J. London Math. Soc. (2) 90 (2014) 879–902
doi:10.1112/jlms/jdu056

Pseudo-reflection groups and essential dimension

Alexander Duncan and Zinovy Reichstein

Abstract

We give a simple formula for the essential dimension of a finite pseudo-reflection group at a prime p and determine the absolute essential dimension for most irreducible pseudo-reflection groups. We also study the 'poor man's essential dimension' of an arbitrary finite group, an intermediate notion between the absolute essential dimension and the essential dimension at a prime p.

1. *Introduction*

Let k be a field and G be a finite group. We begin by recalling the definition of the essential dimension $\mathrm{ed}_k(G)$.

A G-variety is a k-variety X with a G-action. A G-variety X is *primitive* if G acts transitively on the irreducible components of $X_{\bar{k}}$. Here $\bar{k}$ denotes the algebraic closure of k. A *compression* is a dominant G-equivariant k-map $X \dashrightarrow Y$, where X and Y are primitive faithful G-varieties defined over k. The essential dimension of a primitive faithful G-variety X, denoted by $\mathrm{ed}(X)$, is defined as the minimal dimension of Y, where X is fixed, Y varies and the minimum is taken over all compressions $X \dashrightarrow Y$. The essential dimension $\mathrm{ed}_k(G)$ of G is the maximal value of $\mathrm{ed}(X)$ over all primitive faithful G-varieties X defined over k. This maximal value is attained in the case where $X = V$ is a finite-dimensional k-vector space on which G acts via a faithful representation $G \hookrightarrow \mathrm{GL}(V)$. We will denote this numerical invariant of G by $\mathrm{ed}_k(G)$, or simply $\mathrm{ed}(G)$ when the base field k is clear.

The notion of essential dimension has classical origins, even though it was only formalized relatively recently [**3**]. In particular, Klein showed (using different terminology) $\mathrm{ed}_{\mathbb{C}}(S_5) = 2$ in his 1884 book [**21**]. In Galois-theoretic language, $\mathrm{ed}_k(G)$ is the minimal integer $d \geqslant 0$ such that for every field K/k and every G-Galois field extension L/K, one can write $L \simeq K[x]/(f(x))$, where at most d of the coefficients of the polynomial $f(x) \in K[x]$ are algebraically independent over k. This number naturally comes up in the construction of so-called 'generic polynomials' for the group G in inverse Galois theory; see [**16**, Chapter 8]. Essential dimension can also be defined in a broader context as a numerical invariant of more general algebraic objects. In this paper, our focus will be solely on finite groups. For surveys of the broader theory, we refer an interested reader to [**28**, **34**, **35**].

The essential dimension has turned out to be surprisingly difficult to compute for many finite groups. For example, the exact value of $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/n\mathbb{Z})$ is only known for a few small values of n. The relative version of essential dimension at a prime integer p, denoted by $\mathrm{ed}(G;p)$, has proved to be more accessible. If X is a primitive faithful G-variety, then $\mathrm{ed}(X;p)$ is defined as the minimum of $\dim(Y)$ over all primitive faithful G-varieties Y which admit a G-equivariant correspondence $X \rightsquigarrow Y$ of degree prime to p. The essential dimension $\mathrm{ed}(G;p)$ is, once again, defined as the minimal value of $\mathrm{ed}(X;p)$. Recall that a correspondence $X \rightsquigarrow Y$ of degree 1 is the

Received 6 March 2014; revised 20 August 2014; published online 31 October 2014.

2010 *Mathematics Subject Classification* 20F55, 20D15 (primary).

Alexander Duncan was partially supported by National Science Foundation RTG grants DMS 0838697 and DMS 0943832. Zinovy Reichstein was partially supported by National Sciences and Engineering Research Council of Canada Discovery grant 250217-2012.

same thing as a dominant rational map $X \dashrightarrow Y$. Thus $\operatorname{ed}(X;p) \leqslant \operatorname{ed}(X)$ and $\operatorname{ed}(G;p) \leqslant \operatorname{ed}(G)$ for every prime p. The best known lower bound for $\operatorname{ed}(G)$ is usually deduced from this inequality.

The computation of $\operatorname{ed}(G;p)$ is greatly facilitated by a theorem of Karpenko and Merkurjev [**19**], which asserts

$$\operatorname{ed}(G;p) = \operatorname{ed}(G_p) = \operatorname{rdim}(G_p). \tag{1.1}$$

Here G_p is any Sylow p-subgroup of G, and for a finite group H, $\operatorname{rdim}(H)$ denotes the minimal dimension of a faithful representation of H defined over k, and we assume that $\zeta_p \in k$, where ζ_p is a primitive pth root of unity. Note that since $[k(\zeta_p) : k]$ is prime to p, $\operatorname{ed}_k(G;p) = \operatorname{ed}_{k(\zeta_p)}(G;p)$.

The case where $G = S_n$ is the symmetric group is of particular interest because it relates to classical questions in the theory of polynomials; see [**3**, **4**]. Here the relative essential dimension is known exactly for every prime p:

$$\operatorname{ed}(S_n;p) = \left\lfloor \frac{n}{p} \right\rfloor; \tag{1.2}$$

see [**29**, Corollary 4.2]. The absolute essential dimension $\operatorname{ed}(S_n)$ is largely unknown. In characteristic zero, we know only that

$$\max_p \operatorname{ed}(S_n;p) = \left\lfloor \frac{n}{2} \right\rfloor \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor \leqslant \operatorname{ed}(S_n) \leqslant n-3 \tag{1.3}$$

for any $n \geqslant 6$; see [**3**, **11**, **26**]. We know even less about $\operatorname{ed}(S_n)$ in prime characteristic.

The symmetric groups S_n belong to the larger family of pseudo-reflection groups. Pseudo-reflection groups play an important role in representation theory and invariant theory of finite groups; see, for example, [**18**, **24**, **41**]. It is thus natural to try to compute $\operatorname{ed}(G)$ and $\operatorname{ed}(G;p)$, where G is a finite pseudo-reflection group, and p is a prime. The first steps in this direction were taken by MacDonald [**26**, Section 5.1], who computed $\operatorname{ed}(G;p)$ for all primes p and all irreducible Weyl groups G. He also computed $\operatorname{ed}(G)$ for every irreducible Weyl group G except for $G = S_n$ and $G = W(\mathbf{E_6})$, the Weyl group of the root system of type $\mathbf{E_6}$. His proofs are based on case-by-case analysis.

The aim of this paper is twofold. First, we will generalize MacDonald's results to all finite pseudo-reflection groups except the symmetric groups, with a more uniform statement and proof. Second, we will investigate a new intermediate notion between $\max_p \operatorname{ed}(G;p)$ and $\operatorname{ed}(G)$, which we call 'poor man's essential dimension'.

Throughout this paper, we will assume that $\operatorname{char}(k)$ does not divide the order of G. Our finite groups will be viewed as split algebraic groups over k. We will denote by $\bar{k}$ the algebraic closure of k and by ζ_d a primitive dth root of unity in $\bar{k}$ where d is a positive integer coprime to $\operatorname{char}(k)$. By a *variety*, we will mean a separated reduced scheme of finite type over k, not necessarily irreducible. We will also adopt the following notational conventions inspired by Springer [**43**]. Let $\phi\colon G \hookrightarrow \operatorname{GL}(V)$ be a faithful representation of G and m be a positive integer prime to the characteristic of k. Set $V(g,\zeta_m) := \ker(\zeta_m I - \phi(g))$ to be the ζ_m-eigenspace of g and let

$$a_\phi(m) := \max_{g\in G} \dim V(g,\zeta_m).$$

Note that $V(g,\zeta_m)$ is defined over $k(\zeta_m)$ but may not be defined over k. Replacing g by a suitable power, we see that $a_\phi(m)$ depends only on ϕ and m and not on the choice of the primitive mth root of unity ζ_m. If the reference to ϕ is clear from the context, then we will write g in place of $\phi(g)$ and $a(m)$ in place of $a_\phi(m)$. By convention, we set $a(m) = 0$ if m is a multiple of the characteristic of k.

Recall that an element $g \in \operatorname{GL}(V)$ is a *pseudo-reflection* if it is conjugate to a diagonal matrix of the form $\operatorname{diag}(1,\dots,1,\zeta)$, where $\zeta \neq 1$ is a root of unity.

THEOREM 1.1. *Let G be a finite subgroup of* $\mathrm{GL}(V)$. *Assume that the characteristic of the base field k does not divide $|G|$.*

(a) *Then* $\mathrm{ed}(G;p) \leqslant a(p)$ *for every prime p.*
(b) *Moreover, if G is generated by pseudo-reflections, then* $\mathrm{ed}(G;p) = a(p)$ *for every prime p.*

Suppose that $\phi\colon G \hookrightarrow \mathrm{GL}(V)$ is generated by pseudo-reflections with $n = \dim(V)$. Then $k[V]^G = k[f_1, \dots, f_n]$ for some homogeneous polynomials $f_1, \dots, f_n$. Set $d_i := \deg(f_i)$. The integers $d_1, \dots, d_n$ are called the *degrees of the fundamental invariants* of ϕ. These numbers are uniquely determined by ϕ up to reordering. They are independent of the choice of $f_1, \dots, f_n$ and can be recovered directly from the Poincaré series of $k[V]^G$; see, for example, [**18**] or [**24**]. Springer [**43**, Theorem 3.4(i)] showed

$$a(m) = |\{i \mid d_i \text{ is divisible by } m\}|. \tag{1.4}$$

Note that while the base field k is assumed to be the field of complex numbers $\mathbb{C}$ in [**43**, Theorem 3.4(i)], the above formula remains valid under our less restrictive assumptions on k; see, for example, [**18**, Section 33-1].

Complex groups generated by pseudo-reflections have been classified by Shephard and Todd [**41**]. Their classification lists $d_1, \dots, d_n$ in every case; Springer's theorem (1.4) makes it possible to read $a(m)$ directly off their table for every G and every m. The same can be done for other base fields k, as long as $\mathrm{char}(k)$ does not divide $|G|$; for details and further references, see Section 4.

EXAMPLE 1.2. For $G = W(\mathbf{E_8})$ (group number 37 in the Shephard–Todd classification), the values of $d_1, \dots, d_8$ are

$$2,\ 8,\ 12,\ 14,\ 18,\ 20,\ 24,\ 30,$$

respectively; see, for example, [**24**, Appendix D]. Counting how many of these numbers are divisible by each prime p and applying Theorem 1.1(b) in combination with (1.4), we recover the following values from [**26**, Table IV].

p	2	3	5	7	>7
$\mathrm{ed}(W(\mathbf{E_8});p)$	8	4	2	1	0

Our proof of Theorem 1.1 relies on both the uniform arguments in Sections 2 and 3 and some case-by-case analysis using the Shephard–Todd classification in Section 4.

Our next result, Theorem 1.3, gives the exact value for the *absolute* essential dimension of all irreducible pseudo-reflection groups, except for S_n. Recall that in the Shephard–Todd classification there are three infinite families: the symmetric groups, the family $G(m,l,n)$ depending on three integer parameters (m,l,n) and the cyclic groups. In addition, there are 34 exceptional groups.

THEOREM 1.3. *Let $G \subset \mathrm{GL}(V)$ be an irreducible representation of a finite group generated by pseudo-reflections. Suppose that G is not isomorphic to a symmetric group S_n and* $\mathrm{char}(k)$ *does not divide $|G|$. Then the following equalities hold:*

(a) $\mathrm{ed}(G) = \dim(V) - 2 = 4$, *if* $G \simeq W(\mathbf{E_6})$;
(b) $\mathrm{ed}(G) = \dim(V) - 1 = n - 1$, *if* $G \simeq G(m,m,n)$ *with m, n relatively prime*;
(c) $\mathrm{ed}(G) = \dim(V)$ *in all other cases.*

As we mentioned above, the exact value of $\mathrm{ed}(S_n)$ is not known; see (1.3). Theorem 1.3(a) answers an open question posed in [**26**, Remark 5.2]. The proof of this part relies on a geometric construction suggested to us by Dolgachev.

We now recall that $\mathrm{ed}(G)$ is the minimal dimension of a versal G-variety and $\mathrm{ed}(G;p)$ is the minimal dimension of a p-versal G-variety; see [**12**, Remark 2.5; **40**, Section 5]. *Poor man's essential dimension*, denoted by $\mathrm{pmed}(G)$, is defined as the minimal dimension of a G-variety which is simultaneously p-versal for every prime p. We have

$$\max_p \mathrm{ed}(G;p) \leqslant \mathrm{pmed}(G) \leqslant \mathrm{ed}(G). \tag{1.5}$$

The term 'poor man's essential dimension' is meant to suggest that $\mathrm{pmed}(G)$ is a more accessible substitute for $\mathrm{ed}(G)$. Where exactly it fits between $\max_p \mathrm{ed}(G;p)$ and $\mathrm{ed}(G)$, is a key motivating question for this paper.

Theorem 1.4. *Let G be a finite subgroup of $\mathrm{GL}(V)$. Assume that $\mathrm{char}(k)$ does not divide $|G|$.*

(a) *Then* $\mathrm{pmed}(G) \leqslant \max_p a(p)$.
(b) *Moreover, if G is generated by pseudo-reflections, then*

$$\mathrm{pmed}(G) = \max_p a(p) = \max_p \mathrm{ed}(G;p).$$

In both parts, the maximum is taken over all prime integers p.

In particular, $\mathrm{pmed}(S_n) = \lfloor n/2 \rfloor$ for every n, assuming $\mathrm{char}(k) = 0$, a result we found somewhat surprising considering that $\mathrm{ed}(S_n) > \lfloor n/2 \rfloor$ for every odd $n \geqslant 7$; see (1.3).

Our proof of Theorem 1.4 relies on a variant of Bertini's theorem; see Theorem 8.1. If k is an infinite field, then Theorem 8.1 is classical. In the case where k is a finite field, we make use of the probabilistic versions of Bertini's smoothness and irreducibility theorems, due to Poonen [**32**, **33**] and Charles and Poonen [**5**], respectively. Note that [**5**] was motivated, in part, by the application in this paper.

In view of Theorem 1.4(b), it is natural to ask whether

$$\mathrm{pmed}(G) = \max_p \mathrm{ed}(G;p) \tag{1.6}$$

for every finite group G. In addition to the case of pseudo-reflection groups covered by Theorem 1.4(b), we will also prove that this is the case for alternating groups (Example 12.1) and for groups all of whose Sylow subgroups are abelian (Proposition 11.1). A conjectural approach to proving (1.6) for other finite groups is outlined at the end of Section 11.

2. *Proof of Theorem* 1.1(a)

Throughout this section, we fix a prime p and assume that the base field k is of characteristic not equal to p.

Lemma 2.1. *Let V be a finite-dimensional k-vector space, and $G_p \subset \mathrm{GL}(V)$ be a finite p-group. Assume $\zeta_p \in k$ and that V' is a minimal (with respect to inclusion) faithful G_p-subrepresentation of V. Then there exists a central element $g \in G_p$ of order p such that $V' \subset V(g, \zeta_p)$, where ζ_p is a primitive pth root of unity.*

Proof. Let C be the socle of G_p, that is, the p-torsion subgroup of the centre $Z(G_p)$.

Decompose $V' = V_1 \oplus \cdots \oplus V_r$ as a direct sum of irreducible G_p-representations. Each V_i decomposes into a direct sum of character spaces for C. Since C is central, each of these character spaces is G_p-invariant. As V_i is irreducible as a G_p-module, there is only one such character space. That is, C acts on each V_i by scalar multiplication via a character $\chi_i : C \to k^*$.

We will view the characters χ_i as elements of the dual group $C^* = \mathrm{Hom}(C, k^*)$. Note that since C is an elementary abelian p-group, C^* has the natural structure of an $\mathbb{F}_p$-vector space. Since V' is minimal, an easy argument shows that $\chi_1, \ldots, \chi_r$ form an $\mathbb{F}_p$-basis of C^*; see [**30**, Lemma 2.3]. Consequently, there is a unique element $g \in C$ such that $\chi_i(g) = \zeta_p$ for every $i = 1, \ldots, r$. In other words, $V' \subset V(g, \zeta_p)$, as desired. □

Proof of Theorem 1.1(a). Neither $\mathrm{ed}(G; p)$ nor $a(p)$ will change if we replace k by $k(\zeta_p)$. Hence, we may assume without loss of generality that k contains ζ_p. Let G_p be a Sylow p-subgroup of G and define V' and g as in Lemma 2.1. Then $V' \subset V(g, \zeta_p)$. Thus

$$\mathrm{ed}(G;p) = \mathrm{ed}(G_p;p) \leqslant \mathrm{ed}(G_p) \leqslant \dim(V') \leqslant \dim V(g,\zeta_p) \leqslant a(p),$$

as desired. Note that the inequality $\mathrm{ed}(G_p) \leqslant \dim(V')$ is a consequence of the definition of essential dimension; see, for example, [**34**, (2.3)]. □

We conclude this section with a refinement of Lemma 2.1 which will be used in the proofs of both Theorem 1.1(b) and Corollary 5.1.

LEMMA 2.2. *Let V be a finite-dimensional k-vector space, $G \subset \mathrm{GL}(V)$ be a finite group generated by pseudo-reflections and G_p be a p-Sylow subgroup of G. Assume $\zeta_p \in k$ and that V', g are as in the statement of Lemma* 2.1. *Then $\dim V(g, \zeta_p) = a(p)$.*

Proof. By Springer [**43**, Theorem 3.4(ii)], there exists an $h \in G$ such that $\dim V(h, \zeta_p) = a(p)$ and $V(g, \zeta_p) \subset V(h, \zeta_p)$. Springer originally proved this result over $\mathbb{C}$; a proof over an arbitrary base field (containing ζ_p) can be found in [**18**, Chapter 33]. Recall that by Lemma 2.1, $V' \subset V(g, \zeta_p)$.

After replacing h by a suitable power, we may assume that the order of h is a power of p. Let $N = \{x \in G \mid x(V') = V'\}$ be the stabilizer of V' in G. Note that $G_p \subset N$ and thus G_p is a p-Sylow subgroup of N. Since $V' \subset V(h, \zeta_p)$, we clearly have $h \in N$. On the other hand, since the order of h is a power of p, there exists an element $n \in N$ such that $h' = nhn^{-1}$ is in G_p. Note that h acts on V' as $\zeta_p \,\mathrm{id}_{V'}$, and hence, so does h'. Now, h' and g both lie in G_p and have identical actions on V', which is a faithful representation of G_p. Thus $h' = g$, and $a(p) = \dim V(h, \zeta_p) = \dim V(h', \zeta_p) = \dim V(g, \zeta_p)$, as desired. □

3. *Proof of Theorem* 1.1(b): *first reductions*

We now turn to the proof of Theorem 1.1(b). In view of part (a), it suffices to show $\mathrm{ed}(G; p) \geqslant a(p)$. Since $\mathrm{ed}_k(G; p) \geqslant \mathrm{ed}_l(G; p)$, for any field extension l/k, we may assume without loss of generality that k is algebraically closed, and, in particular, $\zeta_p \in k$.

Our proof of Theorem 1.1(b) will proceed by contradiction. We begin by studying a minimal counterexample, with the ultimate goal of showing that it cannot exist.

PROPOSITION 3.1. *Let $\phi \colon G \hookrightarrow \mathrm{GL}(V)$ be a counterexample to Theorem* 1.1(b) *of minimal dimension. That is, V is a vector space of minimal dimension with the following properties: there exists a finite group G, a faithful representation $\phi \colon G \hookrightarrow \mathrm{GL}(V)$ and a prime p, such that*

$\phi(G)$ is generated by pseudo-reflections, and

$$\mathrm{ed}(G;p) < a_\phi(p). \tag{3.1}$$

(a) *Then* $\dim(V) \geqslant 2$.
(b) *The representation ϕ is irreducible.*
(c) *Some element $g \in G$ of order p acts on V as a scalar. In particular, $a_\phi(p) = \dim(V)$.*
(d) *The group G contains no elements of order p with exactly two eigenvalues.*
(e) *The group G contains no pseudo-reflections of order p.*
(f) *If $p = 2$, then $g = -\mathrm{id}_V$ is the unique element of order 2 in G.*
(g) *Let G_p be a Sylow p-subgroup of G. Then G_p is contained in the commutator subgroup $[G,G]$.*
(h) *Let $g \in G$ be as in part* (c) *and $\phi' \colon G \to \mathrm{GL}(V')$ be an irreducible representation such that $\phi'(g) \neq 1$. Then $\dim(V')$ is a multiple of p. In particular, $\dim(V)$ is a multiple of p.*
(i) *Moreover,* $\dim(V) \geqslant 2p$.

Proof. (a) Assume the contrary: $\dim(V) = 1$. In this case, G is a cyclic group. If $|G|$ is divisible by p, then $\mathrm{ed}(G;p) = a(p) = 1$; otherwise $\mathrm{ed}(G;p) = a(p) = 0$. In both cases, (3.1) fails, a contradiction.

(b) Assume the contrary: $V = V_1 \oplus V_2$, where V_1 and V_2 are proper G-stable subspaces. Each pseudo-reflection $g \in G$ acts non-trivially on exactly one summand V_i. For $i = 1, 2$, let G_i be the subgroup of G generated by those reflections that act non-trivially on V_i. Then G is isomorphic to the direct product $G_1 \times G_2$, and $\phi = \phi_1 \oplus \phi_2$, where ϕ restricts to $\phi_i \colon G_i \to \mathrm{GL}(V_i)$, and $\phi_1(G_1)$, $\phi_2(G_2)$ are generated by pseudo-reflections. Note $a_\phi(p) = a_{\phi_1}(p) + a_{\phi_2}(p)$. In addition, by Karpenko and Merkurjev [**19**, Theorem 5.1],

$$\mathrm{ed}(G;p) = \mathrm{ed}(G_1;p) + \mathrm{ed}(G_2;p).$$

By minimality of ϕ, we have $\mathrm{ed}(G_1;p) \geqslant a_{\phi_1}(p)$ and $\mathrm{ed}(G_2;p) \geqslant a_{\phi_2}(p)$. Thus $\mathrm{ed}(G;p) \geqslant a_\phi(p)$, a contradiction.

(c) Choose V' and g as in Lemmas 2.1 and 2.2. Recall that g is a central element of G_p of order p and $a_\phi(p) = \dim V(g, \zeta_p)$. Set $W := V(g, \zeta_p)$. The element g acts on W as a scalar; our goal is to show $W = V$.

Let $S = \{s \in G \mid s(W) = W\}$ be the stabilizer of W in G and let S_0 be the subgroup of S consisting of elements that fix W pointwise. Note that since g is central in G_p, we have $G_p \subset S$. Moreover, since G_p acts faithfully on $V' \subset W$, we have $G_p \cap S_0 = \{1\}$. Restricting the action of S to W, we obtain a faithful representation of $H = S/S_0$ on W, which we will denote by ψ. By Lehrer and Michel [**23**, Theorem 1.1], $\psi(H) \subset \mathrm{GL}(W)$ is generated by pseudo-reflections. (Note that while [**23**, Theorem 1.1] assumes $k = \mathbb{C}$, its proof goes through under our less restrictive assumptions on k.) By our construction,

$$a_\phi(p) = \dim(W) = a_\psi(p).$$

Since $G_p \subset S$ and $G_p \cap S_0 = \{1\}$, the quotient $H = S/S_0$ contains an isomorphic image of G_p, which is a Sylow p-subgroup of H, so that

$$\mathrm{ed}(G;p) = \mathrm{ed}(G_p;p) = \mathrm{ed}(H;p).$$

Thus by (3.1), $\mathrm{ed}(H;p) = \mathrm{ed}(G;p) < a_\phi(p) = a_\psi(p)$. By the minimality of ϕ, we see that $\dim(V) = \dim(W)$, that is, $V = W = V(g, \zeta_p)$. This proves part (c).

(d) Assume the contrary: an element h of G of order p has exactly two distinct eigenvalues, ζ_p^i and ζ_p^j. After replacing h by a suitable power of hg^{-i}, where g is the central element we constructed in part (c), we may assume $i = 0$ and $j = 1$. Then V is the direct sum of eigenspaces

$V_0 \oplus V_1$, where $V_i = V(h, \zeta_p^i)$. Let G_1 (respectively, G_0) be the subgroup of G consisting of elements which fix V_0 (respectively, V_1) pointwise (note the reversed indices).

Since G has order prime to the characteristic of k, the direct sum $V_0 \oplus V_1$ is the unique decomposition of V into isotypic components for the group $\langle g, h\rangle$. Since $gh^{-1} \in G_0$ acts non-trivially on V_0, the space V_0 is the unique G_0-invariant complement to $V_1 = V^{G_0}$. Similarly, V_1 is the unique G_1-invariant complement to $V_0 = V^{G_1}$. We now see that G_0 and G_1 commute and $G_0 \cap G_1 = \{1\}$. Hence, G_0 and G_1 generate a subgroup of G isomorphic to $G_0 \times G_1$. By abuse of notation, we shall denote this group by $G_0 \times G_1$.

Note that ϕ restricts to faithful representations $\phi_0\colon G_0 \to \mathrm{GL}(V_0)$ and $\phi_1\colon G_1 \to \mathrm{GL}(V_1)$. Since $\phi_0(gh^{-1}) = \zeta_p \,\mathrm{id}_{V_0}$ and $\phi_1(h) = \zeta_p \,\mathrm{id}_{V_1}$, we have

$$a_{\phi_0}(p) = \dim(V_0) \quad \text{and} \quad a_{\phi_1}(p) = \dim(V_1).$$

We now recall that by a theorem of Steinberg [**44**, Theorem 1.5], G_0 and $G_1 \subset \mathrm{GL}(V)$ are both generated by pseudo-reflections. (In positive characteristic, this is due to Serre [**38**]; cf. [**7**, Proposition 3.7.8].) Since G_1 acts trivially on V_0 and G_0 acts trivially on V_1, we conclude that $\phi_0(G_0)$ and $\phi_1(G_1)$ are also generated by pseudo-reflections.

By the minimality of ϕ, Theorem 1.1(b) holds for ϕ_0 and ϕ_1. Thus

$$\begin{aligned}\mathrm{ed}(G;p) &\geqslant \mathrm{ed}(G_0 \times G_1;p) = \mathrm{ed}(G_0;p) + \mathrm{ed}(G_1;p)\\ &= a_{\phi_0}(p) + a_{\phi_1}(p) = \dim(V_0) + \dim(V_1) = \dim(V) = a_\phi(p).\end{aligned}$$

Here the first equality is [**19**, Theorem 5.1], and the second follows from the minimality of ϕ. The resulting inequality contradicts (3.1).

(e) By part (a), $\dim(V) \geqslant 2$. Hence, a pseudo-reflection has exactly two distinct eigenvalues, and (e) follows from (d).

(f) Every element of $\mathrm{GL}(V)$ of order 2, other than $-\mathrm{id}_V$, has exactly two distinct eigenvalues and thus cannot lie in G by (d).

(g) By (e), G does not have any pseudo-reflections of order p, and hence of any order divisible by p. The finite abelian group $G/[G,G]$ is generated by the images of the pseudo-reflections. All of these images have order prime to p. Hence, the order of $G/[G,G]$ is prime to p. We conclude that $G_p \subset [G,G]$.

(h) Since g is central, $\phi'(g) = \lambda\,\mathrm{id}_{V'}$, where λ is a primitive pth root of unity. Thus $\det \phi'(g) = \lambda^{\dim(V')}$. On the other hand, by part (g), $g \in G_p \subset [G,G]$ and hence, $\det\phi'(g) = 1$. Thus $\dim(V')$ is divisible by p.

(i) Let $C = \langle g\rangle$, where g is as in part (c). Applying [**34**, Theorem 4.1] (with $r = 1$) to the central exact sequence $1 \to C \to G \to G/C \to 1$, we obtain the inequality

$$\mathrm{ed}(G;p) \geqslant \gcd_{\phi'} \dim(\phi'), \tag{3.2}$$

where $\phi'\colon G \to \mathrm{GL}(V')$ runs over all irreducible representations of G such that the restriction of ϕ' to C is non-trivial, or equivalently, $\phi'(g) \neq 1$. Note that the statement of [**34**, Theorem 4.1] only gives this inequality for $\mathrm{ed}(G)$. However, it remains valid for $\mathrm{ed}(G;p)$; see [**34**, Section 5] or the proof of [**25**, Theorem 3.1].

By part (h), $\dim(\phi')$ is divisible by p for every such ϕ'. Thus $\mathrm{ed}(G;p) \geqslant p$. Assumption (3.1) now tells us that $a_\phi(p) > p$. By part (c), $a_\phi(p) = \dim(V)$. Hence, $\dim(V) > p$. Applying part (h) once again, we see that $\dim(V)$ is divisible by p. Thus $\dim(V) \geqslant 2p$, as claimed. □

4. *Conclusion of the proof of Theorem* 1.1(b)

The remainder of the proof of Theorem 1.1(b) relies on the classification of irreducible pseudo-reflection groups due to Shephard and Todd [**41**]. Their classification consists of 3 infinite families and 34 exceptional groups. The first family contains the natural $(n-1)$-dimensional representations of the group S_n. The second family consists of certain semidirect products of an abelian group and a symmetric group. The third family is simply the one-dimensional representations of cyclic groups. The representations of the exceptional groups range from dimension 2 to 8. We will denote the infinite families by ST_1, ST_2 and ST_3, and the exceptional groups ST_4 to ST_{37}, following the numbering in [**41**].

Shephard and Todd worked over the field $k = \mathbb{C}$ of complex numbers. We are working over a base field k such that $\mathrm{char}(k)$ does not divide $|G|$. As we explained at the beginning of the previous section, we may (and will) assume that k is algebraically closed. Before we proceed with the proof of Theorem 1.1(b), we would like to explain how the Shephard–Todd classification applies in this more general situation.

If k is an algebraically closed field of characteristic zero, then any representation of a finite group over k descends to $\bar{\mathbb{Q}} \subset k$; see [**39**, Section 12.3]. Hence, this representation is defined over $\mathbb{C}$, and the entire Shephard–Todd classification remains valid over k.

Now suppose that k is an algebraically closed field of positive characteristic. Let $A = W(k)$ be its Witt ring. Recall that A is a complete discrete valuation ring of characteristic zero, whose residue field is k. Denote the fraction field of A by K and the maximal ideal by M. It is well known that if $\mathrm{char}(k)$ does not divide $|G|$ (which is our standing assumption), then every n-dimensional $k[G]$-module V lifts to a unique $A[G]$-module V_A, which is free of rank n over A.

It is shown in [**39**, Section 15.5] that the lifting operation $V \mapsto V_K := V_A \otimes K$ and the 'reduction mod M' operation $V_K \mapsto V$ give rise to mutually inverse bijections between the representation rings $R_k(G)$ and $R_K(G)$ of G. These bijections send irreducible k-representations to irreducible K-representations of the same dimension, and they are functorial in both V and G. In particular, if $g \in G$ and $\zeta_d \in k$ is a primitive dth root of unity, then the eigenspace $V(g, \zeta_d)$, viewed as a representation of the cyclic subgroup $\langle g \rangle \subset G$, lifts to $V_K(g, \eta_d)$ for some primitive dth root of unity $\eta_d \in A$ such that

$$\zeta_d = \eta_d \pmod{M}. \tag{4.1}$$

Taking $d = 1$, we see that $g \in G$ acts on V as a pseudo-reflection if and only if it acts on V_K as a pseudo-reflection.

This shows that for every pseudo-reflection group $\phi\colon G \hookrightarrow \mathrm{GL}(V)$ over k there is an abstractly isomorphic pseudo-reflection group $\phi_K\colon G \hookrightarrow \mathrm{GL}(V_K)$ over K. For each $g \in G$, the eigenvalues of $\phi(g)$ and $\phi_K(g)$ are the same, modulo M, in the sense that if η_d is an eigenvalue of $\phi_K(g)$, then ζ_d is an eigenvalue of $\phi(g)$, as in (4.1). Thus $\dim_k V(g, \zeta_d) = \dim_K V(g, \eta_d)$ and consequently,

$$a_\phi(d) = \max_{g \in G} \dim_k V(g, \zeta_d) = \max_{g \in G} \dim_K V_K(g, \eta_d) = a_{\phi_K}(d)$$

for every $d \geqslant 1$. Note also that the degrees of the fundamental invariants are the same since they can be recovered from the numbers $a(d)$, as d varies; see (1.4).

We conclude that if k is an algebraically closed field satisfying the above assumptions, then many properties of irreducible pseudo-reflection groups, whose orders are prime to $\mathrm{char}(k)$, are the same over k as they are over $\mathbb{C}$: their isomorphism types, the numbers $a(d)$ for each $d \geqslant 1$, the numbers of pseudo-reflections of each order, the number of central elements of each order and the degrees of the fundamental invariants. This allows us to use the Shephard–Todd classification (for example, from [**24**, Appendix D], where k is assumed to be $\mathbb{C}$) in our setting; cf. [**18**, Section 15.3].

We now proceed with the proof of Theorem 1.1(b). Let $\phi\colon G \hookrightarrow \mathrm{GL}(V)$ be a minimal counterexample, as in the statement of Proposition 3.1. Then by Proposition 3.1(b), ϕ is irreducible.

The infinite families ST_1–ST_3. *Case* ST_1. Here V is the natural $(n-1)$-dimensional representation of $G := S_n$. For $n \geqslant 3$, G has trivial centre and hence, cannot be minimal by Proposition 3.1(c). For $n = 2$, $\dim(V) = 1$, contradicting Proposition 3.1(a).

Case ST_2. Here $G = G(m, l, n) \subset \mathrm{GL}_n$, where $m, n > 1$, l divides m and $(m, l, n) \neq (2, 2, 2)$. Here $G(m, l, n)$ is defined as a semidirect product of the diagonal subgroup

$$A(m, l, n) = \{\mathrm{diag}(\zeta_m^{a_1}, \ldots, \zeta_m^{a_n}) \,|\, a_1 + \cdots + a_n \equiv 0 \pmod{l}\} \subset \mathrm{GL}_n$$

and the symmetric group S_n, whose elements are viewed as permutation matrices in GL_n; see [**24**, Chapter 2]. (Note that [**24**] assumes $k = \mathbb{C}$, but the same construction works in our more general context.) By Proposition 3.1(c), $G(m, l, n)$ contains the scalar matrix ζ_p id. This matrix has to be contained in $A(m, l, n)$; hence, p divides m. Moreover by Proposition 3.1(i), we may assume $n \geqslant 2p$. Consider $g = \mathrm{diag}(\zeta_m^{m/p}, \ldots, \zeta_m^{m/p}, 1, \ldots, 1) \in A(m, l, n) \subset G(m, l, n)$, where $\zeta_m^{m/p}$ occurs p times. This element has order p and exactly two eigenvalues, contradicting Proposition 3.1(d).

Case ST_3. Here G is cyclic and V is one-dimensional. Once again, this contradicts Proposition 3.1(a).

The exceptional cases ST_4–ST_{37}. All of the exceptional cases satisfy $\dim(V) \leqslant 8$. On the other hand, by Proposition 3.1(h), $\dim(V) = mp$, for some integer m. Moreover, by Proposition 3.1(i), $m \geqslant 2$.

We conclude that either:

(I) $p = 2$ and $\dim(V) \in \{4, 6, 8\}$; or
(II) $p = 3$ and $\dim(V) = 6$.

Case I. We need to consider the groups ST_{28}–ST_{32}, ST_{34}, ST_{35} and ST_{37}, with $p = 2$. With the exception of ST_{32}, each of these groups has a reflection of order 2 and thus is ruled out by Proposition 3.1(e). The group ST_{32} is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathrm{Sp}_4(\mathbb{F}_3)$ (see [**24**, Theorem 8.43]). The group $\mathrm{Sp}_4(\mathbb{F}_3)$ has non-central elements of order 2, contradicting Proposition 3.1(f).

Case II. Here $p = 3$ and we need to consider only two groups: ST_{34} and ST_{35}. The group ST_{35} has trivial centre and thus is ruled out by Proposition 3.1(c). (Recall that the order of the centre is the greatest common divisor of the degrees $d_1, \ldots, d_6$. For $\mathrm{ST}_{35} = W(\mathbf{E_6})$ these are 2, 5, 6, 8, 9 and 12.) This leaves us with $G = \mathrm{ST}_{34}$, otherwise known as the Mitchell group. The structure of this group was investigated by Conway and Sloane. In [**6**, Section 2], they constructed four isomorphic lattices $\Lambda^{(i)}$, where $i = 2, 3, 4$ and 7, whose automorphism group is ST_{34}. In [**6**, Subsection 2.3], they showed that $\mathrm{ST}_{34} \simeq \mathrm{Aut}(\Lambda^{(3)})$ contains the group $(2 \times 3^5) \rtimes S_6$, which, in turn, contains a 3-group $H \simeq (3^2 \rtimes \langle(123)\rangle) \times (3^2 \rtimes \langle(456)\rangle) \simeq P \times P$, where P is a non-abelian group of order 27. By Meyer and Reichstein [**30**, Theorem 1.3] (or, alternatively, by Meyer and Reichstein [**30**, Theorem 1.4(b)]), $\mathrm{ed}(P) = 3$. On the other hand, by Karpenko and Merkurjev [**19**, Theorem 4.1], $\mathrm{ed}(H; 3) = \mathrm{ed}(H)$, and by Karpenko and Merkurjev [**19**, Theorem 5.1], $\mathrm{ed}(H) = \mathrm{ed}(P \times P) = \mathrm{ed}(P) + \mathrm{ed}(P) = 6$. Since we are assuming that ST_{34}, with its natural six-dimensional representation, is a counterexample to Theorem 1.1(b), we obtain

$$6 = \mathrm{ed}(H) = \mathrm{ed}(H; 3) \leqslant \mathrm{ed}(\mathrm{ST}_{34}; 3) < a(3) = 6.$$

This contradiction completes the proof of Theorem 1.1(b).

5. *A representation-theoretic corollary*

Before proceeding further, we record a representation-theoretic corollary of our proof of Theorem 1.1(b), which, to the best of our knowledge, has not been previously noticed. Recall that $\mathrm{rdim}(H)$ denotes the minimal dimension of a faithful representation of a finite group H over the base field k.

Corollary 5.1. *Suppose $\zeta_p \in k$. Let $G \subset \mathrm{GL}(V)$ be a finite subgroup generated by pseudo-reflections, G_p be a p-Sylow subgroup of G, and $V' \subset V$ be a minimal (with respect to inclusion) faithful k-subrepresentation of G_p. Then $\dim(V') = \mathrm{rdim}(G_p)$.*

Proof. Since $\zeta_p \in k$, $\mathrm{rdim}(G_p) = \mathrm{ed}(G;p)$ by the Karpenko–Merkurjev theorem (1.1). Choose g as in Lemma 2.1. Then, by Lemma 2.2,

$$\mathrm{ed}(G;p) = \mathrm{rdim}(G_p) \leqslant \dim(V') \leqslant \dim V(g,\zeta_p) = a(p).$$

By Theorem 1.1(b), $\mathrm{ed}(G;p) = a(p)$ and thus the above inequalities are all equalities. This completes the proof of Corollary 5.1. □

The following example shows that Corollary 5.1 fails if $G \subset \mathrm{GL}(V)$ is not assumed to be generated by pseudo-reflections.

Example 5.2. Let $p > 2$ be a prime, P be a non-abelian group of order p^3 and $\psi\colon P \hookrightarrow \mathrm{GL}(U)$ be a faithful p-dimensional representation of P. Set $G = P \times P$ and

$$\phi = \psi_1 \otimes \psi_2 \oplus \psi_1 \colon G \longrightarrow \mathrm{GL}(U \otimes U \oplus U),$$

where for $i = 1, 2$, ψ_i is the composition of ψ with the projection $G \to P$ to the ith factor. Both $\psi_1 \otimes \psi_2$ and ψ_1 are irreducible representations of G; the irreducibility of $\psi_1 \otimes \psi_2$ follows from [**39**, Theorem 3.2.10(i)]. These irreducible representations are distinct, because $\dim(\psi_1 \otimes \psi_2) = p^2$ and $\dim(\psi_1) = p$.

Note that $G = G_p$ is a group of order p^6, and $V = U \otimes U \oplus U$ is a faithful representation of G. Since it is a direct sum of two distinct irreducibles, neither of which is faithful, the only faithful G_p-subrepresentation V' of V is V itself. On the other hand, G has a $2p$-dimensional faithful representation $\psi_1 \oplus \psi_2$; hence, $\mathrm{rdim}(G) \leqslant 2p$. In summary, $G = G_p$, $V = V'$ and $\dim(V') = p^2 + p > 2p \geqslant \mathrm{rdim}(G_p)$. Thus the assertion of Corollary 5.1 fails for $\phi(G) \subset \mathrm{GL}(V)$.

6. *Proof of Theorem* 1.3(a)

The degrees of the fundamental invariants of $W(\mathbf{E_6})$ are $2, 5, 6, 8, 9$ and 12; see, for example, [**24**, p. 275]. Thus by Theorem 1.1(b), $\mathrm{ed}(W(\mathbf{E_6}); 2) = 4$. This shows $\mathrm{ed}(W(\mathbf{E_6})) \geqslant 4$.

Recall that $\mathrm{ed}(W(\mathbf{E_6}))$ is the minimal value of $\dim(Y)$ such that there exists a dominant rational $W(\mathbf{E_6})$-equivariant map $V \dashrightarrow Y$ defined over k, where V is a linear representation of $W(\mathbf{E_6})$, and Y is a k-variety with a faithful action of $W(\mathbf{E_6})$; see, for example, [**34**, Section 2]. To prove the opposite inequality, $\mathrm{ed}(W(\mathbf{E_6})) \leqslant 4$, it thus suffices to establish the following lemma suggested to us by Dolgachev.

Lemma 6.1. *Let k be a field of characteristic not equal to $2, 3$. There exists a dominant $W(\mathbf{E_6})$-equivariant map*

$$f\colon \mathbb{A}^6 \dashrightarrow Y,$$

defined over k, where $\mathbb{A}^6$ is a linear representation of $W(\mathbf{E_6})$ and Y is a four-dimensional variety with a faithful action of $W(\mathbf{E_6})$.

Proof. First, we construct Y. Consider the space $(\mathbb{P}^2)^6$ of ordered 6-tuples of points in the projective plane. Let $U \subset (\mathbb{P}^2)^6$ be the dense open subset consisting of 6-tuples $(a_1, \ldots, a_6)$ such that no two points a_i lie on the same line, and no six lie on the same conic. This open subset is invariant under the natural (diagonal) PGL_3-action on $(\mathbb{P}^2)^6$. Moreover, U is contained in the stable locus of $(\mathbb{P}^2)^6$ for this action; see, for example, [**10**, p. 116]. Thus there exists a geometric quotient $q\colon U \to Y := U/\mathrm{PGL}_3$. The explicit description in [**10**, Example I.3] shows that Y and q are defined over k. Note that

$$\dim(Y) = \dim(U) - \dim(\mathrm{PGL}_3) = \dim(\mathbb{P}^2)^6 - \dim(\mathrm{PGL}_3) = 12 - 8 = 4,$$

as desired.

We will now construct the affine space $\mathbb{A}^6$ and its map to Y. Let x, y, z be projective coordinates on $\mathbb{P}^2$ and $C \subset \mathbb{P}^2$ be the cubic $yz^2 = x^3$. Note that C has a cusp at $(0 : 1 : 0)$. The smooth locus $C_{\mathrm{sm}} = C \setminus \{(0 : 1 : 0)\}$ is an algebraic group isomorphic to the additive group $\mathbb{G}_a$. Indeed, we identify $\mathbb{G}_a \simeq \mathbb{A}^1$ with C_{sm} via $t \mapsto (t : t^3 : 1)$. Thus the space C_{sm}^6 is isomorphic to the affine space $\mathbb{A}^6$ over k.

This yields an embedding

$$\phi\colon C_{\mathrm{sm}}^6 \hookrightarrow C^6 \hookrightarrow (\mathbb{P}^2)^6.$$

Three points $t_1, t_2, t_3 \in C_{\mathrm{sm}}$ lie on a line if and only if $t_1 + t_2 + t_3 = 0$; six points $t_1, \ldots, t_6 \in C_{\mathrm{sm}}$ lie on a conic if and only if $t_1 + \cdots + t_6 = 0$. Thus for general $(t_1, \ldots, t_6) \in C_{\mathrm{sm}}^6$, we have $\phi(t_1, \ldots, t_6) \in U$. In other words, we may view ϕ as a rational map $C_{\mathrm{sm}}^6 \dashrightarrow U$. We now define the map $f\colon C_{\mathrm{sm}}^6 \dashrightarrow Y$ as the composition

$$f\colon C_{\mathrm{sm}}^6 \overset{\phi}{\dashrightarrow} U \xrightarrow{q} Y.$$

By Shioda [**42**, Lemma 13], over the algebraic closure of k, if $(t_1, \ldots, t_6)$ is a 6-tuple of points in general position in $\mathbb{P}^2$, then there is a cuspidal cubic $C' \subset \mathbb{P}^2$ such that $t_1, \ldots, t_6$ lie in the smooth locus of C'. Since any two cuspidal cubics in $\mathbb{P}^2$ are projectively equivalent (recall our assumptions on the characteristic), we conclude that f is dominant.

It remains to construct actions of $W(\mathbf{E_6})$ on $\mathbb{A}^6$ and Y, and to show that f is equivariant. Recall that blowing up six points in $\mathbb{P}^2$ produces a cubic surface X with the six exceptional divisors of the blow-up corresponding to a ‘sixer’: six pairwise disjoint lines in X. Conversely, any sixer can be blown down to produce six points on $\mathbb{P}^2$. Over an algebraically closed field, the elements of $W(\mathbf{E_6})$ act freely and transitively on the set of sixers in X (where we keep track of the ordering of the six lines). This produces a faithful action of $W(\mathbf{E_6})$ on Y which is defined over k. This action of the Weyl group $W(\mathbf{E_6})$ on Y is sometimes called the *Cremona representation* or the *Coble representation*. For more details, see [**8**, Section 7; **9**, Section 6; **10**, Chapter 6].

We recall how $W(\mathbf{E_6})$ acts on the Picard group N of a smooth cubic surface $X \subset \mathbb{P}^3$ over an algebraically closed field; see, for example, [**8**, Sections 4 and 5] or [**27**, Section 26]. The Picard group $N \simeq \mathbb{Z}^7$ with its intersection form is a lattice with a symmetric bilinear form given by $\mathrm{diag}(1, -1, \ldots, -1)$ with respect to the basis $e_0, \ldots, e_6$, where e_0 is the hyperplane section of X and $e_1, \ldots, e_6$ is a collection of six mutually disjoint lines on X.

Consider a set of fundamental roots in N given by

$$\alpha_1 = e_0 - e_1 - e_2 - e_3, \quad \alpha_2 = e_2 - e_1, \quad \ldots, \quad \alpha_6 = e_6 - e_5.$$

The reflections associated to these roots generate a group isomorphic to $W(\mathbf{E_6})$. (Note that $\alpha_1, \ldots, \alpha_6$ are the same as the fundamental roots used by Dolgachev in [**8**], up to reordering, and as the fundamental roots used by Manin in [**27**], up to sign; see [**27**, Proof of Proposition 25.2].) The reflections associated to $\alpha_2, \ldots, \alpha_6$ generate a subgroup isomorphic to S_6 which permutes the basis elements $e_1, \ldots, e_6$. The symmetric group S_6 naturally acts on C_{sm}^6 and $(\mathbb{P}^2)^6$ by permutations; thus f is S_6-equivariant. It remains to consider the reflection $g \in W(\mathbf{E_6})$ associated to the root α_1.

First, we identify the action of g on Y. Suppose that $\pi : X \to \mathbb{P}^2$ is the blow-up of six points $a_1, \ldots, a_6$. Identifying each e_i with the class of each exceptional divisor $E_i := \pi^{-1}(a_i) \subset X$ we can describe the action of g as follows. For triples of distinct integers i, j, k taken from $\{1, 2, 3\}$, the line E_i is taken to the strict transform of the line between a_j and a_k, while E_4, E_5, E_6 are all left fixed. Recall that the standard quadratic transform $s : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ at the points a_1, a_2, a_3 is the map obtained by blowing up these points and then blowing down the strict transforms of the lines between them. In this language, $g : Y \to Y$ is given by

$$[a_1, \ldots, a_6] \mapsto [s(a'_1), s(a'_2), s(a'_3), s(a_4), s(a_5), s(a_6)],$$

where a'_1 is any point on the line between a_2 and a_3 (and similarly for a'_2 and a'_3).

We now construct an action of g on C^6_{sm} following Pinkham [**31**]. If $C \subset \mathbb{P}^2$ is a cuspidal cubic, then, for any three points u_1, u_2 and u_3 in the smooth locus C_{sm} of C, $C' = s(C)$ is also a cuspidal cubic in $\mathbb{P}^2$. Since any two cuspidal cubics in $\mathbb{P}^2$ are linear translates of each other, there exists an $l \in \mathrm{PGL}_3$ such that $l(C') = C$. Composing s with l, one obtains a rational map $l \cdot s : C_{\mathrm{sm}} \dashrightarrow C_{\mathrm{sm}}$ which is regular on $C_{\mathrm{sm}} \setminus \{u_1, u_2, u_3\}$. Let u'_1 be the unique third intersection point of C with the line passing through u_2 and u_3 (and similarly for u'_2 and u'_3). We define a map $g : C^6_{\mathrm{sm}} \to C^6_{\mathrm{sm}}$ via

$$(u_1, \ldots, u_6) \to (l \cdot s(u'_1), l \cdot s(u'_2), l \cdot s(u'_3), l \cdot s(u_4), l \cdot s(u_5), l \cdot s(u_6)).$$

By construction, we see that f is g-equivariant.

Note that the choice of l and thus of the map $l \cdot s : C_{\mathrm{sm}} \dashrightarrow C_{\mathrm{sm}}$ above is not unique. Pinkham's observation [**31**, pp. 196–197] is that there is a choice of l such that the resulting map g gives rise to a linear representation of $W(\mathbf{E_6}) = \langle g, S_6 \rangle$ on $C^6_{\mathrm{sm}} \simeq \mathbb{A}^6$. In fact, C^6_{sm} can be identified with a Cartan subalgebra of the Lie algebra of type $\mathbf{E_6}$ with the standard action of the Weyl group. This construction is valid over any field k of characteristic not equal to $2, 3$. This completes the proof of Lemma 6.1 and thus of Theorem 1.3(a). $\square$

7. *Proof of Theorem* 1.3(b) *and* (c)

As we have previously pointed out, $\mathrm{ed}(G) \leqslant \dim(V)$; see, for example, [**34**, (2.3)]. In the case where $G = G(m, m, n)$ and $m \geqslant 2$ and (m, n) are relatively prime, no element of G acts as a scalar on V. The natural G-equivariant dominant rational map $V \dashrightarrow \mathbb{P}(V)$ tells us that $\mathrm{ed}(G) \leqslant \dim(V) - 1$.

It now suffices to show that for every irreducible $G \subset \mathrm{GL}(V)$ generated by pseudo-reflections there exists a prime p such that

$$a(p) = \begin{cases} \dim(V) - 1 & \text{if } G \simeq G(m, m, n) \text{ with } m,\ n \text{ relatively prime,} \\ \dim(V) & \text{otherwise.} \end{cases}$$

Indeed, Theorem 1.1(b) will then tell us that $\mathrm{ed}(G) \geqslant \mathrm{ed}(G; p) \geqslant a(p) \geqslant \dim(V) - 1$ in the first case and $\mathrm{ed}(G) \geqslant \mathrm{ed}(G; p) \geqslant a(p) \geqslant \dim(V)$ in the second. Since we have established the opposite inequalities, this will complete the proof in both cases.

By Springer's theorem (1.4), $a(p)$ is equal to the number of invariant degrees d_i which are divisible by p. In the case where $G = G(m, m, n)$, $m \geqslant 2$ and (m, n) are relatively prime, the degrees d_i are $m, 2m, \ldots, (n-1)m$ and n. Taking p to be a prime divisor of m, we see that $a(p) = n - 1 = \dim(V) - 1$, as desired.

For all other groups of the form $G = G(m, l, n)$, with $m \geqslant 2$ the degrees d_i are $m, 2m, \ldots,$ $(n-1)m$ and mn/l. Note that in this case $\gcd(m, \frac{mn}{l}) > 1$. Choose a prime divisor p of $\gcd(m, \frac{mn}{l})$. Then p divides every d_i. Hence, in this case $a(p) = n = \dim(V)$, as desired.

Finally, in the case where $m = 1$, $G(m, l, n) = G(1, 1, n) = S_n$ is excluded by our hypothesis.

This leaves us with the exceptional groups ST_4–ST_{37}. If $G \neq \mathrm{ST}_{25}, \mathrm{ST}_{35}$ then every degree d_i of G is divisible by 2. Hence, $a(2) = \dim(V)$, as above. Similarly, if $G = ST_{25}$ then every degree d_i is divisible by 3 and $a(3) = \dim(V)$. Finally, $\mathrm{ST}_{35} = W(\mathbf{E_6})$ was treated in part (a).

Remark 7.1. Our proof shows that for every G in the statement of Theorem 1.3 there is a prime p such that $\mathrm{ed}(G) = a(p) = \mathrm{ed}(G; p)$.

Remark 7.2. Pinkham's construction applies in greater generality than the case of $W(\mathbf{E_6})$ used in Lemma 6.1. In particular, one can use it to construct a dominant rational $W(\mathbf{E_7})$-equivariant map $\mathbb{A}^7 \dashrightarrow Z$, where Z is a dense open subset of the six-dimensional variety $(\mathbb{P}^2)^7_{ss}/\!/\,\mathrm{PGL}_3$. Here the subscript $_{ss}$ denotes the semistable locus. Since we know that $\mathrm{ed}(W(\mathbf{E_7})) = 7$ by Theorem 1.3(c), this gives an alternative (indirect) proof of the classical fact that the Coble representation of $W(\mathbf{E_7})$ on $(\mathbb{P}^2)^7_{ss}/\!/\,\mathrm{PGL}_3$ is not faithful; see [**8**, p. 293] or [**10**, p. 122].

8. *A variant of Bertini's theorem*

Our proof of Theorem 1.4 will rely on the following variant of Bertini's theorem.

Theorem 8.1. *Let Y be a smooth, geometrically irreducible subscheme of $\mathbb{P}^N := \mathrm{Proj}(k[y_0, \ldots, y_N])$, $C \subset Y$ be a smooth zero-dimensional closed subscheme of Y, X be a geometrically irreducible variety and $\psi\colon X \to Y$ be a smooth morphism, all defined over k. Assume $\dim(Y) \geqslant 2$. When k is an infinite field of positive characteristic, we also assume that ψ is étale.*

Given a homogeneous polynomial $f \in k[y_0, \ldots, y_N]$, let Y^f be the intersection of Y with the hypersurface $\{f = 0\}$ and let X^f denote the preimage of Y^f under ψ. Then for $a \gg 0$ there exists a homogeneous polynomial f of degree a satisfying the following conditions:

(i) *X^f is geometrically irreducible,*
(ii) *Y^f is smooth,*
(iii) *Y^f contains C,*
(iv) *$\dim(X^f) = \dim(X) - 1$.*

In the case where k is infinite, Theorem 8.1 can be deduced from the classical Bertini theorem. In the situation where $X = Y$ and $\psi = \mathrm{id}$, this is done in [**20**]. A similar argument can be used to prove Theorem 8.1 in full generality (here k is still assumed to be infinite). For the sake of completeness, we briefly outline this argument below.

Proof of Theorem 8.1 *in the case where k is an infinite field.* Denote the ideal of $C \subset \mathbb{P}^N$ by $\mathcal{I} \subset k[y_0, \ldots, y_N]$. Let $\mathcal{I}_a$ be the homogeneous part of $\mathcal{I}$ of degree a. For $f \in \mathcal{I}_a$ in general position, Y^f is smooth at C and of dimension $\dim(Y) - 1$. Now consider the map

$$\phi_a\colon X \setminus \psi^{-1}(C) \longrightarrow \mathbb{P}(\mathcal{I}_a)$$

obtained by composing ψ with the morphism $\iota\colon Y \setminus C \to \mathbb{P}(\mathcal{I}_a)$, given by the linear system of degree a hypersurfaces passing through C. (Note that ι is an embedding for $a \gg 0$.) By Bertini's smoothness theorem [**17**, Corollaire 6.11(2)], for $f \in \mathcal{I}_a$ in general position, Y^f is smooth away from C. Since Y^f is also smooth at C, we conclude that Y^f is smooth, every irreducible component of Y^f is of dimension $\dim(Y) - 1$ and hence, every irreducible component of X^f is smooth of dimension $\dim(X) - 1$. By Bertini's irreducibility theorem [**17**, Corollaire 6.11(3)], for $f \in \mathcal{I}_a$ in general position, $X^f \setminus \psi^{-1}(C)$ is geometrically irreducible of dimension $\dim(X) - 1$. (This is where the assumption that ψ is étale is used when k is of positive characteristic.) Since $\dim(Y) \geqslant 2$, we have $\dim(X) - \dim(Y) \leqslant \dim(X) - 2$ and thus $\psi^{-1}(C)$ cannot contain a component of X^f. Hence, X^f itself is geometrically irreducible. This completes the proof of Theorem 8.1 in the case where k is infinite. □

If k is a finite field, then the classical Bertini theorems break down. In this case, our proof will be based on the probabilistic versions of Bertini's smoothness and irreducibility theorems, due to Poonen [33] and Charles and Poonen [5], respectively.

We begin by recalling the notion of density from [32]. Let $\mathcal{S} = k[y_0, \ldots, y_N]$ be the homogeneous coordinate ring of $\mathbb{P}^N$, $\mathcal{S}_a \subset \mathcal{S}$ be the k-vector subspace of homogeneous polynomials of degree a and $\mathcal{S}_{\text{hom}} = \bigcup_{a \geqslant 0} \mathcal{S}_a$. The *density* $\mu(\mathcal{P})$ of any subset $\mathcal{P} \subset \mathcal{S}_{\text{hom}}$ is defined as

$$\mu(\mathcal{P}) := \lim_{a \to \infty} \frac{|\mathcal{P} \cap \mathcal{S}_a|}{|\mathcal{S}_a|}.$$

Note $\mu(\mathcal{P})$ is either a real number between 0 and 1 or undefined (if the above limit does not exist).

LEMMA 8.2. *Suppose $\mathcal{P}_1, \mathcal{P}_2 \subset \mathcal{S}_{\text{hom}}$. If $\mu(\mathcal{P}_1) = 1$, then $\mu(\mathcal{P}_1 \cap \mathcal{P}_2) = \mu(\mathcal{P}_2)$.*

Proof. The lemma is a consequence of the inequalities

$$|\mathcal{P}_2 \cap \mathcal{S}_a| - |\mathcal{S}_a \setminus \mathcal{P}_1| \leqslant |\mathcal{P}_1 \cap \mathcal{P}_2 \cap \mathcal{S}_a| \leqslant |\mathcal{P}_2 \cap \mathcal{S}_a|,$$

since $\lim_{a \to \infty}(|\mathcal{S}_a \setminus \mathcal{P}_1|/|\mathcal{S}_a|) = 0$. □

Proof of Theorem 8.1 *in the case where k is a finite field.* Let $\mathcal{S} := k[y_0, \ldots, y_N]$ and $\mathcal{I}$ be the ideal in $\mathcal{S}$ corresponding to $C \subset \mathbb{P}^N$, and let $\mathcal{S}_{\text{hom}}$, $\mathcal{I}_{\text{hom}}$ be the sets of homogeneous polynomials in $\mathcal{S}$, $\mathcal{I}$, respectively.

We define $\mathcal{P}_1$ as the set of $f \in \mathcal{S}_{\text{hom}}$ such that X^f is geometrically irreducible, and $\mathcal{P}_2$ as the set of $f \in \mathcal{I}_{\text{hom}}$ such that Y^f is smooth and $\dim(Y^f) = \dim(Y) - 1$. Thus $\mathcal{P}_1 \cap \mathcal{P}_2$ is precisely the set of homogeneous polynomials satisfying conditions (i)–(iv) of the theorem. Our goal is to show that $\mu(\mathcal{P}_1 \cap \mathcal{P}_2)$ exists and is greater than 0. If we can prove this, then the theorem will immediately follow.

Since we are assuming ψ is smooth and $\dim(Y) \geqslant 2$, every fibre of ψ has codimension $\geqslant 2$ in X. Hence, no irreducible component of X^f can be contained in a fibre of ψ. Thus by Charles and Poonen [5, Theorem 1.6],

$$\mu(\mathcal{P}_1) = 1.$$

On the other hand, by Poonen [33, Theorem 1.1], the local density

$$\mu_C(\mathcal{P}_2) = \lim_{a \to \infty} \frac{|\mathcal{P}_2 \cap \mathcal{I}_a|}{|\mathcal{I}_a|} \text{ exists and is greater than 0.}$$

(This uses our assumptions that C is smooth and zero-dimensional. In particular, $\dim(X) > 2\dim(C)$.) Since C is a zero-dimensional subscheme of $\mathbb{P}^n$, we have $\dim_k(\mathcal{I}_a) = \dim_k(\mathcal{S}_a) - \deg(C)$, for large a. Here $\deg(C)$ denotes the degree of C in $\mathbb{P}^n$. Thus

$$\lim_{a \to \infty} \frac{|\mathcal{I}_a|}{|\mathcal{S}_a|} = |k|^{-\deg(C)} > 0.$$

Since $\mathcal{P}_2$ is, by definition, a subset of $\mathcal{I}_{\text{hom}}$, we have $\mathcal{P}_2 \cap \mathcal{I}_a = \mathcal{P}_2 \cap \mathcal{S}_a$ and thus

$$\mu(\mathcal{P}_2) = \lim_{a \to \infty} \frac{|\mathcal{P}_2 \cap \mathcal{S}_a|}{|\mathcal{S}_a|} = \lim_{a \to \infty} \frac{|\mathcal{P}_2 \cap \mathcal{I}_a|}{|\mathcal{I}_a|} \cdot \frac{|\mathcal{I}_a|}{|\mathcal{S}_a|} \text{ also exists and is greater than 0.}$$

Lemma 8.2 now tells us that $\mu(\mathcal{P}_1 \cap \mathcal{P}_2)$ exists and is greater than 0, as desired. □

9. *Proof of Theorem* 1.4: *preliminaries*

First we observe that Theorem 1.4(b) is an immediate consequence of Theorem 1.4(a). Indeed, combining the first inequality in (1.5) with part (a), we have

$$\max_p \operatorname{ed}(G;p) \leqslant \operatorname{pmed}(G) \leqslant \max_p a(p).$$

Theorem 1.1(b) now tells us that $a(p) = \operatorname{ed}(G;p)$ for each prime p, and part Theorem 1.4(b) follows.

From now on, we will focus on the proof of Theorem 1.4(a). Let G be a finite group and $G \hookrightarrow \mathrm{GL}(V)$ be a faithful linear representation defined over k. We will assume throughout that $\operatorname{char}(k)$ does not divide $|G|$. Consider the closed subscheme

$$B := \bigcup_{g\in G,\ \zeta\neq 1} V(g,\zeta) \quad \text{or equivalently,} \quad B = \bigcup_{\substack{g\in G,\ \zeta^p=1 \\ \zeta\neq 1,\ p \text{ prime}}} V(g,\zeta),$$

where ζ ranges over the roots of unity in $\bar{k}$. Note that, although each $V(g,\zeta)$ is defined only over $k(\zeta)$, their union B is defined over k.

The following lemma may be viewed as a variant of [**43**, Proposition 3.2].

Lemma 9.1. *Let $m \geqslant |G|$ be an integer. Suppose that $v \in V$ has the property that $f(v) = 0$ for every G-invariant homogeneous polynomial $f \in k[V]$ of degree m. Then $v \in B$.*

Proof. We may assume $v \neq 0$. Let $\bar{v} \in \mathbb{P}(V)$ be the projective point associated to v. Denote the G-orbit of $\bar{v}$ by $\bar{v}_1 = \bar{v}, \bar{v}_2, \dots, \bar{v}_r \in \mathbb{P}(V)$. Note that $r \leqslant |G| \leqslant m$.

We claim that there exists a homogeneous polynomial $h \in k[V]$ of degree m such that $h(\bar{v}_1) \neq 0$ but $h(\bar{v}_i) = 0$ for any $i = 2, \dots, r$. To construct h, for every $i = 2, \dots, r$ choose a linear form $l_i \in V^*$ such that $l_i(\bar{v}_i) = 0$ but $l_i(\bar{v}_1) \neq 0$. Now set $h = l_2^{m+2-r} l_3 \cdots l_r$. This proves the claim.

We now define a G-invariant homogeneous polynomial f of degree m by summing the translates of h over G:

$$f(v') = \sum_{g\in G} h(g\cdot v') \quad \forall v' \in V.$$

By our assumption, $f(v) = 0$.

Let $S \subset G$ be the stabilizer of $\bar{v}$, that is, the subgroup of elements $s \in G$ such that v is an eigenvector for s. Then $s(v) = \chi(s)v$ for some multiplicative character $\chi\colon S \to k^*$. It now suffices to show that $\chi(s) \neq 1$ for some $s \in S$. Indeed, if we denote $\chi(s)$ by ζ, for this s, then $v \in V(s,\zeta) \subset B$, as desired.

To show $\chi(s) \neq 1$ for some $s \in S$, recall that by our choice of h, $h(g\cdot v) = 0$ unless $g \in S$. Thus

$$0 = f(v) = \sum_{s\in S} h(s\cdot v) = \sum_{s\in S} h(\chi(s)v) = \sum_{s\in S} \chi(s)^m h(v).$$

If $\chi(s) = 1$ for every $s \in S$, then the above equation reduces to $0 = |S|\cdot h(v)$. This is a contradiction since $h(v) \neq 0$, and we are assuming that $\operatorname{char}(k)$ does not divide $|G|$ (and consequently does not divide $|S|$). Thus $\chi(s) \neq 1$ for some $s \in S$, as claimed. $\square$

Denote the direct sum of V and the trivial one-dimensional representation of G by $W := V \times k$. Let z be the coordinate along the second factor in $W = V \times k$. We will identify V with the open subvariety of $\mathbb{P}(W)$ given by $z \neq 0$, and $\mathbb{P}(V)$ with the closed subvariety of $\mathbb{P}(W)$ given by $z = 0$. Set $n := \dim(V) = \dim(\mathbb{P}(W))$. If C is a cone in V with vertex at the origin, then we will denote by $\mathbb{P}(C)$ the image of $C \setminus \{0\}$ under the natural projection $(V \setminus \{0\}) \to \mathbb{P}(V)$.

Proposition 9.2. *Consider the rational map*

$$\psi_m \colon \mathbb{P}(W) \dashrightarrow \mathbb{P}^N$$

given by the linear system $k[W]_m^G$ of G-invariant homogeneous polynomials of degree m on W. Denote the closure of the image of ψ_m by $Y \subset \mathbb{P}^N$. Assume $m \geqslant |G|$.

(a) *Then the map ψ_m is regular away from $\mathbb{P}(B)$.*

(b) *The inclusion of fields $k(Y) \hookrightarrow k(\mathbb{P}(W))^G$ induced by ψ_m is an isomorphism. Here $k(\mathbb{P}(W))^G$ denotes the field of G-invariant rational functions on $\mathbb{P}(W)$.*

(c) *For a prime $q \gg 0$, every fibre of the morphism $\psi_q \colon \mathbb{P}(W \setminus B) \to Y$ is finite.*

Proof. (a) We may assume without loss of generality that k is algebraically closed. Since $z^m \in k[W]_m^G$, we see that the indeterminacy locus of ψ_m consists of points $(v : a) \in \mathbb{P}(W)$ with $a = 0$ and $f(v) = 0$ for every $f \in k[V]_m^G$, where $k[V]_m^G$ denotes the k-vector space of G-invariant homogeneous polynomials on V of degree m. By Lemma 9.1, $v \in B$. Thus $(v : a) \in \mathbb{P}(B) \subset \mathbb{P}(V \times \{0\}) \subset \mathbb{P}(W)$, as claimed.

(b) To show that the natural inclusion $\psi_m^* \colon k(Y) \hookrightarrow k(\mathbb{P}(W))^G$ of fields is an isomorphism, we restrict ψ_m to the dense open subset $V \subset \mathbb{P}(W)$ given by $z \neq 0$. This restriction is the morphism

$$V \to \mathbb{A}^N,$$
$$v \mapsto (f_1(v), \ldots, f_N(v)),$$

where $f_1, \ldots, f_N$ form a basis of the vector space $k[V]_{\leqslant m}^G$ of G-invariant polynomials of degree at most m. Consequently, $f_1, \ldots, f_N \in \psi_m^*(k(Y))$. By the Noether bound, $k[V]^G$ is generated by polynomials of degree at most $|G|$ as a k-algebra; see Remark 9.6. Since $|G| \leqslant m$, we conclude that $\psi_m^*(k(Y))$ contains $k[V]^G$ and thus its fraction field $k(V)^G$. Since V is a G-invariant dense open subset of $\mathbb{P}(W)$, we have $k(V) = k(\mathbb{P}(W))$. Therefore, $\psi_m^*(k(Y)) \supset k(V)^G = k(\mathbb{P}(W))^G$, as desired.

(c) Suppose $v \in V \subset \mathbb{P}(W)$, that is, $z(v) \neq 0$. The argument of part (b) shows that in this case w lies in the same fibre of ψ as v if and only if $w \in V$ and $f(v) = f(w)$ for every $f \in k[V]^G$. Since elements of $k[V]^G$ separate the G-orbits in V, this shows that the fibres of ψ_q in V are precisely the G-orbits in V, and hence, are finite.

We may thus restrict ψ_q to $\mathbb{P}(V) \subset \mathbb{P}(W)$, where $z = 0$. That is, it suffices to show that if q is a large enough prime, then every fibre of the morphism $\psi_q \colon \mathbb{P}(V \setminus B) \to \mathbb{P}^N$ is finite. Equivalently, it suffices to show that every fibre of the morphism

$$\phi_q \colon V \setminus B \longrightarrow \mathbb{A}(k[V]_q^G)$$

given by the linear system $k[V]_q^G$ of G-invariant polynomials of degree q, is finite. In particular, we may assume without loss of generality that $B \subsetneq V$.

Choose homogeneous generators $g_1, \ldots, g_r$ for $k[V]^G$ and fix them for the rest of the proof. Denote their degrees by $d_1, \ldots, d_r$, respectively. By the Noether bound, we may assume $d_1, \ldots, d_r \leqslant |G|$.

Let $\Lambda_{d_1,\ldots,d_r}^q \subset \mathbb{Z}_{\geqslant 0}^r$ be the set of non-negative integers solutions $(a_1, \ldots, a_r)$ of the linear Diophantine equation

$$a_1 d_1 + \cdots + a_r d_r = q.$$

Then the polynomials $g_1^{a_1} \cdots g_r^{a_r}$ span $k[V]_q^G$, as $(a_1, \ldots, a_r)$ ranges over $\Lambda_{d_1,\ldots,d_r}^q$. In other words, $\phi_q(v) = \phi_q(w)$ if and only if $g_1^{a_1}(v) \cdots g_r^{a_r}(v) = g_1^{a_1}(w) \cdots g_r^{a_r}(w)$ for every $(a_1, \ldots, a_r) \in \Lambda_{d_1,\ldots,d_r}^q$.

Let us now fix $v \in V \setminus B$ and consider $w \in V \setminus B$ such that $\phi_q(w) = \phi_q(v)$. Our ultimate goal is to show that if q is a large enough prime, then there are only finitely many such w. After renumbering $g_1, \dots, g_r$, we may assume $g_1(v), \dots, g_s(v) \neq 0$ but $g_{s+1}(v) = \cdots = g_r(v) = 0$.

Claim 9.3. $d_1, \dots, d_s$ are relatively prime.

Indeed, assume the contrary: $\gcd(d_1, \dots, d_s) \geqslant 2$. Choose a prime $q > |G|$. Since $v \notin B$, Lemma 9.1 tells us that there exists an $f \in k[V]_q^G$ such that $f(v) \neq 0$. Since f is a polynomial in $g_1, \dots, g_r$, some monomial $g_1^{a_1} \cdots g_r^{a_r}$ of total degree $a_1 d_1 + \cdots + a_r d_r = q$ does not vanish at v. After replacing f by this monomial, we may assume $f = g_1^{a_1} \cdots g_r^{a_r}$. Note that $a_j \geqslant 1$ for some $j \geqslant s+1, \dots, r$. Otherwise q would be divisible by $\gcd(d_1, \dots, d_s)$, which is not possible, because q is a prime and $q > |G| \geqslant d_1, \dots, d_s \geqslant \gcd(d_1, \dots, d_s) \geqslant 2$. Since $g_j(v) = 0$, we conclude that $f(v) = g_1^{a_1}(v) \cdots g_r^{a_r}(v) = 0$, a contradiction. This completes the proof of Claim 9.3.

It is well known that if $d_1, \dots, d_s \geqslant 1$ are relatively prime integers, then for large enough integers q (not necessarily prime), $\Lambda^q_{d_1,\dots,d_s} \neq \emptyset$. The largest integer $q \geqslant 0$ such that $\Lambda^q_{d_1,\dots,d_s} = \emptyset$ is called the *Frobenius number*; we will denote it by $F(d_1, \dots, d_s)$. This number has been extensively studied; for an explicit upper bound on F in terms of $d_1, \dots, d_s$, see, for example, [**13**].

Claim 9.4. Suppose that our prime q is greater than $F(d_1, \dots, d_s) + d_1 + \cdots + d_r$. Then:

(i) $g_i(w) \neq 0$ for every $i = 1, \dots, s$; and
(ii) $g_j(w) = 0$ for every $j = s+1, \dots, r$.

To prove (i), note that since $q - d_1 - \cdots - d_s > F(d_1, \dots, d_s)$, there is an s-tuple $(a_1, \dots, a_s)$ of non-negative integers such that $a_1 d_1 + \cdots + a_s d_s = q - d_1 - \cdots - d_s$. Thus the polynomial $P := g_1^{a_1+1} \cdots g_s^{a_s+1}$ lies in $k[V]_q^G$. By our assumption, $P(w) = P(v) \neq 0$. Hence, $g_i(w) \neq 0$ for any $i = 1, \dots, s$.

To prove (ii), choose j between $s+1$ and r. Since $q - d_j > F(d_1, \dots, d_s)$, there is an s-tuple $(b_1, \dots, b_s)$ of non-negative integers such that $b_1 d_1 + \cdots + b_s d_s = q - d_j$. Now the polynomial $Q := g_1^{b_1} \cdots g_s^{b_s} g_j$ lies in $k[V]_q^G$. Since $g_j(v) = 0$, we have $Q(w) = Q(v) = 0$. By (i), $Q(w) = 0$ is only possible if $g_j(w) = 0$. This completes the proof of Claim 9.4.

Claim 9.5. There exists a $q_0 > 0$ such that for any integer $q \geqslant q_0$ (not necessarily a prime), the set $\Lambda^q_{d_1,\dots,d_s}$ spans $\mathbb{Q}^s$ as a $\mathbb{Q}$-vector space.

To prove Claim 9.5, choose an integer basis $\vec{z}_1, \dots, \vec{z}_{s-1} \in \mathbb{Z}^s$ for the $\mathbb{Q}$-vector space of solutions of the homogeneous linear equation $a_1 d_1 + \cdots + a_s d_s = 0$. Denote the maximal absolute value of the coordinates of $\vec{z}_1, \dots \vec{z}_{s-1}$ by M and set $q_0 := F(d_1, \dots, d_s) + (d_1 + \cdots + d_s)M$.

For every $q > q_0$, we will construct an $\vec{a} = (a_1, \dots, a_s) \in \Lambda^q_{d_1,\dots,d_s}$ such that $a_i \geqslant M$ for every i. Indeed, since $q - (d_1 + \cdots + d_s)M > F$ there are non-negative $b_1, \dots, b_s$ such that $b_1 d_1 + \cdots + b_s d_s = q - (d_1 + \cdots + d_s)M$. We can now take $\vec{a} := (b_1 + M, \dots, b_s + M)$.

Finally, for $q > q_0$, the s integer vectors

$$\vec{a}, \vec{a} + \vec{z}_1, \dots, \vec{a} + \vec{z}_{s-1}$$

lie in $\Lambda^q_{d_1,\dots,d_s}$ and are linearly independent. This completes the proof of Claim 9.5.

Suppose that q is a prime, large enough to satisfy the assumptions of Claims 9.4 and 9.5. We are now in a position to show that for any $v \in V \setminus B$, there are only finitely many $w \in V \setminus B$ such that $\phi_q(v) = \phi_q(w)$. By Claim 9.5, there exist s linearly independent vectors $(a_{11}, \dots, a_{1s}), \dots, (a_{s1}, \dots, a_{ss})$ in $\Lambda^q_{d_1,\dots,d_s}$. Thus

$$\begin{cases} g_1(w)^{a_{11}} \cdots g_s(w)^{a_{1s}} = g_1(v)^{a_{11}} \cdots g_s(v)^{a_{1s}}, \\ g_1(w)^{a_{21}} \cdots g_s(w)^{a_{2s}} = g_1(v)^{a_{21}} \cdots g_s(v)^{a_{2s}}, \\ \qquad \vdots \\ g_1(w)^{a_{s1}} \cdots g_s(w)^{a_{ss}} = g_1(v)^{a_{s1}} \cdots g_s(v)^{a_{ss}}, \end{cases}$$

where the elements on the right-hand side are non-zero. We view v as fixed and allow w to range over the fibre of $\phi_q(v)$. The matrix $A := (a_{ij})$ is invertible. The inverse matrix A^{-1} has rational entries, and $\det(A)A^{-1}$ has integer entries. Thus, we can solve the above system for $g_1^{\det(A)}(w), \dots, g_s^{\det A}(w)$.

In conclusion, as w ranges over the fibre of $\phi_q(v)$, we see that $g_{s+1}(w) = \cdots = g_r(w) = 0$ (by Claim 9.4) and $g_1(w) = \cdots = g_s(w)$ assume only finitely many values. Thus w can lie in only finitely many G-orbits, as desired. $\square$

REMARK 9.6. Noether showed that $k[V]^G$ is generated by polynomials of degree at most $|G|$ as a k-algebra under the assumption $\mathrm{char}(k) = 0$. The more general variant of the Noether bound used in the proof of Proposition 9.2 (where $\mathrm{char}(k) > 0$ is allowed, as long as $\mathrm{char}(k)$ does not divide $|G|$) is due to Fleischmann, Fogarty and Benson. For details and further references, see [**7**, Section 3.8].

10. *Proof of Theorem* 1.4(a)

Set $d := \dim(B) = \max_p a(p)$. Our goal is to construct a d-dimensional irreducible faithful G-variety X_d which is p-versal for every prime p. This would imply $\mathrm{pmed}(G) \leqslant \dim(X_d) = d$, as desired.

If $|G| = 1$ (or, equivalently, $d = 0$), then we can take X_d to be a point. Thus, from now on, we will assume that G is non-trivial or, equivalently, $d \geqslant 1$.

Choose a sufficiently large prime integer q so that $q \neq \mathrm{char}(k)$, and every part of Proposition 9.2 holds; in particular, we will assume $q > |G|$. This prime will remain fixed throughout the proof. For notational simplicity, we will write $\psi \colon \mathbb{P}(W) \dashrightarrow Y \subset \mathbb{P}^N$ for the rational map given by the linear system $k[W]^G_q$ of G-invariant homogeneous polynomials of degree q, instead of ψ_q. By Proposition 9.2(a), ψ is regular away from B, and by Proposition 9.2(b), ψ is generically a G-torsor.

Let Y_n be a dense open subset of Y such that $\psi \colon X_n \to Y_n$ is a G-torsor (and in particular, étale). Here X_n is the preimage of Y_n in $\mathbb{P}(W \setminus B)$. The subscript n in X_n and Y_n is intended to remind us that $\dim(X_n) = \dim(Y_n) = n$, where $n = \dim(V) = \dim(\mathbb{P}(W))$, as before. The idea of our construction of X_d is to start with a G-invariant open subset X_n of $\mathbb{P}(W \setminus B)$ and to construct successive hyperplane sections $X_{n-1}, \dots, X_d$ recursively by appealing to Theorem 8.1.

If $n = d$, then we are done. Indeed, our variety X_n is G-equivariantly birationally isomorphic to a vector space V, with a faithful linear G-action. Hence, X_n is versal, and, in particular, p-versal for every prime p. Therefore, we may assume without loss of generality that $n \geqslant d + 1 \geqslant 2$.

Since X_n is birationally isomorphic to V, there exists an F-point $x \in X_n(F)$, where F/k is a finite separable field extension of degree prime to q. In fact, such points are dense in X_n. Note that if k is infinite, then we can take $F = k$.

By Theorem 8.1 for sufficiently large s_1, there is a homogeneous polynomial $f \in k[y_0, \dots, y_N]$ of degree q^{s_1} such that the following conditions hold:

(i) $(X_n)^{f_1}$ is geometrically irreducible,
(ii) $(Y_n)^{f_1}$ is smooth,
(iii) $\psi(x) \in (Y_n)^{f_1}$,
(iv) $\dim((X_n)^{f_1}) = \dim(X_n) - 1$.

Here $y_0, \dots, y_N$ denote homogeneous coordinates on $\mathbb{P}^N$.

We now set $X_{n-1} := (X_n)^{f_1}$, $Y_{n-1} := (Y_n)^{f_1}$ and proceed to construct $Y_{n-2}, \dots, Y_{n-d}$ and $X_{n-2}, \dots, X_d$ recursively, where each X_{n-i} is the preimage of Y_{n-i} in $\mathbb{P}(W \setminus B)$ under ψ, each X_{n-i} is irreducible, each Y_{n-i} (and hence, X_{n-i}) is smooth of dimension $n-i$, each Y_{n-i} contains $\psi(x)$ and each Y_{n-i-1} is obtained by intersecting Y_{n-i} with a hypersurface $f_i = 0$ in $\mathbb{P}^N$, for a homogeneous polynomial $f_i \in k[y_0, \dots, y_N]$ of degree q^{s_i}.

Note that since ψ is given by the linear system of $k[V]^G_q$ of homogeneous G-invariant polynomials of degree q, f_i lifts to a homogeneous polynomial $\psi^*(f_i)$ of degree q^{s_1+1} on $\mathbb{P}(W)$. In other words,

$$X_d = (H[1] \cap \cdots \cap H[n-d]) \setminus (\mathbb{P}(B) \cup \psi^{-1}(\bar{Y}_d \setminus Y_d)), \tag{10.1}$$

where $\bar{Y}_d$ is the closure of Y_d in $\mathbb{P}^N$ and $H[i]$ is a hypersurface of degree q^{s_i+1} in $\mathbb{P}(W)$ cut out by $\psi^*(f_i)$.

Since each $\psi\colon X_{n-i} \to Y_{n-i}$ is a G-torsor, the G-action on X_d is faithful. Thus it remains to show that the G-action on X_d is p-versal for every prime p.

Case 1: Assume $p = q$. Recall that the G-action on X_d is p-versal if and only if the G_p-action on X_d is p-versal, where G_p is a Sylow p-subgroup of G; see [**12**, Corollary 8.6]. Since $q > |G|$, we have $G_q = \{1\}$. Thus in order to show that X_d is q-versal, it suffices to show that X_d has a 0-cycle of degree prime to q; see [**12**, Lemma 8.2 and Theorem 8.3]. By our construction, Y_d contains $\psi(x)$ and hence, X_d contains x, where x is a point of degree prime to q. This shows that X_d is q-versal.

Case 2: Now assume $p \neq q$. To show that the G-action on X_d is p-versal, it suffices to prove that for every field extension K/k, with K infinite, and every G-torsor $T \to \mathrm{Spec}(K)$, the twisted K-variety ${}^T X_d$ contains a 0-cycle Z, whose degree over K is a power of q (and thus prime to p); see [**12**, Section 8].

Since the G-action on $\mathbb{P}(W)$ lifts to a linear G-action on W, Hilbert's theorem 90 tells us that ${}^T\mathbb{P}(W) = \mathbb{P}(W_K)$ is a projective space over K; see, for example, [**12**, Lemma 10.1]. Twisting both sides of (10.1) by T, we obtain

$${}^T X_d = ({}^T H[1] \cap \cdots \cap {}^T H[n-d]) \setminus ({}^T\mathbb{P}(B) \cup {}^T\psi^{-1}(\bar{Y}_d \setminus Y_d))$$

in $\mathbb{P}(W_K)$. We will construct the desired 0-cycle Z on ${}^T X_d$ by intersecting ${}^T X_d$ with d hyperplanes $M_1, \dots, M_d$ in $\mathbb{P}(W_K)$ in general position. Note that since Y_d is irreducible, Proposition 9.2(c) tells us that

$$\dim_k \psi^{-1}(\bar{Y}_d \setminus Y_d) \leqslant \dim_k(\bar{Y}_d \setminus Y_d) \leqslant \dim_k(Y_d) - 1 = d - 1.$$

Since $\dim_k(\mathbb{P}(B)) = \dim_k(B) - 1 = d - 1$, we see that a linear subspace $M = M_1 \cap \cdots \cap M_d$ of codimension d in $\mathbb{P}(W_K)$ in general position misses both ${}^T\mathbb{P}(B)$ and ${}^T\psi^{-1}(\bar{Y}_d \setminus Y_d)$.

Let Z be the intersection cycle obtained by intersecting ${}^T X_d$ with M. By Duncan and Reichstein [**12**, Lemma 10.1(c)], each ${}^T H[i]$ is a hypersurface of degree q^{s_i+1} in $\mathbb{P}(W_K)$. Hence, by Bezout's theorem [**14**, Proposition 8.4],

$$\begin{aligned}\deg_K(Z) &= \deg({}^T H[1]) \cdots \deg({}^T H[n-d]) \cdot \deg(M_1) \cdots \deg(M_d) \\ &= q^{s_1+1} \cdots q^{s_{n-d}+1} \cdot \underbrace{1 \cdots 1}_{d \text{ times}}\end{aligned}$$

is a power of q, as desired. □

11. *A-groups*

Let G be a finite group, p be a prime and G_p be a Sylow p-subgroup of G. Recall that G is called an *A-group* if G_p is abelian for every p; see, for example, [**2**, **15**, **45**]. For the rest of this section, with the exception of Conjecture 11.5, we will assume that the base field k is of characteristic zero and $\zeta_e \in k$, where e is the exponent of G.

Proposition 11.1. *Let G be an A-group. Then*

$$\mathrm{pmed}(G) = \max_p \mathrm{ed}(G; p) = \max_p \mathrm{rank}(G_p),$$

where the maximum is taken over all primes p.

Here, as usual, by the rank of a finite abelian group H we mean the minimal number of generators of H.

Proof. The second equality is well known; see, for example, [**36**, Corollary 7.3]. Note also that this is a very special case of (1.1). In view of (1.5), in order to prove the first equality, we need to show only that $\mathrm{pmed}(G) \leqslant \max_p \mathrm{rank}(G_p)$.

Let $p_1, \ldots, p_r$ be the prime divisors of $|G|$ and $d = \max \mathrm{rank}(G_{p_i})$, as i ranges from 1 to r. By Reichstein and Youssin [**37**, Theorem 8.6], there exists a faithful primitive d-dimensional G-variety Y with smooth k-points $y_1, \ldots, y_r$ such that $G_{p_i} \subset \mathrm{Stab}_G(y_i)$ for $i = 1, \ldots, r$.

Recall that 'primitive' means that G transitively permutes the irreducible components of $Y_{\bar{k}}$. We claim that any such Y is, in fact, absolutely irreducible. Let us assume this claim for a moment. The G-orbit of y_i is a 0-cycle of degree prime to p_i. Thus for any given prime p, the degree of one of these orbits is prime to p. By Duncan and Reichstein [**12**, Corollary 8.6(b)], this implies that Y is p-versal for every p. Hence, $\mathrm{pmed}(G) \leqslant \dim(Y) = d$, and the proposition follows.

It remains to show that Y is absolutely irreducible. After replacing k by its algebraic closure $\bar{k}$, we may assume that k is algebraically closed. Let Y_0 be an irreducible component of Y and H be the stabilizer of Y_0 in G. Our goal is to prove $H = G$. Since G acts transitively on the irreducible components of Y, this will imply $Y = Y_0$.

Since y_i is a smooth point of Y, it lies on exactly one irreducible component of Y, say on $g_i(Y_0)$ for some $g_i \in G$. Since y_i is G_{p_i}-invariant, y_i also lies on $gg_i(Y_0)$ for every $g \in G_{p_i}$. In other words, $gg_i(Y_0) = g_i(Y_0)$ for every $g \in G_{p_i}$ or equivalently, $g_i^{-1} G_{p_i} g_i \subset H$ for every $i = 1, \ldots, s$. This shows that H contains a Sylow p_i-subgroup of G for $i = 1, \ldots, r$. Hence, $|H|$ is divisible by $|G_{p_i}|$ for every $i = 1, \ldots, r$. We conclude that $|H|$ is divisible by $|G| = |G_{p_1}| \cdots |G_{p_s}|$ and hence, $H = G$. □

Remark 11.2. The above argument relies, in a key way, on [**37**, Theorem 8.6]. This theorem is proved in [**37**] over an algebraically closed field of characteristic 0 but the proof goes through for any k as above. The condition that $\zeta_e \in k$, is necessary; it is not mentioned in [**37**, Remark 9.9] due to an oversight.

EXAMPLE 11.3. If G is a non-abelian group of order pq, where p and q are odd primes, then Proposition 11.1 tells us that $\mathrm{pmed}(G) = 1$. On the other hand, $\mathrm{ed}(G) \geqslant 2$; see [**3**, Theorem 6.2]. This is, perhaps, the simplest example where $\mathrm{pmed}(G) < \mathrm{ed}(G)$.

REMARK 11.4. Non-abelian simple A-groups are classified in [**2**, Theorem 3.2]: they are J_1, the first Janko group, and $\mathrm{PSL}_2(q)$ for $q > 3$ and $q \equiv 0$, 3 or 5 (mod 8). By Proposition 11.1,

$$\mathrm{pmed}(G) = \begin{cases} 3 & \text{if } G \simeq J_1, \\ 2 & \text{if } G \simeq \mathrm{PSL}_2(q), \text{ with } q \text{ as above.} \end{cases}$$

On the other hand, by Beauville [**1**], $\mathrm{ed}(G) \geqslant 4$ for any of these groups, except for $G \simeq \mathrm{PSL}_2(5)$ and (possibly) $\mathrm{PSL}_2(11)$.

It is natural to conjecture the following generalization of [**37**, Theorem 8.6].

CONJECTURE 11.5. Let d be a positive integer. Suppose that G is a finite group with subgroups $H_1, \ldots, H_r$ such that $\mathrm{rdim}_k(H_i) \leqslant d$ for all $i = 1, \ldots, r$. Then there exists a d-dimensional k-variety X with a faithful G-action and smooth k-points $x_1, \ldots, x_r \in X$ such that H_i fixes x_i for each $i = 1, \ldots, r$.

Note that each H_i must act faithfully on the tangent space of the corresponding x_i. Thus the assumption that $\mathrm{rdim}(H_i) \leqslant d$ for each i is necessary.

Of particular interest is the special case where $p_1, \ldots, p_r$ are the distinct primes dividing $|G|$, each H_i is a Sylow p_i-subgroup and d is the maximum of $\mathrm{ed}_k(G; p_i) = \mathrm{rdim}_k(H_i)$. If Conjecture 11.5 could be established in this special case, then the argument we used in the proof of Proposition 11.1 would show that the G-action on X is p-versal for every prime p and, consequently, that (1.6) holds for G. We have not been able to prove (1.6) by this method beyond the case of A-groups.

12. *Examples*

In this section, we present two examples that complement Theorem 1.4(b). Example 12.1 shows that the inequality of Theorem 1.4(a) is in fact an equality, for the natural n-dimensional representation V of the alternating group A_n. Note that Theorem 1.4(b) cannot be applied to $A_n \subset \mathrm{GL}(V)$, since A_n contains no pseudo-reflections. Nevertheless, the conclusion of Theorem 1.4(b) continues to hold in this case. On the other hand, Example 12.2 shows that for $G = \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, the inequality of Theorem 1.4(a) is strict for every faithful representation $G \hookrightarrow \mathrm{GL}(V)$.

EXAMPLE 12.1. Let A_n be the alternating group on n letters. Assume $n \geqslant 4$. Then $\mathrm{pmed}(A_n) = \mathrm{ed}(A_n; 2) = 2\lfloor n/4 \rfloor$ for any $n \geqslant 4$.

Proof. Since A_n contains an elementary abelian subgroup of rank $2\lfloor n/4 \rfloor$ generated by $(12)(34), (13)(24), (56)(78)$, etc., we have $\mathrm{pmed}(A_n) \geqslant \mathrm{ed}(A_n; 2) = 2\lfloor n/4 \rfloor$; see [**3**, Theorem 6.7(c)].

We will now deduce the opposite inequality,

$$\mathrm{pmed}(A_n) \leqslant 2 \left\lfloor \frac{n}{4} \right\rfloor, \tag{12.1}$$

from Theorem 1.4(a). Let $V = k^n$ be the natural representation of S_n. One checks that for any $g \in S_n$ and any prime p, the dimension of the eigenspace $V(g, \zeta_p)$ is the number of cycles of length divisible by p in the cycle decomposition of g. Thus

$$a(p) = \max_{g \in A_n} \dim V(g, \zeta_p) = \begin{cases} \lfloor n/p \rfloor & \text{if } p \text{ is odd, and} \\ 2\lfloor n/4 \rfloor & \text{if } p = 2. \end{cases}$$

Since we are assuming $n \geqslant 4$, the maximal value of $a(p)$ is attained at $p = 2$. The inequality (12.1) now follows from Theorem 1.4(a), as desired. □

Example 12.2. Let $G = \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, where $\mathbb{Z}/4\mathbb{Z}$ acts faithfully on $\mathbb{Z}/5\mathbb{Z}$. Assume $\zeta_{20} \in k$.

(a) Then $\mathrm{pmed}(G) = 1$.
(b) However, $a_\phi(2) \geqslant 2$ for every faithful representation ϕ of G.

Proof. Since the Sylow subgroups of G are $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$, part (a) follows from Proposition 11.1.

(b) Each of the four characters $\mathbb{Z}/4\mathbb{Z} \to k^*$ induces a one-dimensional representation of G. We will denote these representations by $\phi_0 = \mathrm{id}$, ϕ_1, ϕ_2 and ϕ_3. Let $\phi_4 = \mathrm{Ind}_{\mathbb{Z}/5\mathbb{Z}}^G(\chi)$, where χ is a non-trivial multiplicative character $\mathbb{Z}/5\mathbb{Z} \to k^*$. We see that ϕ_4 is a faithful irreducible four-dimensional representation of G (irreducibility follows, for example, from Mackey's criterion) and $a_{\phi_4}(2) = 2$. Since $\dim(\phi_0)^2 + \cdots + \dim(\phi_4)^2 = 4 \cdot 1^2 + 4^2 = 20 = |G|$, $\phi_0, \ldots, \phi_4$ are the only irreducible representations of G. Moreover, since $\mathbb{Z}/5\mathbb{Z}$ lies in the kernel of $\phi_0, \ldots, \phi_3$, every faithful representation ϕ of G must contain a copy of ϕ_4. Thus $a_\phi(2) \geqslant a_{\phi_4}(2) = 2$. □

Remark 12.3. Ledet showed $\mathrm{ed}(\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}) = 2$; see [**22**, p. 426]. Note that in [**22**] this group is denoted by C_5.

Acknowledgements. The authors are grateful to I. Dolgachev for suggesting the geometric construction used in the proof of Lemma 6.1 and B. Poonen for a helpful discussion of Bertini's theorem over finite fields and for sending us a draft version of his preprint [**5**]. We would also like to thank M. García-Armas, G. I. Lehrer, R. Lötscher, M. MacDonald, J.-P. Serre and an anonymous referee for helpful comments.

References

1. A. Beauville, 'Finite simple groups of small essential dimension', *Trends in contemporary mathematics*, (eds Vincenzo Ancona and Elisabetta Strickland; Springer INdAM series, 2014) 221–228.
2. A. M. Broshi, 'Finite groups whose Sylow subgroups are abelian', *J. Algebra* 17 (1971) 74–82.
3. J. Buhler and Z. Reichstein, 'On the essential dimension of a finite group', *Compos. Math.* 106 (1997) 159–179.
4. J. Buhler and Z. Reichstein, 'On Tschirnhaus transformations', *Topics in number theory (University Park, PA, 1997)*, Mathematics and its Applications 467 (Kluwer Academic Publishers, Dordrecht, 1999) 127–142.
5. F. Charles and B. Poonen, 'Bertini irreducibility theorems over finite fields', Preprint, 2013, arXiv:1311.4960 [math.AG].
6. J. H. Conway and N. J. A. Sloane, 'The Coxeter–Todd lattice, the Mitchell group, and related sphere packings', *Math. Proc. Cambridge Philos. Soc.* 93 (1983) 421–440.
7. H. Derksen and G. Kemper, *Computational invariant theory*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 5. *Invariant theory and algebraic transformation groups, I.* Encyclopaedia of Mathematical Sciences 130 (Springer, Berlin, 2002).

8. I. V. Dolgachev, 'Weyl groups and Cremona transformations', *Singularities, Part 1 (Arcata, CA, 1981)*, Proceedings of Symposia in Pure Mathematics 40 (American Mathematical Society, Providence, RI, 1983) 283–294.
9. I. V. Dolgachev, 'Reflection groups in algebraic geometry', *Bull. Amer. Math. Soc. (N.S.)* 45 (2008) 1–60.
10. I. V. Dolgachev and D. Ortland, *Point sets in projective spaces and theta functions*, Astérisque 165 (Société Mathématique de France, Paris, 1988).
11. A. Duncan, 'Essential dimensions of A_7 and S_7', *Math. Res. Lett.* 17 (2010) 263–266.
12. A. Duncan and Z. Reichstein, 'Versality of algebraic group actions and rational points on twisted varieties', *J. Algebraic Geom.*, Preprint, 2011, arXiv:1109.6093v4 [math.AG].
13. P. Erdös and R. L. Graham, 'On a linear diophantine problem of Frobenius', *Acta Arith.* 21 (1972) 399–408.
14. W. Fulton, *Intersection theory* (Springer, Berlin, 1984).
15. N. Itô, 'Note on A-groups', *Nagoya Math. J.* 4 (1952) 79–81.
16. C. U. Jensen, A. Ledet and N. Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications 45 (Cambridge University Press, Cambridge, 2002).
17. J.-P. Jouanolou, *Théorèmes de Bertini et applications*, Progress in Mathematics 42 (Birkhäuser Boston, Boston, MA, 1983).
18. R. Kane, *Reflection groups and invariant theory*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC 5 (Springer, New York, 2001).
19. N. A. Karpenko and A. S. Merkurjev, 'Essential dimension of finite p-groups', *Invent. Math.* 172 (2008) 491–508.
20. S. L. Kleiman and A. B. Altman, 'Bertini theorems for hypersurface sections containing a subscheme', *Comm. Algebra* 7 (1979) 775–790.
21. F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade* (Teubner, Leipzig, 1884). English translation: *Lectures on the icosahedron and solution of equations of the fifth degree*, translated by G. G. Morrice, 2nd and rev. edition (Dover Publications, New York, 1956).
22. A. Ledet, 'On the essential dimension of some semi-direct products', *Canad. Math. Bull.* 45 (2002) 422–427.
23. G. I. Lehrer and J. Michel, 'Invariant theory and eigenspaces for unitary reflection groups', *C. R. Math. Acad. Sci. Paris* 336 (2003) 795–800.
24. G. I. Lehrer and D. E. Taylor, *Unitary reflection groups*, Australian Mathematical Society Lecture Series 20 (Cambridge University Press, Cambridge, 2009).
25. R. Lötscher, A. Meyer, M. MacDonald and Z. Reichstein, 'Essential dimension of algebraic tori', *J. reine angew. Math.* 677 (2013) 1–13.
26. M. MacDonald, 'Essential p-dimension of the normalizer of a maximal torus', *Transform. Groups* 16 (2011) 1143–1171.
27. Y. I. Manin, *Cubic forms. Algebra, geometry, arithmetic*, 2nd edn, North-Holland Mathematical Library 4 (North-Holland Publishing, Amsterdam, 1986). Translated from the Russian by M. Hazewinkel.
28. A. S. Merkurjev, 'Essential dimension: a survey', *Transform. Groups* 18 (2013) 415–481.
29. A. Meyer and Z. Reichstein, 'The essential dimension of the normalizer of a maximal torus in the projective linear group', *Algebra Number Theory* 3 (2009) 467–487.
30. A. Meyer and Z. Reichstein, 'Some consequences of the Karpenko–Merkurjev theorem', *Doc. Math.* Extra volume dedicated to Andrei A. Suslin sixtieth birthday (2010) 445–457.
31. H. Pinkham, 'Résolution simultanée de points doubles rationnels', *Séminaire sur les Singularités des Surfaces*, by Michel Demazure, Henry Charles Pinkham and Bernard Teissier, Lecture Notes in Mathematics 777 (Springer, Berlin, 1980) 179–203.
32. B. Poonen, 'Bertini theorems over finite fields', *Ann. of Math.* (2) 160 (2004) 1099–1127.
33. B. Poonen, 'Smooth hypersurface sections containing a given subscheme over a finite field', *Math. Res. Lett.* 15 (2008) 265–271.
34. Z. Reichstein, 'Essential dimension', *Proceedings of the International Congress of Mathematicians. Vol. II* (Hindustan Book Agency, New Delhi, 2010) 162–188.
35. Z. Reichstein, 'What is ... essential dimension?', *Notices Amer. Math. Soc.* 59 (2012) 1432–1434.
36. Z. Reichstein and B. Youssin, 'Essential dimensions of algebraic groups and a resolution theorem for G-varieties, with an appendix by J. Kollar and E. Szabo', *Canad. J. Math.* 52 (2000) 1018–1056.
37. Z. Reichstein and B. Youssin, 'Splitting fields of G-varieties', *Pacific J. Math.* 200 (2001) 207–249.
38. J.-P. Serre, 'Groupes finis d'automorphismes d'anneaux locaux réguliers', *Colloque d'Algèbre (Paris, 1967)* (Secrétariat mathématique, Paris, 1968). Exp. 8, 8.01-8.11.
39. J.-P. Serre, *Linear representations of finite groups* (Springer, New York, 1977). Translated from the second French edition by Leonard L. Scott.
40. J.-P. Serre, 'Cohomological invariants, Witt invariants, and trace forms', *Cohomological invariants in Galois cohomology*, University Lecture Series 28 (American Mathematical Society, Providence, RI, 2003) 1–100. Notes by Skip Garibaldi.
41. G. C. Shephard and J. A. Todd, 'Finite unitary reflection groups', *Canad. J. Math.* 6 (1954) 274–304.
42. T. Shioda, 'Weierstrass transformations and cubic surfaces', *Comment. Math. Univ. Sancti Pauli* 44 (1995) 109–128.
43. T. A. Springer, 'Regular elements of finite reflection groups', *Invent. Math.* 25 (1974) 159–198.

44. R. Steinberg, 'Differential equations invariant under finite reflection groups', *Trans. Amer. Math. Soc.* 112 (1964) 392–400.

45. J. H. Walter, 'The characterization of finite groups with abelian Sylow 2-subgroups', *Ann. of Math.* (2) 89 (1969) 405–514.

Alexander Duncan
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA

arduncan@umich.edu

Zinovy Reichstein
Department of Mathematics
University of British Columbia
Vancouver, BC
Canada V6T 1Z2

reichst@math.ubc.ca