SEPARATING INVARIANTS AND LOCAL COHOMOLOGY

EMILIE DUFRESNE AND JACK JEFFRIES

Abstract. The study of separating invariants is a recent trend in invariant theory. For a finite group acting linearly on a vector space, a separating set is a set of invariants whose elements separate the orbits of G. In some ways, separating sets often exhibit better behavior than generating sets for the ring of invariants. We investigate the least possible cardinality of a separating set for a given G-action. Our main result is a lower bound that generalizes the classical result of Serre that if the ring of invariants is polynomial then the group action must be generated by pseudoreflections. We find these bounds to be sharp in a wide range of examples.

1. Introduction

For an action of an algebraic group on an affine variety, a *separating set* is a collection of invariants which, as functions on V, distinguish any two points that can be distinguished by some invariant. While using invariants as a tool to distinguish orbits of a group action on a variety is a classical endeavor, this approach to invariant theory has enjoyed a resurgence of interest in its modern form, initiated by work of Derksen and Kemper [**?**, **?**].

Throughout this paper, we focus on the case of a finite group G acting linearly on a d-dimensional vector space V over the field $\Bbbk$. This action induces a contragredient action of the group G on the polynomial ring $\Bbbk[V] := \operatorname{Sym}(V^*)$; if $\Bbbk$ is infinite, $\Bbbk[V]$ can be identified with the ring of regular functions on V. We consider the *ring of invariants* $\Bbbk[V]^G := \{f \in \Bbbk[V] \mid \forall g \in G,\ g \cdot f = f\}$. We will assume throughout that $\Bbbk$ is algebraically closed. While the results of our paper have analogous statements over general fields (see Remark **??**), the exposition is cleaner with the assumption that $\Bbbk$ is algebraically closed. In this setting, a separating set is a set $E \subset \Bbbk[V]^G$ such that if, for $v, w \in V$, the orbits $G \cdot v$ and $G \cdot w$ are distinct, then there is an $h \in E$ with $h(v) \neq h(w)$; that is, a separating set is a set of invariants which separates orbits.

While the ring of invariants (or a generating set) forms a separating set, there often exist smaller and/or otherwise better-behaved separating sets — especially in the *modular* case, where $|G|$ is not invertible in $\Bbbk$. For example, there always exist separating sets consisting of elements of degree at most $|G|$ ([**?**, Corollary 3.9.14]), and polarizations of separating sets yield separating sets for vector invariants ([**?**,

Date: 10^{th} Nov, 2014.

2010 *Mathematics Subject Classification.* 13A50, 13D45, 06A07, 52C35.

Key words and phrases. Invariant theory, separating invariants, local cohomology, arrangements of linear subspaces, simplicial homology, poset topology.

This material is based upon work supported by the National Science Foundation under Grant No 0932078 000, while the authors were in residence at the Mathematical Science Research Institute in Berkeley, California, during the Spring semester of 2013. The second author was also supported in part by NSF grants DMS 0758474 and DMS 1162585.

Theorem 1.4]). The main question we consider in this paper is: What is the least cardinality of a separating set?

Some general bounds are known. It follows from [**?**, Proposition 2.3.10] that the algebra generated by a separating set, i.e., a *separating algebra*, has dimension d, thus any separating set has at least d elements. On the other hand, a secant variety argument (see [**?**, Proposition 5.1.1]) shows that there always exists a separating set of size $2d + 1$.

Since any separating algebra has dimension d, the existence of a separating set of size d is equivalent to the existence of a polynomial separating algebra. The question of whether the ring of invariants is polynomial is very classical, and two of the cornerstone results of invariant theory largely answer this question: The Shephard-Todd Theorem (see [**?**, p. 104]) says that if $|G|$ is invertible in $\Bbbk$ (the *non-modular* case), then $\Bbbk[V]^G$ is a polynomial ring if and only if the action of G is generated by *pseudoreflections* — elements that fix a hyperplane in V. In this case, one calls G a *reflection group*. A theorem of Serre (see [**?**, Proposition 3.7.8]) states that, with no hypothesis on $|G|$, if $\Bbbk[V]^G$ is a polynomial ring, then G acts as a *rigid reflection group*: every isotropy subgroup is a reflection group. The problem of classifying which actions have polynomial invariant rings in the modular case remains an important open question.

In [**?**, Theorem 1.1], the first author extends Serre's result by showing that if there exists a polynomial separating algebra, then G is a reflection group. As a corollary, in the non-modular case, there exists a polynomial separating algebra if and only if G is a reflection group. The existence of a separating set of size d is thus related to whether G is a reflection group. Further, in [**?**, Theorem 1.3], the first author shows that if there is a graded separating algebra that is a complete intersection, then the action of G is generated by *bireflections* — elements that fix a codimension two subspace in V. Consequently, if there is a separating set consisting of $d + 1$ homogeneous invariants (whence the algebra it generates is a graded hypersurface and hence a complete intersection), then the action of G is generated by bireflections.

In the present paper, we apply techniques of local cohomology to strengthen and extend these bounds. After reviewing some preliminary notions in Section **??**, in Section **??**, we obtain our main result:

Theorem. *If there exists a separating set of size $d+r-1$, then every isotropy subgroup G_U is generated by r-reflections. In particular, G is generated by r-reflections.*

Setting $r = 1$, we obtain the following strengthening of [**?**, Theorem 1.1]: If there exists a separating set of size d, then G is a rigid reflection group. Our approach utilizes Àlvarez, García, and Zarzuela's computation of local cohomology with support in a subspace arrangement in [**?**]. Their formula is a local cohomology analogue of the celebrated Goresky-MacPherson Formula for the singular cohomology of the complement of a real subspace arrangement (see, e.g., [**?**, Theorem 1.3.8]); in this way, one can consider our results a link between the Goresky-MacPherson Formula and the Shephard-Todd Theorem.

In Section **??**, we focus on rigid reflection groups. Applying techniques from poset homology, we show that the cohomological obstructions to small separating sets utilized in Section **??** vanish for all integers greater than d. While there are rigid reflection groups for which the ring of invariants is not polynomial, some of the counterexamples have been proved to have a polynomial separating algebra, e.g. [**?**,

Example 3.1]. We pose the conjecture that there exists a polynomial separating algebra if and only if G is a rigid reflection group.

In Section **??**, we construct a variety of examples of separating sets for which the lower bound from the main theorem is realized: that is, we construct separating sets of the minimal possible cardinality. While we do not have a specific algorithm by which we create such sets, we are able to use an idea from the first author's thesis [**?**, Section 5.2] (the "triangle trick") effectively in a wide range of cases.

2. Preliminaries

2.1. **r-Reflections.** For any subset U of V, we define its *isotropy subgroup* G_U as follows:

$$G_U := \{\sigma \in G \mid \sigma \cdot u = u,\ \forall u \in U\}\,.$$

An element $\sigma \in G$ is called an *r-reflection* if its fixed subspace V^σ has codimension r. In particular, a 1-reflection is a pseudoreflection, and a 2-reflection is a bireflection. We say that G is an *r-reflection group* if it is generated by elements whose fixed space has codimension at most r.

A linear subspace $W \subset V$ is an *r-reflecting subspace* if and only if W has codimension r in V and its isotropy subgroup G_W is non-trivial. An r-reflecting subspace will be called *minimal* if it is not the intersection of r'-reflecting subspaces with $r' < r$. A group is called a *rigid r-reflection group* if every minimal reflecting subspace has codimension at most r. This is equivalent to requiring that every isotropy subgroup is an r-reflection group. We will say that G is a *(rigid) $(<r)$-reflection group* if there exists an $r' < r$ such that G is a (rigid) r'-reflection group. For $r = 1$ we will say *(rigid) reflection group* instead of (rigid) 1-reflection group.

In the non-modular case, it follows from the Shephard-Todd Theorem and Serre's Theorem that every reflection group is a rigid reflection group. For $r > 1$, the condition of being a rigid r-reflection group is stronger than that of being an r-reflection group. For a concrete example, let V be a $(2n+1)$-dimensional vector space over $\mathbb{C}$ with basis $u_1, \ldots, u_n, v_1, \ldots, v_n, w$ and let $G := C_2 \times C_2 = \langle \alpha, \beta \rangle$ act on V by

$$\begin{aligned}
&\alpha(u_i) = -u_i && \beta(u_i) = u_i && \text{for } i = 1, \ldots, n\,,\\
&\alpha(v_i) = v_i && \beta(v_i) = -v_i && \text{for } i = 1, \ldots, n\,,\\
&\alpha(w) = -w && \beta(w) = -w\,. &&
\end{aligned}$$

Here G is generated by $(n+1)$-reflections, but $\langle \alpha\beta \rangle$ is an isotropy subgroup generated by a $(2n)$-reflection, thus G is not a rigid $(<2n)$-reflection group.

2.2. **The Separating Variety.** The *separating variety* $\mathcal{S}_{V,G}$ is a closed subvariety of the product $V \times V$ that completely determines the equivalence relation induced by $\Bbbk[V]^G$ on V. More precisely, we have

$$\begin{aligned}
\mathcal{S}_V :&= \{(u, v) \in V \times V \mid f(u) = f(v),\ \text{for all } f \in \Bbbk[V]^G\}\\
&= \mathcal{V}_{V\times V}(f \otimes 1 - 1 \otimes f \mid f \in \Bbbk[V]^G)\,.
\end{aligned}$$

A separating set can then be characterized as a subset $E \subset \Bbbk[V]^G$ that cuts out the separating variety in $V \times V$, that is, such that $\mathcal{V}_{V\times V}(f \otimes 1 - 1 \otimes f \mid f \in E) = \mathcal{S}_{V,G}$. In ideal-theoretic terms,

Proposition 2.1. [?, Corollary 2.6] *A set of invariants $\{f_1, \dots, f_t\}$ is a separating set for G acting on V if and only if*

$$\sqrt{(f_1 \otimes 1 - 1 \otimes f_1, \dots, f_t \otimes 1 - 1 \otimes f_t)} = \sqrt{(h \otimes 1 - 1 \otimes h \mid h \in \Bbbk[V]^G)} =: \mathcal{I}(\mathcal{S}_{V,G}) .$$

For actions of finite groups, the invariants actually separate orbits (see, for example, [?, Lemma 2.1]) and so the separating variety coincides with the graph of the action

$$\Gamma_{V,G} := \{(v, \sigma \cdot v) \mid v \in V,\ \sigma \in G\} .$$

This provides significant geometric insight into $\mathcal{S}_{V,G}$:

Lemma 2.2 (c.f. [?, Proposition 3.1])**.** *Let G be a finite group acting linearly on V.*

(a) The separating variety has an irreducible decomposition of the form

$$\mathcal{S}_{V,G} = \bigcup_{\sigma \in G} (1 \otimes \sigma)(V)$$

with each $(1 \otimes \sigma)(V)$ a linear subspace isomorphic to V.

(b) If $\sigma, \tau \in G$, then $(1 \otimes \sigma)(V) \cap (1 \otimes \tau)(V) = (1 \otimes \tau)(V^{\tau^{-1}\sigma})$, which has dimension equal to that of the subspace fixed by $\tau^{-1}\sigma$ in V. Every non-empty intersection of components $(1 \otimes \sigma)(V)$ with $\sigma \in G$ is of the form $(1 \otimes \gamma)(V^H)$, where $H \leq G$ is an isotropy subgroup and $\gamma \in G/H$.

Remark 2.3. The assumption that $\Bbbk$ is algebraically closed is essential in Proposition **??**. However, one may obtain results in the non-algebraically closed case by considering a *geometric separating set*: for G finite, this is a subset of $\Bbbk[V]^G$ that separates orbits of G in $V \otimes_{\Bbbk} \overline{\Bbbk}$ (see [?, Section 2]). By [?, Theorem 2.1], a geometric separating set is characterized by the ideal-theoretic equality in Proposition **??**. Accordingly, the results of Section **??** hold for $\Bbbk \neq \overline{\Bbbk}$ if one replaces the phrase "separating set" with "geometric separating set." Further, since $\Bbbk[V]^G$ is a geometric separating set, Corollary **??** holds verbatim for all $\Bbbk$.

2.3. **Posets.** For an arrangement of linear subspaces $X \subset \mathbb{A}^m$, let $P(X)$ denote the *intersection poset* of X: the collection, ordered by inclusion, of linear subspaces that occur as intersections of components of X. For $p \in P(X)$, the *interval* $P(>p)$ is the subposet of $P(X)$ consisting of elements containing p. One defines $P(<p), P(\geqslant p)$, and $P(\leqslant p)$ analogously. The reduced homology of a poset P with coefficients in $\Bbbk$ will be denoted by $\widetilde{\mathrm{H}}_\bullet(P; \Bbbk)$: this is the reduced simplicial homology of the simplicial complex whose vertices are elements of the poset, and whose faces are the chains.

In our setting, for a linear action of a finite group, the separating variety $\mathcal{S}_{V,G}$ is a subspace arrangement. By abuse of notation, we will also denote its intersection poset by $\mathcal{S}_{V,G}$. Note that if $W \subseteq V$ is a subspace, then $\mathcal{S}_{V,G}(> (1 \otimes 1)(W)) \cong \mathcal{S}_{V,G_W}(>(1 \otimes 1)(W))$.

We will also consider the poset $\mathcal{R}_{V,G}$ of r-reflecting subspaces (all possible r's). The two posets $\mathcal{S}_{V,G}$ and $\mathcal{R}_{V,G}$ are related by the following lemma.

Lemma 2.4. *For any $\sigma \in G$, the interval $\mathcal{S}_{V,G}(< (1 \otimes \sigma)(V))$ is isomorphic to $\mathcal{R}_{V,G}$.*

Proof. The map on $\Gamma_{V,G}$ given by applying σ to the second coordinate is an isomorphism, thus $\mathcal{S}_{V,G}(\leqslant(1\otimes\sigma)(V)) \cong \mathcal{S}_{V,G}(\leqslant(1\otimes 1)(V))$. Now,

$$\begin{aligned}(1\otimes 1)(V)\cap(1\otimes\sigma_1)(V)\cap\cdots\cap(1\otimes\sigma_m)(V)&\\ &= \{(v,v)\,|\,v=\sigma_1(v)=\cdots=\sigma_m(v)\}\\ &= (1\otimes 1)(V^{\langle\sigma_1,\ldots,\sigma_m\rangle})\,,\end{aligned}$$

so that the intersections of components of $\mathcal{S}_{V,G}$ contained in $(1\otimes 1)(V)$ coincide with the diagonal embeddings of reflecting subspaces. □

It is worth noting that the order on $\mathcal{R}_{V,G}$ used here is dual to that most commonly used in the literature on subspace arrangements.

2.4. **Local Cohomology.** For the convenience of the reader unfamiliar with local cohomology, we give a quick review with an eye towards the main fact we will employ. A welcoming source on local cohomology which includes the material below is [**?**]. For an ideal I in a commutative noetherian ring R and an R-module M, the *I-torsion* part of M is

$$\Gamma_I(M) = \{m\in M \mid I^t m = 0 \text{ for some } t\in\mathbb{N}\}\,.$$

The assignment $\Gamma_I(-)$ is easily checked to form a left-exact functor (with maps given by restriction), and its right-derived functors are defined as the *local cohomology functors with support in I,* denoted $\mathrm{H}^i_I(-)$. Since $\Gamma_I(-)=\Gamma_J(-)$ if $\sqrt{I}=\sqrt{J}$, we also have $\mathrm{H}^i_I(-)=\mathrm{H}^i_J(-)$.

Given a generating set $I=(f_1,\ldots,f_t)$, the local cohomology of I can also be computed as the cohomology of the Čech complex:

$$\mathrm{H}^i_I(M) = \mathrm{H}^i\Big(\quad 0\to M\to\bigoplus_j M_{f_j}\to\bigoplus_{j<j'} M_{f_jf_{j'}}\to\cdots\to M_{f_1\cdots f_t}\to 0\quad\Big)\,,$$

where the maps on each component are ±1 times the natural maps, with the signs chosen so that the sequence above forms a complex. Consequently, if $\mathrm{H}^i_I(R)\neq 0$ and $f_1,\ldots,f_t$ generates I up to radical, we necessarily have $t\geqslant i$, since the Čech complex must have at least i terms if its i^{th} cohomology is non-zero.

3. Lower bounds on the size of separating sets

In this section, we give a lower bound on the size of a separating set for a ring of invariants of a finite group. We reiterate the assumption that $\Bbbk$ is algebraically closed; see Remark **??** for the non-algebraically closed case. The following lemma will be key to our applications.

Lemma 3.1. *The separating variety is connected in codimension $\leqslant r$ if and only if the action of G is generated by $(\leqslant r)$-reflections.*

Proof. By Lemma **??** (a), the separating variety $\mathcal{S}_{V,G}$ is connected in codimension $\leqslant r$ if and only if, for any $\sigma,\sigma'\in G$, there is a sequence of components

$$(1\otimes\sigma)(V) = (1\otimes\sigma_0)(V)\ ,\ (1\otimes\sigma_1)(V)\ ,\ \ldots\ ,\ (1\otimes\sigma_r)(V) = (1\otimes\sigma')(V)$$

such that $(1\otimes\sigma_i)(V)\cap(1\otimes\sigma_{i+1})(V)$ has codimension $\leqslant r$. By Lemma **??** (b), $\dim(1\otimes\sigma_i)(V)\cap(1\otimes\sigma_{i+1})(V) = \dim V^{\sigma_{i+1}^{-1}\sigma_i}$. Thus, $\mathcal{S}_{V,G}$ is connected in codimension $\leqslant r$ if and only if for any $\sigma,\sigma'\in G$ there exist $(\leqslant r)$-reflections

$$\tau_1=\sigma_0^{-1}\sigma_1\ ,\ \tau_2=\sigma_1^{-1}\sigma_2\ ,\ \ldots\ ,\ \tau_r=\sigma_{r-1}^{-1}\sigma_r$$

such that $\sigma = \tau_1 \cdots \tau_r \sigma'$. But this just means that G is generated by $(\leqslant r)$-reflections. □

We first note that a connectedness theorem of Grothendieck allows for the following generalization of [**?**, Theorem 1.1].

Proposition 3.2. *If there exists a separating set of size $d+r-1$, then the action of G is generated by $(\leqslant r)$-reflections.*

Proof. By Proposition **??**, if there is a separating set of size $d+r-1$, then $\mathcal{I}(\mathcal{S}_{V,G})$ is set-theoretically defined by $d+r-1$ equations. By [**?**, Exposé XIII, Théorème 2.1], if $\mathcal{I}(\mathcal{S}_{V,G})$ can be set-theoretically cut out by $d+r-1$ or fewer equations, then $\mathcal{S}_{V,G}$ is connected in codimension $\leqslant r$. Then, by Lemma **??**, G is generated by $(\leqslant r)$-reflections. □

A stronger result can be obtained by examining the local cohomology with support in $\mathcal{I}(\mathcal{S}_{V,G})$. Local cohomology with support in a subspace arrangement is studied by Àlvarez, García, and Zarzuela in [**?**]. Following along the lines of Björner and Ekedahl's computation of ℓ-adic cohomology of such spaces, they establish a Mayer-Vietoris spectral sequence for local cohomology and show that it degenerates for subspace arrangements, thus obtaining a Goresky-MacPherson analogue in local cohomology. In particular, their formula provides a combinatorial characterization of the vanishing and non-vanishing of the local cohomology modules.

Theorem 3.3. *(a)* [**?**, p. 39], [**?**, Theorem 2.1] *If $I_1, \dots, I_t \subset R$ are ideals, and M an R-module, then there is a Mayer-Vietoris spectral sequence*

$$E_1^{-p,q} = \bigoplus_{i_0<\cdots<i_p} \mathrm{H}^q_{I_{i_0}+\cdots+I_{i_p}}(M) \quad \Longrightarrow \quad \mathrm{H}^{q-p}_{I_1\cap\cdots\cap I_t}(M)\,.$$

(b) [**?**, Corollary 1.3] *If $I_1, \dots, I_t \subset R$ are ideals of linear subspaces in a polynomial ring, then the spectral sequence above degenerates at E_2, and for all $q \geqslant 0$ there is an associated graded module of the local cohomology module $\mathrm{H}^q_{I_1\cap\cdots\cap I_t}(R)$ with*

$$\operatorname{gr}\left(\mathrm{H}^q_{I_1\cap\cdots\cap I_t}(R)\right) \cong \bigoplus_{p\in P} \left[\mathrm{H}^{\operatorname{codim}(p)}_{I(p)}(R) \otimes_{\Bbbk} \widetilde{\mathrm{H}}_{\operatorname{codim}(p)-q-1}(P(>p);\Bbbk)\right],$$

where P is the intersection poset of $\mathcal{V}(I_1 \cap \cdots \cap I_t)$.

With this description of the local cohomology in hand, we obtain the following strengthening of Proposition **??**.

Theorem 3.4. *Let $r_1, \dots, r_s$ be the codimensions of minimal reflecting subspaces. Then $\mathrm{H}^{d+r_i-1}_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2]) \neq 0$. In particular, if r is the maximal codimension of a minimal reflecting subspace, then every separating set has size at least $d+r-1$.*

Proof. Let $W \subset V$ be a minimal r-reflecting subspace in the sense of Subsection **??**. Note that

$$\mathcal{S}_{V,G}(>(1\otimes 1)(W)) \cong \mathcal{S}_{V,G_W}(>(1\otimes 1)(V^{G_W}))\,.$$

The latter poset is connected if and only if $\mathcal{S}_{V,G_W}$ is connected in codimension $<r$. By Lemma **??**, this is the case if and only if G_W is generated by $(<r)$-reflections. Since W is minimal, G_W is not generated by $(<r)$-reflections: if $G_W = \langle g_1, \dots, g_s\rangle$

with each g_i an $(<r)$-reflection, one may write $W = \bigcap_{i=1}^{s} V^{\langle g_i \rangle}$, expressing W as the intersection of larger reflecting subspaces. Thus,

$$\widetilde{\mathrm{H}}_0\left(\mathcal{S}_{V,G}(>(1\otimes 1)(W)); \Bbbk\right) \neq 0\,.$$

Theorem **??** (b) applies to show that $\mathrm{H}^{d+r-1}_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2]) \neq 0$. Thus, $\mathcal{I}(\mathcal{S}_{V,G})$ cannot be set-theoretically defined by $d+r-1$ or fewer equations, and by Proposition **??**, any separating set has size at least $d+r-1$. □

Corollary 3.5. *If r is the maximal codimension of a minimal reflecting subspace, then the embedding dimension of $\Bbbk[V]^G$ is at least $d+r-1$.*

Proof. This follows immediately from Theorem **??** since a minimal generating set is a separating set. Alternatively, one may argue by using Proposition **??** to conclude that the embedding codimension is at least r if G is not a $(<r)$-reflection group, and applying [**?**, Theorem A], according to which the embedding codimension (referred to in *ibid.* as the polynomial defect) does not increase when passing to the invariants of an isotropy subgroup. □

Remark 3.6. In a recent work of Reimers [**?**, Theorem 2.4], the statement of Lemma **??** is established in the more general setting where G acts on a variety that is connected in codimension $\leqslant r$. This result is then applied to study the depth of schemes defining the separating variety of the action — particularly, in terms of local cohomology, the least i for which $\mathrm{H}^i_{\mathsf{m}}(R/J) \neq 0$ for some J with $\sqrt{J} = \mathcal{I}(\mathcal{S}_{V,G})$. In characteristic $p > 0$, the vanishing of these local cohomology modules is related to the vanishing of those considered above by Peskine and Szpiro's vanishing theorem [**?**, Remarque p. 110].

Remark 3.7. It follows from the Hartshorne-Lichtenbaum vanishing theorem [**?**, Theorem 3.1] that $\mathrm{H}^{2d}_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2]) = 0$. This can also be deduced from Theorem **??**. Indeed, the only potential element of the poset $\mathcal{S}_{V,G}$ of codimension $2d$ is $(1\otimes 1)(V^G)$, and this occurs only if V^G is the origin. As $\mathcal{S}_{V,G}(>(1\otimes 1)(V^G))$ is non-empty, $\widetilde{\mathrm{H}}_{-1}(\mathcal{S}_{V,G}(>(1\otimes 1)(V^G)); \Bbbk) = 0$, and we are done.

4. Rigid Reflection Groups

In this section, we focus on rigid reflection groups. In this situation, every minimal reflecting subspace is a hyperplane, and in particular, the arrangement of reflecting subspaces $\mathcal{R}_{V,G}$ is a hyperplane arrangement. Recall that a simplicial complex is *pure* if each of its maximal facets have the same dimension. A pure simplicial complex is *shellable* if there is a linear ordering of its maximal facets (a *shelling*) $F_1, F_2, \ldots, F_t$ such that $F_i \cap \bigcup_{j<i} F_j$ is pure of codimension 1; we call a poset *shellable* if its order complex is pure and shellable. The salient fact we use is the following well-known tool in combinatorial topology; see, e.g., [**?**, Subsection 3.1].

Proposition 4.1. *The only non-vanishing homology of a shellable poset is in the dimension of the poset.*

We refer to [**?**, Subsection 3.2] for the notions and facts from poset topology used in the proof of the following lemma. This lemma is undoubtedly previously known, but we were unable to find it in the literature in the form needed for the subsequent theorem.

Lemma 4.2. *If G acts on V as a rigid reflection group, and H is a reflecting hyperplane, then there exists a shelling of $\mathcal{R}_{V,G}$ starting with a facet containing H.*

Proof. Note first that it is equivalent to find such a shelling of the dual $\mathcal{R}^*_{V,G}$ of $\mathcal{R}_{V,G}$. Since $\mathcal{R}^*_{V,G}$ is the standard poset of a hyperplane arrangement, it is a geometric lattice, whose atoms are the reflecting hyperplanes. For any ordering of these atoms $H = H_1, H_2, \ldots, H_t$, label each edge of the Hasse diagram, (x, y), where y covers x, with the least integer i such that the join of x and H_i is y. This is an EL-labelling, so the associated lexicographic ordering on the maximal chains is a shelling, and the first facet of this shelling contains H. □

Theorem 4.3. *If G acts on V as a rigid reflection group, then the intersection poset of $\mathcal{S}_{V,G}$ is shellable.*

Proof. Order the elements of G

$$1 = \sigma_0 \ , \ \sigma_1 \ , \ \cdots \ , \ \sigma_{|G|-1}$$

so that for each $j > 0$ there is some $i < j$ such that $\sigma_i^{-1}\sigma_j$ is a reflection. We then construct a shelling inductively as follows.

First, by the identification $\mathcal{S}_{V,G}(\leqslant(1 \otimes 1)(W)) \cong \mathcal{R}_{V,G}$ from Lemma **??**, list the facets in a shelling of $\mathcal{S}_{V,G}(\leqslant(1 \otimes 1)(V))$. Then, for $j > 0$, given a list of the facets in

$$\bigcup_{j'<j} \mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_{j'})(V))$$

such that each subsequent facet intersects the union of the others in pure codimension 1, choose an $i < j$ such that $\sigma_i^{-1}\sigma_j$ is a reflection. By Lemmas **??** and **??**, list the facets in a shelling of $\mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_j)(V))$ that starts with a facet F_j containing a facet of

$$\mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_i)(V)) \cap \mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_j)(V)) \ = \ \mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_j)(V^{\sigma_i^{-1}\sigma_j})) \, .$$

As this is a codimension 1 subposet of $\bigcup_{j'<j} \mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_{j'})(V))$, the facet F_j intersects the union of previously listed faces in codimension 1. Continue with the list of facets in the chosen shelling of $\mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_j)(V))$.

Iterating this procedure for all $j = 0, \ldots, |G| - 1$ produces a shelling of $\mathcal{S}_{V,G}$. □

As a consequence, we find that our method from Theorem **??** does not provide sharper bounds for rigid reflection groups.

Corollary 4.4. *If G acts on V as a d-dimensional rigid reflection group, then $\mathrm{H}^t_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2]) = 0$ for all $t \neq d$.*

Proof. Since G is a rigid reflection group, G_W is a reflection group for each isotropy subgroup G_W. Then, by Theorem **??** and Proposition **??**, we find that

$$\widetilde{\mathrm{H}}_i(\mathcal{S}_{V,G}(>(1 \otimes 1)(V^{G_W})); \Bbbk) = 0 \quad \text{for all} \quad i \neq \operatorname{codim}(V^{G_W}) - 1 \, .$$

Since

$$\mathcal{S}_{V,G}(>(1 \otimes 1)(V^{G_W})) \cong \mathcal{S}_{V,G}(>(1 \otimes \tau)(V^{G_W}))$$

for any τ, by Lemma **??**, we have $\widetilde{\mathrm{H}}_i(\mathcal{S}_{V,G}(>p); \Bbbk) = 0$ for all $i \neq \operatorname{codim}(p) - 1$ and all p in the intersection poset. The result follows by Theorem **??**. □

Conjecture 4.5. There exists a separating set of size d (that is, there exists a polynomial separating algebra) if and only if G is a rigid reflection group.

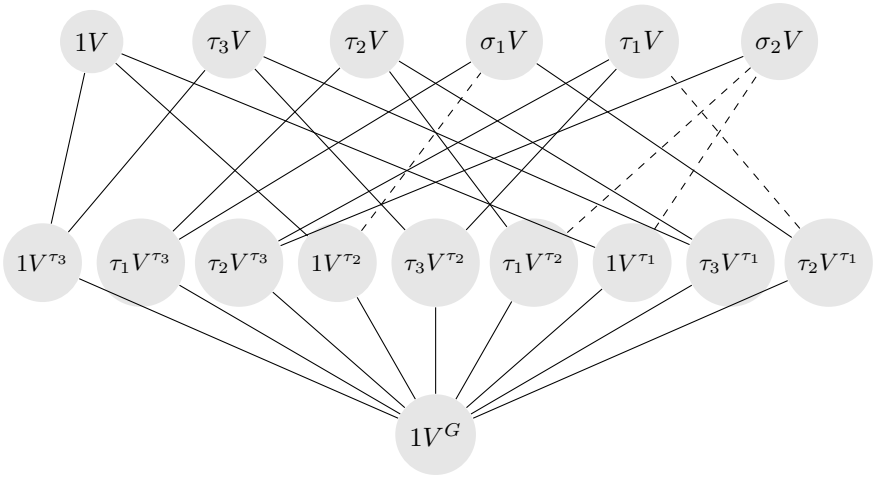

FIGURE 1. The intersection poset of the separating variety of the permutation representation of S_3.

The following example shows that the bounds in Theorem **??** are not necessarily sharp if G is not a reflection group.

Example 4.6. Let G be the symmetric group on three letters, with elements

$$1\ ,\ (12)=\tau_3\ ,\ (13)=\tau_2\ ,\ (23)=\tau_1\ ,\ (132)=\sigma_1\ ,\ (123)=\sigma_2\,.$$

Let V be its standard three-dimensional permutation representation. Let $W = V^{\oplus n}$ with G acting diagonally. The group G acts on V as a rigid reflection group, and its action on W is as a rigid n-reflection group. Note that the intersection poset of $\mathcal{S}_{W,G}$ is isomorphic to that of $\mathcal{S}_{V,G}$, since for any subgroup H of G, one has $W^H = (V^H)^{\oplus n}$. This intersection poset is depicted in Figure **??** where gV is shorthand for $(1 \otimes g)(V)$, and similarly for gV^h.

The complex of $\mathcal{S}_{V,G}(>(1\otimes 1)(V^G))$ is a graph, namely the subgraph of Figure **??** obtained by deleting the bottom vertex. Its homology may be computed by first contracting a maximal tree, depicted with solid lines; the resulting graph consists of the four dotted edges looped around a single point. We thus have

$$\widetilde{\mathrm{H}}_1(\mathcal{S}_{W,G}(>(1\otimes 1)(W^G));\Bbbk) \cong \widetilde{\mathrm{H}}_1(\mathcal{S}_{V,G}(>(1\otimes 1)(V^G));\Bbbk) \cong \Bbbk^4\,.$$

By Theorem **??**, $\mathrm{H}^{5n-2}_{\mathcal{I}(\mathcal{S}_{W,G})}(\Bbbk[W^2]) \neq 0$, so, as in the argument of Theorem **??**, we conclude that any separating set for W has at least $5n-2$ elements. Note that the bound provided by Theorem **??** for W is $4n-1$.

5. Examples of separating sets of minimal size

Below, we present a variety of examples of separating sets that realize the lower bound in Theorem **??**, thereby showing that the bound is sharp for these actions and that the found separating sets are of minimal size. First, we review an example from the first author's thesis:

Proposition 5.1. [**?**, Proposition 5.2.2] *Let $G = \langle\sigma\rangle$ be the cyclic group of order m, and suppose $\Bbbk$ contain ζ, a primitive m^{th} root of unity. Let G act diagonally on*

$\Bbbk[V]$ *by the rule*

$$\sigma(x_i) = \zeta^{d_i} x_i$$

where $1 = d_1 | d_2 | \cdots | d_n | m$. *Then there is a separating set for* $\Bbbk[V]^G$ *of order* $2n-1$.

For this construction, a separating set of monomials $u_{i,j} : 1 \leqslant i \leqslant j \leqslant n$ is first identified; see [**?**, Proposition 5.2.2] for precise formulas for the $u_{i,j}$. The terms naturally align in a triangle. It is then shown that the values of the invariants $u_{i,j}$ can be recovered from the diagonal sums $S_k = \sum_{i+j=k} u_{i,j}$ of the triangle. This "triangle trick" is used in many of the examples below.

It is worth noting that Proposition **??** includes as a special case the m^{th} Veronese subring of a polynomial ring of dimension n, for $\operatorname{char}(\Bbbk) \not| \, m$.

5.1. **Indecomposable representations of cyclic groups of prime order.** In this subsection we construct separating sets of minimal size for the indecomposable modular representations of a cyclic group of prime order, equal to the characteristic of the field $\Bbbk$. Our argument is greatly inspired by Sezer's iterative construction of a separating set (see [**?**]) and uses the triangle trick mentioned above. After an appropriate change of basis, any indecomposable representation of a cyclic group of prime order will be given by a Jordan block of size at most p. We may further choose a basis so that the action on the coordinate ring $\Bbbk[x_1, \ldots, x_n]$ with $n \leqslant p$ is as follows:

$$\begin{aligned} \sigma \cdot x_i &= x_i + x_{i+1}\,, \text{ for } i = 1, \ldots, n-1\,, \\ \sigma \cdot x_n &= x_n\,. \end{aligned}$$

One way to construct some invariants is to take norms (orbit products) and traces (orbit sums) of elements: in fact, by [**?**, Theorem 3], for representations of p-groups, norms and transfers will form a separating set. For $f \in \Bbbk[V]$, the *norm of* f is the orbit product $\mathrm{N}(f) := \prod_{i=0}^{p-1} (\sigma^i \cdot f)$ and the *trace of* f is the orbit sum $\mathrm{Tr}(f) := \sum_{i=0}^{p-1} (\sigma^i \cdot f)$.

Proposition 5.2. *Let* V_n *be the* n*-dimensional indecomposable representation of the cyclic group of order* p. *The set* S_n *of the sum of the elements appearing on the diagonal of the following triangle forms a separating set.*

$$\begin{array}{ccccccc} \mathrm{N}(x_1) & \mathrm{Tr}(x_1 x_2^{p-1}) & \mathrm{Tr}(x_1 x_3^{p-1}) & \cdots & \mathrm{Tr}(x_1 x_{n-1}^{p-1}) & & \\ & \mathrm{N}(x_2) & \mathrm{Tr}(x_2 x_3^{p-1}) & \cdots & \mathrm{Tr}(x_2 x_{n-1}^{p-1}) & & \\ & & \mathrm{N}(x_3) & \ddots & \vdots & & \\ & & & & \mathrm{N}(x_{n-1}) & & \\ & & & & & & x_n^p \end{array} \tag{1}$$

Proof. We proceed by induction on n. For $n = 2$, we have $\Bbbk[x_1, x_2]^{C_p} = \Bbbk[\mathrm{N}(x_1), x_2]$. As x_2 and x_2^p separate the same points, we are done.

Now, suppose $n \geqslant 2$. If $x_n^p = 0$, then $x_n = 0$ and the triangle (**??**) reduces to the triangle for V_{n-1}. Thus the sum of the diagonals separate by the induction hypothesis.

Now suppose that $x_n \neq 0$. For $i \geqslant n-2$, the coefficient of x_i in $\mathrm{Tr}(x_i x_{n-1}^{p-1})$ is

$$\begin{aligned} &x_{n-1}^{p-1} + \textstyle\sum_{l=0}^{p-1} \binom{p-1}{j} x_{n-1}^j x_n^{p-1-j} \left(1 + 2^{p-1-j} + \cdots + (p-1)^{p-1-j}\right) \\ &= x_{n-1}^{p-1} - x_n^{p-1} - x_{n-1}^{p-1} = -x_n^{p-1}. \end{aligned}$$

Indeed, in characteristic p, one has $\left(1+2^{p-1-j}+\ldots+(p-1)^{p-1-j}\right) = -1$ for $j=0$ or $j=p-1$ and zero otherwise. It follows that

$$\Bbbk[x_1,\ldots,x_n,x_n^{-1}] = \Bbbk[\mathrm{Tr}(x_1x_{n-1}^{p-1}),\ldots,\mathrm{Tr}(x_{n-2}x_{n-1}^{p-1}),x_{n-1},x_n,x_n^{-1}]\,.$$

Taking invariants, we then have:

$$\Bbbk[x_1,\ldots,x_n,x_n^{-1}]^{C_p} = \Bbbk[\mathrm{Tr}(x_1x_{n-1}^{p-1}),\ldots,\mathrm{Tr}(x_{n-2}x_{n-1}^{p-1}),\mathrm{N}(x_{n-1}),x_n,x_n^{-1}]\,.$$

That is, the invariants which appear in the one before last column of the triangle (**??**) generate up to dividing by some power of x_n. Now we need only explain how to get these from S_n. The bottom two, $\mathrm{N}(x_{n-1})$ and $\mathrm{Tr}(x_{n-2}x_{n-1}^{p-1})$, are in S_n. As any term in the triangle can be expressed as a polynomial, up to dividing by a power of x_{n-1}, in elements of S_n lying either on the same row or below, we can express the remaining elements of S_n in terms of the sums of the diagonals. □

5.2. **Vector Invariants of V_2.** Let V_2 denote the 2-dimensional indecomposable representation of C_p as above. We consider the diagonal representation of C_p on $V_2^{\oplus n}$. Let $x_1,y_1,\ldots,x_n,y_n$ be a choice of coordinates on $V_2^{\oplus n}$ such that $\sigma\cdot x_i = x_i$, and $\sigma\cdot y_i = x_i+y_i$. The ring of invariants is generated by

$$\begin{aligned}
&x_i\,, && 1\leqslant i\leqslant n\\
&u_{i,i} = \mathrm{N}(y_i) = y_i^p - x_i^{p-1}y_i\,, && 1\leqslant i\leqslant n\\
&u_{i,j} = x_iy_j - x_jy_i\,, && 1\leqslant i<j\leqslant n\\
&\mathrm{Tr}^{C_p}(y_1^{a_1}\cdots y_n^{a_n})\,, && a_i<p\,,\ \Sigma a_i\geqslant 2p-2\,.
\end{aligned}$$

By [**?**, Corollary 3.9.14], the invariants of degree less than $|G|=p$ form a separating set: in particular, the generators

$$x_i : 1\leqslant i\leqslant n \quad \text{and} \quad u_{ij} : 1\leqslant i\leqslant j\leqslant n$$

form a separating set. Note that we have the relations

$$\begin{aligned}
&x_iu_{j,k} - x_ju_{i,k} + x_ku_{i,j} && \forall i<j<k,\\
&x_iu_{j,j} - x_ju_{i,i} + x_i^{p-1}x_j^{p-1}u_{i,j} - u_{i,j}^p && \forall i<j\,.
\end{aligned}$$

Set $S_\ell = \sum_{i+j=\ell} u_{i,j}$ for all $2\leqslant\ell\leqslant 2n$. Remark that the S_ℓ correspond to the diagonal sums of the triangle consisting of the $u_{i,j}$.

Proposition 5.3. *The set of all x_i and S_ℓ is a separating set for $\Bbbk[V_2^{\oplus n}]^{C_p}$.*

Proof. It suffices to show that given the values of all x_i and f_ℓ, we may recover the values of each u_{ij}. We induce on n. If $n=1$, there is nothing to show.

Case 1: $x_n\neq 0$: In this case, we may write

$$u_{i,i} = x_n^{-1}(x_iu_{n,n} + x_i^{p-1}x_n^{p-1}u_{i,n} + (-u_{i,n})^p) \tag{2}$$

$$u_{i,j} = x_n^{-1}(x_ju_{i,n} - x_iu_{j,n})\,, \qquad i<j \tag{3}$$

to express each $u_{i,j}$ with $j<n$ in terms of the x_s and $u_{k,n}$ with $k\geqslant j$. This enables us to express each $u_{i,j}$ in terms of the S_ℓ and x_s: indeed, $u_{n,n}=S_{2n}$, and if each $u_{i,j}$ with $j\geqslant k$ has such an expression, then

$$S_{n+k-1} = u_{k-1,n} + \sum_{\substack{i+j=n+k-1\\ j\geqslant k}} u_{i,j}$$

provides such an expression for $u_{k-1,n}$, and the formulas (**??**) and (**??**) above provide such an expression for $u_{k-1,k-1}$ and each $u_{k-1,j}$.

Case 2: $x_n = 0$: Here, we have $y_n^p = u_{nn}$, so that $u_{i,n} = x_i y_n = x_i u_{n,n}^{1/p}$. Then, by the induction hypothesis, we may express each $u_{i,j}$ with $j < n$ in terms of the x_s and

$$\hat{S}_\ell = \sum_{\substack{i+j=\ell \\ j<n}} u_{i,j} = S_\ell - x_{\ell-n} u_{n,n}^{1/p}$$

(where $x_{\ell-n} := 0$ for $\ell \leqslant n$), and thus in terms of the x_s and S_ℓ. □

As the action of C_p on $V_2^{\oplus n}$ is generated by n-reflections, by Theorem **??**, any separating set for $\Bbbk[V_2^{\oplus n}]^{C_p}$ has at least $3n-1$ elements. Thus, the set

$$\{x_i, S_\ell \mid 1 \leqslant i \leqslant n, 2 \leqslant \ell \leqslant 2n\}$$

is a separating set of minimal size.

5.3. **A Non-Rigid Reflection Group.** Let $\Bbbk$ have characteristic 2 and G be the finite subgroup of $\mathrm{GL}_7(\mathbb{F}_2)$ given by

$$G := \left\{ \left(\begin{array}{cccc|c} & & I_4 & & \mathbf{0} \\ \hline \alpha_1 & 0 & 0 & \alpha_4 & \\ 0 & \alpha_2 & 0 & \alpha_4 & I_3 \\ 0 & 0 & \alpha_3 & \alpha_4 & \end{array} \right) \;\middle|\; \alpha_1, \ldots, \alpha_4 \in \mathbb{F}_2 \right\},$$

where I_m denotes the $m \times m$ identity matrix. The group G is isomorphic to C_2^4, and generated by reflections (namely those elements where exactly one of the α_i's is non-zero). This is a remarkable example since its invariant ring is not Cohen-Macaulay (see [**?**]) and, moreover, neither is any graded separating subalgebra (see [**?**]) despite the action of G being generated by reflections.

Setting all α_i's to be 1 yields an element σ whose fixed space of codimension 3 is a minimal reflecting subspace. By Theorem **??**, it follows that any separating set contains at least 9 elements. Writing x_i for the coordinate functions on $V = \Bbbk^7$, one has the minimal generating set

$$\Bbbk[V]^G = \Bbbk[x_1, x_2, x_3, x_4, f_1, f_2, f_3, g_1, g_2, g_3, r]$$

where $\deg f_i = 3$, $\deg g_i = 4$, and $\deg r = 5$. Using a computer algebra system, one verifies that

$$f_i r \in \Bbbk[x_1, x_2, x_3, x_4, f_1, f_2, f_3, g_1, g_2, g_3], \text{ for } \quad i = 1, 2, 3, \tag{4}$$

$$r^2 \equiv (x_1 + x_4)^2 g_2 g_3 \mod (f_1, f_2, f_3)\,. \tag{5}$$

Thus, given the values of the x_i's, f_i's, and g_i's, one may recover the value of r using (**??**) if some $f_i \neq 0$ and (**??**) if all $f_i = 0$, so we can leave out r still have a separating set. One also finds

$$(x_3 + x_4) f_3 = f_2(x_2 + x_4) + f_1(x_1 + x_4) \tag{6}$$

$$(x_i + x_4)^2 g_3 \equiv f_i^2 \mod (x_3 + x_4), \quad i = 1, 2, \tag{7}$$

$$f_3 \equiv 0 \mod (x_1 + x_4, x_2 + x_4, x_3 + x_4)\,. \tag{8}$$

Hence, given the values of the x_i's, f_1, and f_2, one can either obtain the value of f_3 (using (**??**) if $x_3 \neq x_4$ or (**??**) if $x_1 = x_2 = x_3 = x_4$) or g_3 (using (**??**) if $x_3 = x_4$ and either $x_1 \neq x_4$ or $x_2 \neq x_4$). Concluding, we have the following:

Proposition 5.4. *The invariants $x_1, x_2, x_3, x_4, f_1, f_2, g_1, g_2, f_3 + g_3$ form a separating set for $\Bbbk[V]^G$ of minimal size.*

Acknowledgements

The authors thank MSRI, where most of the work on this project was completed. We also thank Dave Benson, Gregor Kemper, Anurag Singh, and Bernd Sturmfels for helpful conversations.

References

[1] Josep Àlvarez Montaner, Ricardo García López, and Santiago Zarzuela Armengou. Local cohomology, arrangements of subspaces and monomial ideals. *Adv. Math.*, 174 (2003), no. 1, 35–56.

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

[3] Jan Draisma, Gregor Kemper, and David Wehlau. Polarization of separating invariants. *Canad. J. Math.*, 60 (2008), no. 3, 556–571.

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

[5] Emilie Dufresne. *Separating Invariants.* Ph.D. thesis, Queens University, Kingston, Ontario, Canada. 2008.

[6] Emilie Dufresne, Jonathan Elmer, and Martin Kohls. The Cohen-Macaulay property of separating invariants of finite groups. *Transform. Groups*, 14 (2009), no. 4, 771–785.

[7] Alexander Grothendieck. *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux* (*SGA* 2). North-Holland Publishing Co., Amsterdam, 1968. Augmenté d'un exposé par Michèle Raynaud, Séminaire de Géométrie Algébrique du Bois-Marie, 1962, Advanced Studies in Pure Mathematics, Vol. 2.

[8] Robin Hartshorne. Cohomological dimension of algebraic varieties. *Ann. of Math. (2)* 88 (1968), 403–450.

[9] Srikanth B. Iyengar, Graham J. Leuschke, Anton Leykin, Claudia Miller, Ezra Miller, Anurag K. Singh, and Uli Walther. *Twenty-four hours of local cohomology*, volume 87 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007.

[10] Gregor Kemper. On the Cohen-Macaulay property of modular invariant rings. *J. Algebra*, 215 (1999), no. 1, 330–351.

[11] Gregor Kemper. Loci in quotients by finite groups, pointwise stabilizers and the Buchsbaum property, *J. Reine Angew. Math.*, 547 (2002), 69–96.

[12] Gregor Kemper. Computing invariants of reductive groups in positive characteristic. *Transform. Groups*, 8 (2003), no. 2, 159–176.

[13] Gennady Lyubeznik. On some local cohomology modules. *Adv. Math.*, 213 (2007), no. 2, 621–643.

[14] Mara Neusel and Müfit Sezer. Separating invariants for modular p-groups and groups acting diagonally. *Math. Res. Lett.*, 16 (2009), no. 6, 1029–1036.

[15] Christian Peskine and Lucien Szpiro. Dimension projective finie et cohomologie locale. *Inst. Hautes Études Sci. Publ. Math.*, no. 42 (1973), 47–119.

[16] Fabian Reimers. Polynomial separating algebras and reflection groups. arXiv:1307.7522.

[17] Müfit Sezer. Explicit separating invariants for cyclic P-groups. *J. Combin. Theory Ser. A* , 118 (2011), no. 2, 681–689.

[18] Michelle Wachs. Poset topology: tools and applications. *Geometric combinatorics,* 497–615, volume 13 of *IAS/Park City Math. Ser.,* Amer. Math. Soc., Providence, RI, 2007.

Department of Mathematical Sciences, Durham University, Science Laboratories, South Road, Durham DH1 3LE, UK
E-mail address: e.s.dufresne@durham.ac.uk

Department of Mathematics, University of Utah, 155 South 1400 East, Room 233, Salt Lake City, UT 84112-0090, USA
E-mail address: jeffries@math.utah.edu