The subring of group cohomology constructed by permutation representations*

David J. Green Ian J. Leary† Björn Schuster

21 April 1999

Abstract

Each permutation representation of a finite group G can be used to pull cohomology classes back from a symmetric group to G. We study the ring generated by all classes that arise in this fashion, describing its variety in terms of the subgroup structure of G.

We also investigate the effect of restricting to special types of permutation representations, such as $GL_n(\mathbb{F}_p)$ acting on flags of subspaces.

Introduction

Each action of a finite group G on a set X can be used to pull back cohomology classes from the cohomology of the symmetric group on X to the cohomology of G. For example, the characteristic classes of Segal and Stretch [6] arise in this way.

We shall study the cohomology classes that come from all actions of a fixed group G by taking the ring S_h they generate and investigating its variety. In Theorem 1.5 we obtain a description of this variety in terms of the group structure of G. Typically the inclusion of S_h in the cohomology ring is not an inseparable isogeny; but it does always induce a bijection of irreducible components. Equivalently, distinct minimal prime ideals in the cohomology ring have distinct intersections with S_h. The idea of studying the variety of the cohomology ring originates in Quillen's paper [5]. Our results rely on work in [4], where two of the current authors suggest an extension of Quillen's results to certain subrings of the cohomology ring.

We also investigate what happens when we impose conditions on the G-sets by putting restrictions on the point stabilizers. In particular we show that, for

*1991 *Mathematics Subject Classification* 20J06.

†Partially funded by the Nuffield Foundation, grant no. SCI/180/96/127

large values of n, the $GL_{2n}(\mathbb{F}_p)$ actions with parabolic stabilizers give rise to a strictly smaller subring than the subring for arbitrary actions, which in turn is strictly smaller than the whole cohomology ring.

Throughout this paper, G will be a finite group and p a prime number. We write $\mathrm{H}^*(G)$ for the mod-p cohomology $\mathrm{H}^*(G, \mathbb{F}_p)$ of G.

1 Definitions and our main theorem

First we describe the object of study precisely.

Definition 1.1 A non-empty family $\mathcal{F}$ of subgroups of G will be called *admissible* if it is closed under conjugation in G, and the subgroup $\bigcap_{H\in\mathcal{F}} H$ of G is a p'-group. A G-set X will be called an $\mathcal{F}$-set if each point stabilizer belongs to $\mathcal{F}$.

In particular, the family $\mathcal{F}_h$ consisting of all subgroups of G is admissible, and all G-sets are $\mathcal{F}_h$-sets.

Definition 1.2 Each finite G-set X induces a homomorphism $\rho_X\colon G \to \Sigma_n$, where n is $|X|$. This induces in turn a ring homomorphism $\rho_X^*\colon \mathrm{H}^*(\Sigma_n) \to \mathrm{H}^*(G)$. Define $S_\mathcal{F}$ as the subring of $\mathrm{H}^*(G)$ generated by all $\mathrm{Im}(\rho_X^*)$ with X an $\mathcal{F}$-set.

We shall now determine the variety of this ring $S_\mathcal{F}$. The following definition is needed to state the result.

Definition 1.3 Denote by $\mathcal{A}_\mathcal{F}$ the category whose objects are the elementary abelian p-subgroups of G, with $\mathcal{A}_\mathcal{F}(V, W)$ the set of injective group homomorphisms $f\colon V \to W$ satisfying: for every $H \in \mathcal{F}$ the V-sets $f^!(G/H)$ and G/H are isomorphic. Here $f^!(G/H)$ means the following action of V on G/H:

$$k * gH = f(k)gH\,.$$

Remark 1.4 The category $\mathcal{A}_{\mathcal{F}_h}$ is identified in Lemma 2.2.

Recall that the variety $\mathrm{var}(R)$ of a connected graded commutative $\mathbb{F}_p$-algebra R is the functor that assigns to each algebraically closed field k the topological space of ring homomorphisms from R to k with the Zariski topology.

Theorem 1.5 *The cohomology ring* $\mathrm{H}^*(G)$ *is finitely generated as a module over* $S_\mathcal{F}$. *The restriction maps in cohomology induce a natural homeomorphism*

$$\operatorname*{colim}_{V\in\mathcal{A}_\mathcal{F}} \mathrm{var}(\mathrm{H}^*(V)) \cong \mathrm{var}(S_\mathcal{F})\,.$$

Proof. Let $H_1, \ldots, H_r$ be a full set of class representatives for the conjugation action of G on $\mathcal{F}$. Let X be the G-set $(G/H_1)\amalg\cdots\amalg(G/H_r)$, and $n = |X|$. Then

X is an $\mathcal{F}$-set, and the kernel of the associated group homomorphism $\rho\colon G \to \Sigma_n$ is a p'-group by admissibility.

Now compose ρ with the regular representation reg_{Σ_n} of Σ_n. We obtain a degree $n!$ representation of G, whose restriction to a Sylow p-subgroup P of G is a direct sum of copies of the regular representation. In particular, it is a faithful representation of P. The Chern classes of $\mathrm{reg}_{\Sigma_n} \circ \rho$ lie in $S_{\mathcal{F}}$ as they are images under ρ^*. Hence by Venkov's proof [7] of the Evens–Venkov theorem, $H^*(P)$ is finitely generated as a module over $S_{\mathcal{F}}$. Therefore $\mathrm{H}^*(G)$ is finitely generated too.

This representation $\mathrm{reg}_{\Sigma_n} \circ \rho$ also restricts to every elementary abelian p-subgroup of G as a (non-zero) direct sum of copies of the regular representation, and so is p-regular in the sense of [4]. So $S_{\mathcal{F}}$ contains the Chern classes of a p-regular representation. Moreover, the ring $S_{\mathcal{F}}$ is clearly homogeneously generated and closed under the action of the Steenrod algebra. By Theorem 6.1 of [4] it follows firstly that $\mathrm{var}(S_{\mathcal{F}})$ is a colimit of the desired form over *some* category of elementary abelians; and secondly that Lemma 1.6 identifies this category as being $\mathcal{A}_{\mathcal{F}}$. ■

Lemma 1.6 *Let V, W be elementary abelian subgroups of G, and $f\colon V \to W$ an injective group homomorphism. Then f lies in $\mathcal{A}_{\mathcal{F}}$ if and only if for every $x \in S_{\mathcal{F}}$, the class $\mathrm{Res}^G_V(x) - f^* \mathrm{Res}^G_W(x)$ lies in the nilradical of $\mathrm{H}^*(V)$.*

Proof. Suppose $f \in \mathcal{A}_{\mathcal{F}}$. Pick any $\mathcal{F}$-set Y, and let $\rho\colon G \to \Sigma_{|Y|}$ be the associated group homomorphism. Since the V-sets Y and $f^!(Y)$ are isomorphic, f induces a map $\rho(V) \to \rho(W)$, and this is conjugation by some $\sigma \in \Sigma_{|Y|}$. Hence $\mathrm{Res}^G_V - f^* \mathrm{Res}^G_W$ kills $\mathrm{Im}(\rho^*)$.

Conversely, suppose that $f \notin \mathcal{A}_{\mathcal{F}}$. Recall that in the proof of Theorem 1.5 we constructed an $\mathcal{F}$-set X, such that the kernel of the associated group homomorphism $\rho\colon G \to \Sigma_{|X|}$ is a p'-group. By assumption on f there is some $H \in \mathcal{F}$ with $f^!(G/H)$, G/H non-isomorphic as V-sets. Define Y by

$$Y = \begin{cases} X \amalg (G/H) & \text{if } f^!(X),\ X \text{ isomorphic as } V\text{-sets} \\ X & \text{otherwise.} \end{cases}$$

Then Y is an $\mathcal{F}$-set and V acts faithfully on $Y, f^!(Y)$, but these two V-sets are non-isomorphic.

We have thus constructed embeddings of V and W in $\Sigma_{|Y|}$, such that f is not induced by conjugation in $\Sigma_{|Y|}$. Therefore there is a class $\xi \in \mathrm{H}^*(\Sigma_{|Y|})$ such that $\mathrm{Res}^{\Sigma_{|Y|}}_V(\xi) - f^* \mathrm{Res}^{\Sigma_{|Y|}}_W(\xi)$ is not nilpotent (apply the results of [4, §9] to the group $\Sigma_{|Y|}$). Moreover, these embeddings of V, W in $\Sigma_{|Y|}$ factor through $G \to \Sigma_{|Y|}$. Pulling ξ back to $\mathrm{H}^*(G)$, we get the desired class. ■

2 Examples

Definition 2.1 We define the hereditary category $\mathcal{A}_h$ of G to be $\mathcal{A}_{\mathcal{F}_h}$, where $\mathcal{F}_h$ is the admissible family of all subgroups of G. Write S_h for $S_{\mathcal{F}_h}$.

Recall that $\sim_G$ denotes the equivalence relation conjugacy in G.

Lemma 2.2 *Let $f\colon V \to W$ be an injective group homomorphism between elementary abelian subgroups of G. Then f lies in $\mathcal{A}_h$ if and only if $f(U) \sim_G U$ for every elementary abelian $U \leq V$.*

Let $\mathcal{F}$ be an admissible family containing all nontrivial elementary abelian p-subgroups of G. Then $\mathcal{A}_{\mathcal{F}} = \mathcal{A}_h$.

Remark 2.3 This property of $\mathcal{A}_h$ is the reason for the name hereditary.

Proof. We prove the first part holds for any $\mathcal{F}$ satisfying the conditions of the second part, not just for $\mathcal{F}_h$.

First suppose that U is a subgroup of V and $f(U) \not\sim_G U$. Then the V-set G/U has a point stabilized by U, but $f^!(G/U)$ does not. Hence these two V-sets are not isomorphic, and so f does not lie in $\mathcal{A}_{\mathcal{F}}$.

For the if part, consider any $H \in \mathcal{F}$ and any $U \leq V$. The coset gH is fixed by U if and only if $U^g \leq H$. Since $f(U) \sim_G U$, the number of U-fixed points in $f^!(G/H)$ is the same as for G/H. It follows that the V-sets $f^!(G/H)$ and G/H are isomorphic. ∎

Corollary 2.4 *The category $\mathcal{A}_h$ is the unique largest category of elementary abelians which is closed in the sense of [4, §9], and in which objects are isomorphic if and only if they are conjugate as subgroups of G.*

Proof. Closure means that all inclusion and conjugation maps are contained in $\mathcal{A}_h$; that isomorphisms lie in $\mathcal{A}_h$ if and only if their inverses do; and that $f_{|U}\colon U \to f(U)$ lies in $\mathcal{A}_h$ for every $f\colon V \to W$ in $\mathcal{A}_h$ and every $U \leq V$. ∎

Remark 2.5 It follows that "intersection with S_h" induces a bijection from the minimal primes of $\mathrm{H}^*(G)$ to those of S_h. Hence the irreducible components of $\mathrm{var}(\mathrm{H}^*(G))$ and of $\mathrm{var}(S_h)$ are in natural one-to-one correspondence.

Definition 2.6 Let G be the general linear group $GL_n(\mathbb{F}_p)$. We define the parabolic category $\mathcal{A}_\pi$ to be $\mathcal{A}_{\mathcal{F}_\pi}$, where $\mathcal{F}_\pi$ is the collection of all parabolic subgroups of G. Write S_π for $S_{\mathcal{F}_\pi}$.

Proposition 2.7 *The parabolic category is admissible. We have*

$$\mathrm{var}(S_h) \cong \operatorname*{colim}_{V \in \mathcal{A}_h} \mathrm{var}(\mathrm{H}^*(V)) \quad \textit{and} \quad \mathrm{var}(S_\pi) \cong \operatorname*{colim}_{V \in \mathcal{A}_\pi} \mathrm{var}(\mathrm{H}^*(V)) \,.$$

Proof. The upper triangular matrices constitute a parabolic subgroup, as do the lower triangular matrices. These two groups intersect in a p'-group, so $\mathcal{F}_\pi$ is admissible. Apply Theorem 1.5 for the admissible families $\mathcal{F}_h$ and $\mathcal{F}_\pi$. ∎

Define the Quillen category $\mathcal{A}$ to be the category whose objects are the elementary abelian p-subgroups of G, with morphisms induced by inclusion and conjugation. It is a well-known theorem of Quillen (see [2, §9.2]) that the restriction maps induce a natural isomorphism

$$\operatorname*{colim}_{V \in \mathcal{A}} \operatorname{var}(\mathrm{H}^*(V)) \cong \operatorname{var}(\mathrm{H}^*(G)) .$$

It follows from [4] that the inclusion of $S_\mathcal{F}$ in $\mathrm{H}^*(G)$ induces an isomorphism of varieties if and only if $\mathcal{A}_\mathcal{F} = \mathcal{A}$, and that $S_{\mathcal{F}_1}$, $S_{\mathcal{F}_2}$ have the same variety as each other if and only if $\mathcal{A}_{\mathcal{F}_1} = \mathcal{A}_{\mathcal{F}_2}$.

Example 2.8 Let p be an odd prime, and let $1 < q < p$. For any finite group G and any elementary abelian $V \leq G$, the automorphism $v \mapsto v^q$ of V lies in $\mathcal{A}_h$ by Lemma 2.2. But in general this map does not lie in $\mathcal{A}$. An example is when G is abelian (and not a p'-group). For such groups, the inclusion of S_h in $\mathrm{H}^*(G)$ in not an inseparable isogeny.

Example 2.9 In Corollary 3.4, we shall see that for $n \geq 3$ and G the group $GL_{2n}(\mathbb{F}_p)$, there is a rank two elementary abelian subgroup E of G such that not all automorphisms of E lie in $\mathcal{A}$; and yet all nontrivial elements of E are conjugate in G, which means that all automorphisms of E lie in $\mathcal{A}_h$. Hence the inclusion of S_h in $\mathrm{H}^*(G)$ is not an inseparable isogeny.

Example 2.10 In Theorem 3.6, we shall see that for $n \geq 6$ and G the group $GL_{2n}(\mathbb{F}_p)$, there are non-conjugate rank two elementary abelian subgroups of G which are isomorphic in $\mathcal{A}_\pi$. Hence the varieties of S_π, S_h and $\mathrm{H}^*(G)$ are all distinct.

Example 2.11 The elementary abelian p-subgroups of G form an admissible family, as do all p-subgroups of G. If G has p-rank at least two, then we can omit the trivial subgroup in both families.

In all these cases, the category $\mathcal{A}_\mathcal{F}$ is equal to $\mathcal{A}_h$ by Lemma 2.2. Hence inclusion of $S_\mathcal{F}$ in S_h is an inseparable isogeny.

Example 2.12 Following Alperin [1], we define a subgroup H of an abstract finite group G to be parabolic if $H = N_G(O_p(H))$. That is, the parabolics are the normalizers of the p-stubborn subgroups. For $G = GL_n(\mathbb{F}_p)$, this coincides with the normal definition of parabolic subgroup.

If $O_p(G) = 1$ then the parabolic subgroups and the p-stubborn subgroups each form admissible families, since Sylow p-subgroups are p-stubborn and $O_p(G)$ is the intersection of all Sylow p-subgroups.

For $p = 11$ the sporadic finite simple group J_4 has the trivial intersection property: distinct Sylow p-subgroups intersect trivially. Hence the parabolic subgroups are the admissible family consisting of J_4 itself and the Sylow normalizers. The action of any order p cyclic subgroup on cosets of a Sylow normalizer has one fixed point, with the remaining orbits having length p. As there are two distinct conjugacy classes of order p cyclics, the parabolic category is larger than the hereditary category. The cohomology of J_4 at the prime 11 was computed in [3].

Example 2.13 In general the subring S_h is far larger than the subring generated by Chern classes of permutation representations: i.e., the subring generated by all images of $\mathrm{H}^*(BU(n))$ under homomorphisms $G \to \Sigma_n \to U(n)$, where Σ_n is embedded in $U(n)$ as the permutation matrices.

In [4] it was shown that the variety for this subring is the colimit over the category $\mathcal{A}_P$, where $f\colon V \to W$ lies in $\mathcal{A}_P$ if and only if $f(U) \sim_G U$ for every *cyclic* subgroup U of V. This category is in general far larger than $\mathcal{A}_h$. For example, there are elementary abelian p-groups of rank two in $GL_3(\mathbb{F}_p)$ that are not conjugate (and hence not isomorphic in $\mathcal{A}_h$), but are isomorphic in $\mathcal{A}_P$.

3 An extended example

Fred Cohen asked the third author about the subring of $\mathrm{H}^*(GL_n(\mathbb{F}_p))$ generated by the permutation representations on flags. In our language, the question concerns the subring S_π. This question provided the starting point for the current paper. We provide a partial answer to this question by comparing the varieties for $\mathrm{H}^*(GL_n(\mathbb{F}_p))$, S_h and S_π, which is equivalent to comparing the categories $\mathcal{A}$, $\mathcal{A}_h$ and $\mathcal{A}_\pi$. Recall that there are inclusions

$$\mathcal{A} \subseteq \mathcal{A}_h \subseteq \mathcal{A}_\pi \,.$$

Let G be the general linear group $GL_{2n}(\mathbb{F}_p)$. We show that all three categories are distinct for $n \geq 6$. The most time consuming part is showing that $\mathcal{A}_\pi$ differs from $\mathcal{A}_h$ for such n. By Corollary 2.4 it suffices to show that there are elementary abelian p-subgroups of G which are isomorphic in $\mathcal{A}_\pi$ but not conjugate in G. We shall find rank 2 examples using modular representation theory.

Let p be a prime number, and let A, B be generators for the rank 2 elementary abelian p-group $V \cong C_p \times C_p$. To each matrix $J \in GL_n(\mathbb{F}_p)$, there is an associated representation $\rho_J\colon V \to GL_{2n}(\mathbb{F}_p)$ defined by

$$A \overset{\rho_J}{\longmapsto} \begin{pmatrix} I & I \\ 0 & I \end{pmatrix} \qquad B \overset{\rho_J}{\longmapsto} \begin{pmatrix} I & J \\ 0 & I \end{pmatrix} ,$$

where $I \in GL_n(\mathbb{F}_p)$ is the identity matrix. The following lemma is well-known in the modular representation theory of V.

Lemma 3.1 *Let $J, J' \in GL_n(\mathbb{F}_p)$. Then the representations $\rho_J, \rho_{J'}$ are isomorphic if and only if J, J' are conjugate in $GL_n(\mathbb{F}_p)$.*

Proof. The centralizer of $\left(\begin{smallmatrix} I & I \\ 0 & I \end{smallmatrix}\right)$ consists of all matrices of the form $\left(\begin{smallmatrix} A & B \\ 0 & A \end{smallmatrix}\right)$. The conjugate of $\left(\begin{smallmatrix} I & J \\ 0 & I \end{smallmatrix}\right)$ under such a matrix is $\left(\begin{smallmatrix} I & J' \\ 0 & I \end{smallmatrix}\right)$ with $J' = AJA^{-1}$. ∎

Lemma 3.2 *For any matrix $M \in GL_n(\mathbb{F}_p)$, the matrix $\left(\begin{smallmatrix} I & M \\ 0 & I \end{smallmatrix}\right)$ is conjugate in $GL_{2n}(\mathbb{F}_p)$ to $\left(\begin{smallmatrix} I & I \\ 0 & I \end{smallmatrix}\right)$.*

Proof. Conjugate on the right by $\left(\begin{smallmatrix} M & 0 \\ 0 & I \end{smallmatrix}\right)$. ∎

First we compare the categories $\mathcal{A}_h$ and $\mathcal{A}$.

Lemma 3.3 *Suppose there is a primitive element $\theta \in \mathbb{F}_{p^n}/\mathbb{F}_p$ with minimal polynomial f such that $\theta + 1$ is not a root of f. Then the Quillen category $\mathcal{A}$ for $G = GL_{2n}(\mathbb{F}_p)$ is strictly smaller than the hereditary category $\mathcal{A}_h$.*

Proof. Let $J \in GL_n(\mathbb{F}_p)$ be the matrix in rational canonical form with characteristic polynomial f. Since f is irreducible, J has no eigenvalues in $\mathbb{F}_p$. In particular, this means that $I + J$ lies in $GL_n(\mathbb{F}_p)$. The condition on the roots of f means that J and $I + J$ have distinct characteristic polynomials, and so are non-conjugate in $GL_n(\mathbb{F}_p)$.

Let E be $\mathrm{Im}(\rho_J)$, the rank 2 elementary abelian generated by $a = \rho_J(A)$ and $b = \rho_J(B)$. Hence

$$a = \begin{pmatrix} I & I \\ 0 & I \end{pmatrix} \qquad b = \begin{pmatrix} I & J \\ 0 & I \end{pmatrix} \qquad ab = \begin{pmatrix} I & I+J \\ 0 & I \end{pmatrix} .$$

Let ϕ be the automorphism of E which fixes a and sends b to ab. By the proof of Lemma 3.1 we see that $\phi \notin \mathcal{A}$, since J and $I + J$ are not conjugate. To see that $\phi \in \mathcal{A}_h$, it suffices by Lemma 2.2 to show that $e, \phi(e)$ are conjugate in $G = GL_{2n}(\mathbb{F}_p)$ for each nontrivial $e \in E$. But this follows from Lemma 3.2. ∎

Corollary 3.4 *Set $n_0 = 2$ for $p \geq 3$ and $n_0 = 3$ for $p = 2$. For $G = GL_{2n}(\mathbb{F}_p)$ and $n \geq n_0$, the Quillen category $\mathcal{A}$ is strictly smaller than the hereditary category $\mathcal{A}_h$.*

Proof. We show that there is a θ satisfying the conditions of Lemma 3.3. The Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ is cyclic of order n, generated by the Frobenius automorphism. Hence $\theta \in \mathbb{F}_{p^n}$ has the same minimal polynomial as $\theta + 1$ if and only if θ is a root of $x^{p^m} - x - 1$ for some $m < n$. Therefore there are at least $p^n - p^{n-1} - p^{n-2} - \cdots - p$ elements θ of $\mathbb{F}_{p^n}$ such that $\theta, \theta + 1$ do not have the same minimal polynomial. If $p \geq 3$ and $n \geq 2$ then this exceeds p^{n-1}, and there are at most p^{n-1} non-primitive elements of $\mathbb{F}_{p^n}/\mathbb{F}_p$: hence there exists a θ of the required form.

Now suppose that p is 2. The roots of $x^{2^m} - x - 1$ all lie in $\mathbb{F}_{2^{2m}}$, and so can only be primitive elements of $\mathbb{F}_{2^n}/\mathbb{F}_2$ if $n \mid 2m$. Since $m < n$, this can only happen if $n = 2m$. So the number of $\theta \in \mathbb{F}_{2^n}/\mathbb{F}_2$ such that θ, $\theta + 1$ have distinct minimal polynomials exceeds 2^{n-1} provided $n > 2$, and there are at most 2^{n-1} non-primitives. Again, the required θ exists. ∎

Now we compare the categories $\mathcal{A}_\pi$ and $\mathcal{A}_h$. To each irreducible degree n monic polynomial $f \in \mathbb{F}_p[x]$ there is an associated $(n \times n)$-matrix J_f in rational canonical form. Define the representation $\rho_f \colon V \to GL_{2n}(\mathbb{F}_p)$ to be ρ_{J_f}. By Lemma 3.1, distinct f give rise to non-isomorphic representations.

Proposition 3.5 *Let H be a parabolic subgroup of $GL_{2n}(\mathbb{F}_p)$, and let f be an irreducible degree n polynomial. The embedding ρ_f turns G/H into a V-set. The isomorphism type of this V-set does not depend on f.*

Theorem 3.6 *Set $n_0 = 5$ for $p \geq 5$ and $n_0 = 6$ for $p = 2, 3$. For $G = GL_{2n}(\mathbb{F}_p)$ and $n \geq n_0$, there are rank two elementary abelian subgroups of G which are isomorphic in the parabolic category $\mathcal{A}_\pi$ without being conjugate in G.*

Proof. For any pair f, g of irreducible degree n monic polynomials over $\mathbb{F}_p$, the isomorphism

$$\rho_g \circ \rho_f^{-1} \colon \operatorname{Im}(\rho_f) \longrightarrow \operatorname{Im}(\rho_g)$$

lies in $\mathcal{A}_\pi$ by Proposition 3.5. As distinct irreducible polynomials give rise to non-isomorphic representations, the number of irreducible g such that $\operatorname{Im}(\rho_g)$ is conjugate to a given $\operatorname{Im}(\rho_f)$ cannot exceed $|\operatorname{Aut}(V)| = (p^2 - 1)(p^2 - p)$. But for $n \geq n_0$ there are always more irreducibles than this. For the total number of irreducibles is equal to π_n/n, where π_n is the number of primitive elements in $\mathbb{F}_{p^n}/\mathbb{F}_p$. We have $\pi_5 = p^5 - p$, $\pi_6 = p^6 - p^3 - p^2 + p$ and $\pi_n \geq p^n - p^{n-2}$ for $n \geq 7$. It is then straightforward to check that $\pi_n/n > (p^2 - 1)(p^2 - p)$ for $n \geq n_0$. ∎

We now derive some results needed in the proof of Proposition 3.5. We take f to be a degree n irreducible polynomial over $\mathbb{F}_p$, and $J = J_f$ to be the associated matrix in rational canonical form.

Lemma 3.7 *Let W be a proper subspace of $\mathbb{F}_p^n$. Define m, r by $m = \dim(W)$ and $m + r = \dim(W + JW)$. Then there is partition $\lambda = (\lambda_1, \ldots, \lambda_r)$ of m with length r (so $\lambda_r \geq 1$) and elements $w_1, \ldots, w_r$ of W, such that*

1. *The $J^a w_i$ for $1 \leq i \leq r$ and $0 \leq a \leq \lambda_i - 1$ are a basis for W, and*
2. *The $J^a w_i$ for $1 \leq i \leq r$ and $0 \leq a \leq \lambda_i$ are a basis for $W + JW$.*

We call such an r-tuple $w_1, \ldots, w_r$ a (J,λ)-base for W.

Furthermore, λ is uniquely determined by J, W; and the number of (J,λ)-bases for W depends solely on λ.

Observe that $m + r \leq n$ and that $r \leq m$. Since J is the rational canonical form associated to an irreducible polynomial, there are no J-invariant subspaces other than 0 and $\mathbb{F}_p^n$. Hence $r = 0$ if and only if $m = 0$.

Proof. The proof is by induction on m. The case $m = 0$ is clear. Now suppose that $m > 0$ and the result has been proved for $\dim(W) \leq m - 1$. Set $W' = W \cap J^{-1}W$, so $\dim(W') = m - r$. Define r' by $r' = \dim(W' + JW') - \dim(W')$.

As $m > 0$ we have $m - r \leq m - 1$, so can apply the result to W'. Thus we obtain a length r' partition $\lambda' = (\lambda'_1, \ldots, \lambda'_{r'})$ of $m - r$ and an r'-tuple $w'_1, \ldots, w'_{r'} \in W'$. For $1 \leq i \leq r'$ set $\lambda_i = \lambda'_i + 1$ and $w_i = w'_i$. Observe that

$$\dim(W) - \dim(W' + JW') = r - r' .$$

Pick a basis $w_{r'+1}, \ldots, w_r$ for any complement of $W' + JW'$ in W, and set $\lambda_i = 1$ for $r' < i \leq r$. Then λ is a length r partition of n, and the $J^a w_i$ for $1 \leq i \leq r$ and $0 \leq a \leq \lambda_i - 1$ are a basis for W.

Moreover, the $J^{\lambda'_i} w'_i$ for $1 \leq i \leq r'$ are a basis for a complement of W' in $W' + JW'$; and $w_{r'+1}, \ldots, w_r$ are a basis for a complement of $W' + JW'$ in W. Hence the $J^{\lambda_i - 1} w_i$ for $1 \leq i \leq r$ are a basis for a complement of W' in W. By definition of W', this means that the $J^{\lambda_i} w_i$ for $1 \leq i \leq r$ are a basis for a complement of W in $W + JW$. So the w_i constitute a (J,λ)-base.

Conversely, suppose that $\mu \dashv m$ has length r, and that $v_1, \ldots, v_r$ is a (J,μ)-base for W. The elements $J^a v_i$ for $0 \leq a \leq \mu_i - 2$ are a basis for W', the $J^{\mu_i - 1} v_i$ with $\mu_i \geq 2$ extend this to a basis for $W' + JW'$, and the v_i with $\mu_i = 1$ extend this to a basis for W. Hence the number of i with $\mu_i = 1$ is equal to $\dim(W) - \dim(W' + JW')$. Passing to W', we deduce by induction that λ and μ are equal; and that λ alone determines the number of (J,λ)-bases $w_1, \ldots, w_r$. ■

Lemma 3.8 *Fix J and fix partitions λ, λ'. For any proper $W \subset \mathbb{F}_p^n$ with partition λ, the number of subspaces W' of W with partition λ' depends solely on λ, λ'.*

Proof. Denote by w_i, w'_i the elements of a (J,λ)-base for W, W' respectively. Set $m = \dim(W)$ and $r = \dim(W + JW) - m$, as in Lemma 3.7.

Construct a basis $b_1, \ldots, b_n$ for $\mathbb{F}_p^n$ as follows:

- $b_1, \ldots, b_m$ is the the basis $w_1, Jw_1, \ldots, J^{\lambda_1 - 1} w_1,\ w_2, \ldots, J^{\lambda_r - 1} w_r$ for W given by Lemma 3.7;
- $b_{m+1}, \ldots, b_{m+r}$ is the corresponding extension $J^{\lambda_1} w_1, \ldots, J^{\lambda_r} w_r$ to a basis for $W + JW$;

- $b_{m+r+1}, \dots, b_n$ is any extension to a basis for $\mathbb{F}_p^n$.

Consider the matrix of J for this basis: the first m columns describe the action on W, and depend solely on λ. Hence the number of (J, λ')-bases giving rise to a subspace of W with partition λ' is independent of J. Moreover, the number of (J, λ')-bases for any such W' depends solely on λ', by Lemma 3.7. ∎

Corollary 3.9 *Let λ be a partition of $m < n$. The number of proper subspaces W of $\mathbb{F}_p^n$ with partition λ is independent of f.*

Proof. The codimension 1 subspaces of $\mathbb{F}_p^n$ all have partition $(n-1)$: so by Lemma 3.8 each contains the same number of such W, and this number is independent of f. ∎

Corollary 3.10 *Fix $0 \leq m_0 < m_1 < \cdots < m_s$ and partitions $\lambda^i \dashv m_i$. The number of flags $W_0 \subset W_1 \subset \cdots \subset W_s$ of proper subspaces of $\mathbb{F}_p^n$ in which W_i has partition λ^i is independent of f.*

Proof. The case $s = 1$ is Corollary 3.9. The general case is by induction on s using Lemma 3.8. ∎

Proof of Proposition 3.5. We must show that for each parabolic subgroup $H \leq G$, the isomorphism class of the V-set structure induced on G/H by ρ_f does not depend on f. Now, two finite V-sets X, Y are isomorphic if and only if for each subgroup U of V, the sets X^U, Y^U have the same cardinality.

The case $U = 1$ is clear. For the cyclic subgroups, observe that since J has no invariant subspaces and therefore no eigenvectors, the matrix $\lambda I + \mu J$ is invertible for all $(\lambda, \mu) \in \mathbb{F}_p^2 \setminus \{0\}$. Therefore by Lemma 3.2, all nontrivial elements of $\mathrm{Im}(\rho_f)$ are conjugate in $GL_{2n}(\mathbb{F}_p)$ to each other, and so the number of fixed cosets is independent of f.

Only the hardest case remains to be proved: that the number of cosets fixed by V itself is independent of f. Recall that the parabolic subgroups in GL_{2n} are the flag stabilizers. Define the type of a flag

$$X_0 \subset X_1 \subset \cdots \subset X_t$$

of subspaces of $\mathbb{F}_p^{2n}$ to be the $(t+1)$-tuple $(\dim(X_0), \dots, \dim(X_t))$. The flags of any given type are permuted transitively by $GL_{2n}(\mathbb{F}_p)$. Our task is to show that the number of V-invariant flags of any given type does not depend on the choice of irreducible polynomial f.

Associated to the block matrices is a splitting of $\mathbb{F}_p^{2n}$ as $\mathbb{F}_p^n \oplus \mathbb{F}_p^n$. Let $i\colon \mathbb{F}_p^n \to \mathbb{F}_p^{2n}$ be inclusion as the first factor, and $j\colon \mathbb{F}_p^{2n} \to \mathbb{F}_p^n$ projection onto the second factor. Let X be an invariant subspace of $\mathbb{F}_p^{2n}$, and set $W = j(X)$, $Z = i^{-1}(X)$. Then

$$\begin{pmatrix} I & I \\ 0 & I \end{pmatrix} \begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} z + w \\ w \end{pmatrix} \qquad \begin{pmatrix} I & J \\ 0 & I \end{pmatrix} \begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} z + Jw \\ w \end{pmatrix}.$$

We deduce that X is invariant if and only if $W + JW \subseteq Z$. In particular, the only invariant subspace with W equal to $\mathbb{F}_p^n$ is $\mathbb{F}_p^{2n}$.

Clearly we may restrict our attention to invariant flags of proper subspaces. Based on Lemma 3.7, we define the *fine type* of an invariant flag $X_0 \subset X_1 \subset \cdots \subset X_t$ of proper subspaces to be $(d_0, \ldots, d_t; \lambda^0, \ldots, \lambda^t)$, where $d_i = \dim(X_i)$, and λ^i is the partition associated to W_i. Of course, the fine type of a flag determines its type. But by Lemma 3.11, the number of flags of a given fine type is independent of f. ∎

Lemma 3.11 *The number of invariant flags $X_0 \subset X_1 \subset \cdots \subset X_t$ of proper subspaces with given fine type $(d_0, \ldots, d_t; \lambda^0, \ldots, \lambda^t)$ does not depend on f.*

Proof. An invariant subspace X determines W, Z and a linear map $\alpha\colon W \to \mathbb{F}_p^n/Z$ defined by $w + \alpha(w) \subseteq X \subseteq \mathbb{F}_p^{2n} = \mathbb{F}_p^n \oplus \mathbb{F}_p^n$. Conversely, any such triple W, Z, α with $W + JW \subseteq Z$ determines an invariant X. For an invariant flag we also require that $W_i \subseteq W_j$ and $Z_i \subseteq Z_j$ for $i < j$; and that $\alpha_i(w) + Z_j = \alpha_j(w)$ for all $w \in W_i$.

By Corollary 3.10, the number of flags $W_0 \subseteq W_1 \subseteq \cdots \subseteq W_t$ with partition type $(\lambda^0, \ldots, \lambda^t)$ is independent of f. The number of flags $Z_0 \subseteq \cdots \subseteq Z_t$ in $\mathbb{F}_p^n$ such that $W_i + JW_i \subseteq Z_i$ and $\dim(Z_i) = d_i - \dim(W_i)$ does not depend on the flag W_i or on f: for the type τ of the flag $W_i + JW_i$ is determined, and all flags of type τ are in the same orbit. Given flags W_i and Z_i, the number of choices for the α_i is independent of f: pick α_1 first, and pick α_{i+1} to be any extension of α_i. ∎

Remark 3.12 Theorem 3.6 can be interpreted in terms of prime ideals. For an elementary abelian p-group $V \leq G$, the classes in $\mathrm{H}^*(G)$ with nilpotent restriction to V constitute a prime ideal $\mathfrak{p}_V$. Let V, W be elementary abelian subgroups of G which are isomorphic in $\mathcal{A}_\pi$ but not conjugate in G. Then $\mathfrak{p}_V \cap S_h$ and $\mathfrak{p}_W \cap S_h$ are distinct prime ideals in S_h, but $\mathfrak{p}_V \cap S_\pi$ and $\mathfrak{p}_W \cap S_\pi$ are the same prime ideal of S_π. In the specific case constructed, V, W have p-rank 2 and lie in an elementary abelian subgroup of rank n^2, the p-rank of G. Hence $\mathfrak{p}_V$ and $\mathfrak{p}_W$ have height $n^2 - 2$.

References

[1] J. L. Alperin, 'A Lie approach to finite groups', *Groups—Canberra 1989* (ed. L. G. Kovács), Lecture Notes in Mathematics 1456 (Springer, Berlin, 1990), pp. 1–9.

[2] L. Evens, *The Cohomology of Groups* (Clarendon Press, Oxford, 1991).

[3] D. J. Green, ‘On the cohomology of the sporadic simple group J_4’, *Math. Proc. Cambridge Philos. Soc.* 113 (1993) 253–266.

[4] D. J. Green and I. J. Leary, ‘The spectrum of the Chern subring’, *Comm. Math. Helv.* 73 (1998) 406–426.

[5] D. Quillen, ‘The spectrum of an equivariant cohomology ring: II’, *Ann. of Math.* 94 (1971) 573–602.

[6] G. B. Segal and C. T. Stretch, ‘Characteristic classes for permutation representations’, *Math. Proc. Cambridge Philos. Soc.* 90 (1981) 265–272.

[7] B. B. Venkov, ‘Cohomology algebras for some classifying spaces’, *Dokl. Akad. Nauk SSSR* 127 (1959) 943–944.

Green & Schuster
Fachbereich 7 Mathematik
Bergische Universität GH Wuppertal
D–42097 Wuppertal
Germany

Leary
Faculty of Mathematical Studies
University of Southampton
Southampton SO17 1BJ
U.K.