of generality, assume $\mathbb{k} = \overline{\mathbb{k}}$. As G/N is an elementary abelian p-group, there is a $g \in H^1(G, \mathbb{k})$ with kernel N. The proof of [22, Theorem 3.9] provides a phsop a_1, a_2, a_3 in $\mathbb{k}[V]^G$, and a homogeneous invariant $h \notin \sqrt{\mathrm{Ann}_{\mathbb{k}[V]^G}(g)}$ such that $ha_i \in \sqrt{\mathrm{Ann}_{\mathbb{k}[V]^G}(g)}$, for $i = 1, 2, 3$. Hence, for some $k \geq 0$, the invariants a_i^k annihilate $g' := h^k g \in H^1(G, \mathbb{k}[V])$. Thus, the annihilator ideal $\mathrm{Ann}_{\mathbb{k}[V]^G}(g')$ has height at least 3. By Theorem 2.1, it now suffices to show that g'^{p^m} is nonzero for all $m \geq 0$. By [22, Proposition 3.5], we have $\sqrt{\mathrm{Ann}_{\mathbb{k}[V]^G}(g^{p^m})} = \sqrt{\mathrm{Ann}_{\mathbb{k}[V]^G}(g)}$. Therefore, if g'^{p^m} is zero, then h^{kp^m} annihilates g^{p^m}, and so $h \in \sqrt{\mathrm{Ann}_{\mathbb{k}[V]^G}(g)}$, a contradiction. □

Example 2.10. Let $\mathbb{k}$ be a finite field. For $m \geq 3$, set $V = \mathbb{k}^{2m+1}$, and consider the group $G \leq \mathrm{GL}(V)$ formed by the $(2m+1) \times (2m+1)$ matrices of the form

$$\left(\begin{array}{ccc|c} & I_{m+1} & & \mathbf{0} \\ \hline \alpha_0 & & \alpha_m & \\ & \ddots & \vdots & I_m \\ & \alpha_{m-1} & \alpha_m & \end{array}\right),$$

where $\alpha_0, \ldots, \alpha_m \in \mathbb{k}$, and I_m denotes the $m \times m$ identity matrix. The group G is a p-group, and is generated by reflections, that is, by elements whose fixed space has codimension at most 1 in V. Example 3.10 in [22] shows that the hypotheses of Proposition 2.9 are satisfied, with N the subgroup formed by the elements such that $\alpha_m = 0$, and σ the element such that $\alpha_i = 1$ for all i. Hence, no graded geometric separating algebra in $\mathbb{k}[V]^G$ is Cohen-Macaulay. ◁

We end this section with a generalization of [22, Theorem 2.7].

Theorem 2.11. *Let V_{reg} be the regular representation of G over $\mathbb{k}$. If p divides $|G|$, then every graded geometric separating algebra in $\mathbb{k}[V_{reg}]^G$ has Cohen-Macaulay defect at least $|G|\frac{p-1}{p} - 2$. For $|G| \geq 5$, this number is at least one.*

Proof. By [22, Lemma 2.6], there is a nonzero $g \in H^1(G, \mathbb{k}[V_{reg}])$. Lemma 2.12 implies all powers g^{p^m} are also nonzero. Since the fixed subspaces of elements of G of order p have codimension $|G|(p-1)/p$, the hypotheses of Lemma 2.7 are satisfied with $k = |G|(p-1)/p$. □

The regular representation of C_4 was studied in Example 2.5. For $G = C_2, C_3$, and $C_2 \times C_2$, the invariant ring $\mathbb{k}[V_{reg}]^G$ is Cohen-Macaulay [22, Theorem 2.7]. Thus, these are the only groups such that there exists a Cohen-Macaulay graded geometric separating algebra in $\mathbb{k}[V_{reg}]^G$.

Lemma 2.12. *Let V be a permutation representation of G. If g in $H^1(G, \Bbbk[V])$ is nonzero, then g^{p^m} is nonzero for all $m \geq 0$. If, in addition, V is faithful, then every graded geometric separating algebra in $\Bbbk[V^{\oplus k}]^G$ has Cohen-Macaulay defect at least $k-2$.*

Proof. As V is a permutation representation, there is a set of monomials $M \subseteq \Bbbk[V]$ such that $\Bbbk[V] = \bigoplus_{h \in M} \langle Gh \rangle$. Thus, if $g \in H^1(G, \Bbbk[V])$, there is a (finite) decomposition $g = \sum_{h \in M} g_h$, where each g_h is in $H^1(G, \langle Gh \rangle)$. For $m \geq 0$, we have the decomposition $g^{p^m} = \sum_{h \in M} g_h^{p^m}$, where $g_h^{p^m}$ is in $H^1(G, \langle Gh' \rangle)$, and h' is the unique element of $Gh^{p^m} \cap M$. If g is nonzero, then g_h is nonzero for some h. As $\langle Gh \rangle$ and $\langle Gh^{p^m} \rangle$ are isomorphic permutation representations of G, the element $g_h^{p^m}$ is also nonzero. The additional statement follows by Lemma 2.7. □

3. The Alternating Group A_4

In this section we concentrate on representations of the alternating group A_4 over an algebraically closed field $\Bbbk$ of characteristic 2. The group A_4 is the smallest modular group G for which the cohomology $H^1(G, \Bbbk)$ is trivial. In order to apply Theorem 2.1, we must look outside the direct summand $H^1(G, \Bbbk)$ of $H^1(G, \Bbbk[V])$.

Pick $\chi \in A_4$, an element of order 2, and τ, a 3-cycle, so that A_4 is generated by χ and τ. The unique Sylow 2-subgroup P in A_4 is generated by χ and $\tau^{-1}\chi\tau$. Let ω be a fixed primitive third root of unity in $\Bbbk$. Define ${}^{\omega}\Bbbk$ and ${}^{\omega^2}\Bbbk$ to be the one-dimensional representations on which P acts trivially, and τ acts via multiplication by ω and ω^2, respectively. Formally, ${}^{1}\Bbbk$ denotes the trivial representation.

Lemma 3.1. *For $i = 1, 2$, the element of $H^1(A_4, {}^{\omega^i}\Bbbk)$ given by the cocycle $\chi \mapsto \omega^{2i}$, $\tau \mapsto 0$ is nonzero.*

Proof. Assume $i = 1$. Let $V := \langle v_1, v_2 \rangle$ be the representation given by

$$\chi \mapsto \begin{pmatrix} 1 & \omega^2 \\ 0 & 1 \end{pmatrix}, \text{ and } \tau \mapsto \begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix}.$$

This is an indecomposable representation [15, Theorem 7.0.3], with a submodule $W := \langle v_1 \rangle$ isomorphic to ${}^{\omega}\Bbbk$. Furthermore, A_4 acts trivially on the quotient V/W, and so we have a nonsplit exact sequence

$$0 \to {}^{\omega}\Bbbk \to V \to \Bbbk \to 0.$$

By [23, section 2], it follows that $H^1(A_4, {}^{\omega}\Bbbk) \neq 0$. In particular, the cocycle given by $\chi \mapsto \omega^2$, $\tau \mapsto 0$ is nontrivial. Similarly, for $i = 2$, the cocycle in $Z^1(A_4, {}^{\omega^2}\Bbbk)$ given by $\chi \mapsto \omega$, $\tau \mapsto 0$ is nontrivial. □

Corollary 3.2. *If $V := {}^{\omega^i}\Bbbk \oplus W^{\oplus k}$, where W is a faithful representation and $i = 1, 2$, then every graded geometric separating algebra in $\Bbbk[V]^{A_4}$ has Cohen-Macaulay defect at least $k-2$.*

Proof. Without loss of generality, $i = 1$. Since $V^* \cong {}^{\omega^2}\Bbbk \oplus (W^*)^{\oplus k}$, there is a direct summand of $\Bbbk[V]$ isomorphic to $S({}^{\omega^2}\Bbbk)$. Since $S^{2^m}({}^{\omega^2}\Bbbk)$ is isomorphic to ${}^{\omega^2}\Bbbk$ or ${}^{\omega}\Bbbk$, Lemma 3.1 implies that the cohomology class $g_m \in H^1(A_4, S^{2^m}({}^{\omega^2}\Bbbk))$, given by the cocycle $\chi \mapsto \omega^{2^m}$, $\tau \mapsto 0$, is nonzero for all m. As $g_m = g_0^{2^m}$, the result follows by Lemma 2.7. □

Exploiting the classification of the finite dimensional representations of A_4 [7] (with the notation of [15, Chapter 7]), we obtain a much stronger result:

Theorem 3.3. *Suppose V is a faithful, indecomposable finite dimensional representation of A_4. If $\Bbbk[V]^{A_4}$ is non Cohen-Macaulay, then no graded geometric separating algebra in $\Bbbk[V]^{A_4}$ is Cohen-Macaulay.*

Remark 3.4. The indecomposable representations V of A_4 such that $\Bbbk[V]^{A_4}$ is Cohen-Macaulay are listed in [15, Corollary 5.2.16]. In particular, when $\dim_{\Bbbk}(V) \geq 7$, $\Bbbk[V]^{A_4}$ is non Cohen-Macaulay.

Proof. Whenever $\Bbbk[V]^{A_4}$ is non Cohen-Macaulay, the fixed space of any nonidentity element in P has codimension at least 3 in V (see the classification). Thus, by Lemma 2.7, it suffices to find $g \in H^1(A_4, \Bbbk[V])$ such that g^{2^m} is nonzero for all $m \geq 0$. We use the classification to separate our argument into two cases.

First, we suppose V is of the form $W_s(\omega^e)$, where $s \in \mathbb{Z}$ (s may be negative only if it is odd), and $0 \leq e \leq 2$. The dimension of V is $n := |s|$. Let $\{v_1, v_2, \ldots, v_n\}$ be a basis of V such that A_4 acts via the matrices given in [15, Theorem 7.0.3]. In particular, the action of A_4 is upper triangular, and τ acts diagonally via multiplication by third roots of unity. If $\Bbbk[V]^{A_4}$ is non Cohen-Macaulay, the subset $\{v_1, v_2, \ldots, v_l\}$ is contained in V^P, for some $l \geq 2$. Moreover for some $r \leq l$, we have $\tau v_r = \omega^{-j} v_r$, where $j = 1$ or 2. Let $\{x_1, x_2, \ldots, x_n\}$ be the dual basis, so that $\Bbbk[V] = \Bbbk[x_1, x_2, \ldots x_n]$. Define $u := \prod_{\sigma \in P}(\sigma x_r)$. Then

$$\tau u = \prod_{\sigma \in P}(\tau\sigma\tau^{-1}(\tau x_r)) = \prod_{\sigma \in P}\omega^j(\sigma x_r) = \omega^j u.$$

Since $v_r \in V^P$, the set $\{x_1, x_2, \ldots, x_{r-1}, x_{r+1}, \ldots, x_n\}$ spans a $\Bbbk P$-submodule of V^*, thus $\Bbbk[V] = \Bbbk[x_1, x_2, \ldots, x_{r-1}, x_{r+1}, \ldots, x_n][x_r]$ as $\Bbbk P$-modules. Therefore, by [15, Proof of Lemma 1.3.2], if M is a $\Bbbk P$-module direct summand of $S(V^*)$, so is $u \cdot M$, and by induction so is $u^i \cdot M$ for any integer i. In particular, as $1 \in S^0(V^*)$, we have a sequence $\langle 1\rangle, \langle u\rangle, \langle u^2\rangle, \ldots$ of $\Bbbk P$-direct summands. Each $\langle u^i\rangle$ is a $\Bbbk A_4$-direct summand, and $\langle u^i\rangle \cong^{\omega^{ij}} \Bbbk$. The element $g_m \in H^1(A_4, \langle u^{2^m}\rangle)$ given by the cocycle $\chi \mapsto \omega^{-2^m j} u^{2^m}$, $\tau \mapsto 0$, is nonzero by Lemma 3.1. As $g_m = g_0^{2^m}$, we are done.

Second, suppose V takes the form $\overline{W}_{6d,\lambda}$, where $\lambda \in \Bbbk \cup \{\infty\}$, not a third root of unity, and $d \geq 1$, an integer, are such that if $d = 1$, then λ is not 0, 1, or ∞ (see [15, Theorem 7.0.3] for notation). As a $\Bbbk P$-module, $V^* \cong V_{2d,\alpha} \oplus V_{2d,\beta} \oplus V_{2d,\gamma}$ [2, Section 4.3], where α, β, and γ are elements of $\Bbbk \cup \{\infty\}$ depending on λ. The element τ acts on V by permuting the three $\Bbbk P$-module summands. As a $\Bbbk P$-module, $S(V^*) \cong S(V_{2d,\alpha}) \otimes S(V_{2d,\beta}) \otimes S(V_{2d,\gamma})$, and therefore, $S(V^*)$ has direct summands isomorphic to $S(V_{2d,\alpha})$, $S(V_{2d,\beta})$, and $S(V_{2d,\gamma})$. These summands are permuted by the action of τ. Let $\{x_1, \ldots, x_{6d}\}$ be a basis of V^* such that the action of P is given in block form; that is, $x_1, \ldots, x_{2d}$ is a basis for the summand isomorphic to $V_{2d,\alpha}$, and so on. Define $u_\alpha := \prod_{\sigma\in P} \sigma x_1$, and $u_\beta := \prod_{\sigma\in P} \sigma x_{2d+1}$, and $u_\gamma := \prod_{\sigma\in P} \sigma x_{4d+1}$. By the same argument as before, for each integer i, $\langle u_\alpha^i\rangle$ is a direct summand (with trivial P-action) of the $\Bbbk P$-module $S(V_{2d,\alpha})$, and hence of the $\Bbbk P$-module $S(V^*)$. The analogue holds for u_β and u_γ. Furthermore, we have

$$\tau u_\alpha^i = \tau(\prod_{\sigma\in P} \sigma x_1)^i = (\prod_{\sigma\in P} (\tau\sigma\tau^{-1}) x_{2d+1})^i = u_\beta^i.$$

Similarly, $\tau u_\beta^i = u_\gamma^i$ and $\tau u_\gamma^i = u_\alpha^i$. Thus, $U^i := \langle u_\alpha^i, u_\beta^i, u_\gamma^i\rangle$ is a $\Bbbk A_4$-direct summand of $S(V^*)$ on which P acts trivially. Since $[A_4 : P]$ is odd, τ acts diagonally with respect to some basis of U^i. A short calculation shows that $u := u_\gamma + \omega u_\beta + \omega^2 u_\alpha$ spans a direct summand of U^1 on which τ acts via multiplication by ω, in other words, $\langle u\rangle \cong {}^{\omega}\Bbbk$. For each m, we have that $u^{2^m} = u_\gamma^{2^m} + \omega^{2^m} u_\beta^{2^m} + \omega^{2^{m+1}} u_\alpha^{2^m}$ spans a direct summand of U^{2^m} isomorphic to ${}^{\omega^{2^m}}\Bbbk$.

The element $g_m \in H^1(A_4, \langle u^{2^m}\rangle)$ given by the cocyle $\chi \mapsto \omega^{2^{m+1}} u^{2^m}$, $\tau \mapsto 0$ is nonzero for each $m \geq 0$. As $g_m = g_0^{2^m}$, the result now follows by Lemma 2.7. □

4. Concluding Remarks

Our results have shown that in many of the situations in which the ring of invariants is non Cohen-Macaulay, the same holds for any graded geometric separating algebra. Hence, one might wonder if the existence of a Cohen-Macaulay graded geometric separating algebra implies that the ring of invariants itself is Cohen-Macaulay. The following example shows this is not true.

Example 4.1. Let $G = C_2 \times C_2 = \langle\sigma, \tau\rangle$ be the Klein four group, and let $\Bbbk$ be a field of characteristic two. Consider the 5-dimensional representation of G given by

$$\sigma \mapsto \begin{pmatrix} 1&0&1&0&0\\ 0&1&0&1&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 1&0&0&1&0\\ 0&1&0&0&1\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}.$$

By [17, Theorem 7], the ring of invariants is not Cohen-Macaulay. In fact, [17] shows that there exists a nonzero cohomology class $g \in H^1(G, \Bbbk[V])$ whose restriction to each proper subgroup of G is zero. By [16, Lemma 2.4, Proposition 2.5], $\sqrt{\mathrm{Ann}_{\Bbbk[V]^G}(g)} = \mathfrak{I}(V^G) \cap \Bbbk[V]^G$, where $\mathfrak{I}(V^G)$ denotes the ideal of polynomials $f \in \Bbbk[V]$ vanishing on V^G. Thus, the height of $\mathrm{Ann}_{\Bbbk[V]^G}(g)$ is $\operatorname{codim}(V^G) = 3$ while, by [22, Corollary 1.6], its depth is only two.

Using MAGMA [4] and the methods of [24, Section 2], one can verify that

$$\begin{aligned}
\{&a_1 := x_3, a_2 := x_4, a_3 := x_5,\\
&a_4 := x_1^4 + x_1^2x_3^2 + x_1^2x_3x_4 + x_1x_3^2x_4 + x_1x_3x_4^2 + x_1x_3x_4x_5 +\\
&\qquad x_1x_4^3 + x_2^2x_3^2 + x_2x_3^2x_5 + x_2x_3x_4^2,\\
&a_5 := x_2^4 + x_2^2x_4^2 + x_2^2x_4x_5 + x_2^2x_5^2 + x_2x_4^2x_5 + x_2x_4x_5^2,\\
&a_6 := x_1^2x_4^2 + x_1x_3x_4x_5 + x_1x_4^3 + x_2^2x_3^2 + x_2x_3^2x_5 + x_2x_3x_4^2,\\
&a_7 := x_1x_4^2x_5 + x_1x_4x_5^2 + x_2^2x_3x_5 + x_2^2x_4^2 + x_2x_3x_5^2 + x_2x_4^3\}
\end{aligned}$$

forms a geometric separating set. Furthermore, $\{a_1, a_2, a_3, a_4, a_5\}$ is a hsop for the geometric separating algebra $A := \Bbbk[a_1, a_2, \ldots, a_7]$. As a module over $\Bbbk[a_1, a_2, a_3, a_4, a_5]$, A is freely generated by $\{1, a_6, a_7, a_6a_7\}$. Therefore, A is Cohen-Macaulay. As G is a p-group, by Theorem 1.5, G must be a bireflection group, which is indeed the case. The Hilbert Series of A is $H(A,t) = \frac{1+2t^4+t^8}{(1-t)^3(1-t^4)^2}$. Since $H(A, 1/t) = (-1)^5t^3H(A,t)$, we even have that A is Gorenstein, but not strongly Gorenstein, as $3 \neq \dim V$.

Note that since $\Bbbk[V]^G$ is integral over A, the height of $\mathrm{Ann}_A(g)$ is also 3, and as A is Cohen-Macaualay, the depth of $\mathrm{Ann}_A(g)$ must be 3. Theorem 2.1 implies that there exists a p-power q such that $g^q = 0$. $\triangleleft$

We end with an example which shows that even in the non-modular case, the good behaviour of separating algebras is not guaranteed by that of the invariant ring.

Example 4.2. Let $G = C_4$ be the cyclic group of order 4, and let $\Bbbk$ be a field of odd characteristic containing a primitive fourth root of unity ζ. Consider the 2-dimensional representation V of $C_4 = \langle\sigma\rangle$ given by $\sigma \mapsto \left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta\end{smallmatrix}\right)$. If $\Bbbk[V] = \Bbbk[x,y]$, then $\Bbbk[V]^{C_4} = \Bbbk[x^4, x^3y, x^2y^2, xy^3, y^4]$. On points where x^4 is zero, the function x^2y^2 also takes the value zero; on any other point v, we have $x^2y^2(v) = \frac{(x^3y(v))^2}{x^4(v)}$. Thus, the value of x^2y^2 as a function is entirely determined by the value of x^4 and x^3y. Therefore x^4, x^3y, xy^3, y^4 form a geometric separating set and $A := \Bbbk[x^4, x^3y, xy^3, y^4]$ is a geometric separating algebra. Note that A is not Cohen-Macaulay, since the hsop x^4, y^4 does not form a regular sequence (despite being coprime) [5, Exercise 2.1.18].

On points where x^4 is zero, xy^3 is zero, and on any other point v, $xy^3(v) = \frac{(x^3y(v))^3}{(x^4(v))^2}$. Thus, the hypersurface $\Bbbk[x^4, x^3y, y^4]$ is also a graded geometric separating algebra. Therefore, we have a Cohen-Macaulay graded geometric separating algebra, inside a non Cohen-Macaulay graded geometric separating algebra, inside a Cohen-Macaulay invariant ring. $\triangleleft$

References

[1] D. J. Benson. *Polynomial invariants of finite groups*, volume 190 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

[2] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1998. Basic representation theory of finite groups and associative algebras.

[3] D. J. Benson. *Representations and cohomology. II*, volume 31 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1998. Cohomology of groups and modules.

[4] 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).

[5] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[6] H. E. A. Campbell, I. P. Hughes, G. Kemper, R. J. Shank, and D. L. Wehlau. Depth of modular invariant rings. *Transform. Groups*, 5(1):21–34, 2000.

[7] S. B. Conlon. Certain representation algebras. *J. Aust. Math. Soc*, 5:83–99, 1965.

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

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

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

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

[12] Emilie Dufresne. Separating invariants. *Ph. D. thesis, Kingston Ontario*, 2008. `http://hdl.handle.net/1974/1407`.

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

[14] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[15] Jonathan Elmer. Symmetric algebras and the depth of invariant rings. *Ph.D thesis, University of Kent*, 2007. `http://www.maths.abdn.ac.uk/~bensondj/papers/e/elmer/klein4new.dvi`.

[16] Jonathan Elmer. Associated primes for cohomology modules. *Arch. Math. (Basel)*, 91(6):481–485, 2008.

[17] Jonathan Elmer and Peter Fleischmann. On the depth of modular invariant rings for the groups $C_p \times C_p$. *Symmetry and Spaces: Festschrift in honour of Gerry Schwarz*, 2006.

[18] Leonard Evens. *The cohomology of groups.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[19] F. D. Grosshans. Vector invariants in arbitrary characteristic. *Transform. Groups*, 12(3):499–514, 2007.

[20] M. Hochster and John A. Eagon. Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. *Amer. J. Math.*, 93:1020–1058, 1971.

[21] 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).

[22] Gregor Kemper. On the Cohen-Macaulay property of modular invariant rings. *J. Algebra*, 215(1):330–351, 1999.

[23] Gregor Kemper. A characterization of linearly reductive groups by their invariants. *Transform. Groups*, 5(1):85–92, 2000.

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

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

[26] 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.

[27] Wilberd van der Kallen. `http://www.math.uu.nl/people/vdkallen/errbmod`.

[28] Wilberd van der Kallen. *Lectures on Frobenius splittings and B-modules*. Published for the Tata Institute of Fundamental Research, Bombay, 1993. Notes by S. P. Inamdar.

[29] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

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

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

Lehrstuhl A für Mathematik, RWTH Aachen, 52062 Aachen, Germany

E-mail address: `jonathan.elmer@mathA.rwth-aachen.de`

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

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