ACADÉMIE
DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus

Mathématique

Oakley Edens and Zinovy Reichstein

Essential dimension of symmetric groups in prime characteristic

Volume 362 (2024), p. 639-647

Online since: 9 July 2024

https://doi.org/10.5802/crmath.577

CENTRE
MERSENNE

The Comptes Rendus. Mathématique *are a member of the*
Mersenne Center for open scientific publishing
www.centre-mersenne.org — e-ISSN : 1778-3569

ACADÉMIE DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus. Mathématique
2024, Vol. 362, p. 639-647
https://doi.org/10.5802/crmath.577

Research article / *Article de recherche*
Algebra / *Algèbre*

Essential dimension of symmetric groups in prime characteristic

Dimension essentielle du groupe symétrique en caractéristique premier

Oakley Edens [a] and Zinovy Reichstein [*,a]

[a] Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
E-mails: oedens@shaw.ca, reichst@math.ubc.ca

Abstract. The essential dimension $\mathrm{ed}_k(\mathrm{S}_n)$ of the symmetric group S_n is the minimal integer d such that the general polynomial $x^n + a_1x^{n-1} + \cdots + a_n$ can be reduced to a d-parameter form by a Tschirnhaus transformation. Finding this number is a long-standing open problem, originating in the work of Felix Klein, long before essential dimension of a finite group was formally defined. We now know that $\mathrm{ed}_k(\mathrm{S}_n)$ lies between $\lfloor n/2 \rfloor$ and $n-3$ for each $n \geqslant 5$ and any field k of characteristic different from 2. Moreover, if $\mathrm{char}(k) = 0$, then $\mathrm{ed}_k(\mathrm{S}_n) \geqslant \lfloor (n+1)/2 \rfloor$ for any $n \geqslant 7$. The value of $\mathrm{ed}_k(\mathrm{S}_n)$ is not known for any $n \geqslant 8$ and any field k, though it is widely believed that $\mathrm{ed}_k(\mathrm{S}_n)$ should be $n-3$ for every $n \geqslant 5$, at least in characteristic 0. In this paper we show that for every prime p there are infinitely many positive integers n such that $\mathrm{ed}_{\mathbb{F}_p}(\mathrm{S}_n) \leqslant n-4$.

Résumé. La dimension essentielle $\mathrm{ed}_k(\mathrm{S}_n)$ du groupe symétrique S_n est le plus petit entier d permettant de réduire le polynôme général $x^n + a_1x^{n-1} + \cdots + a_n$ à une forme comportant d paramètres par une transformation de Tschirnhaus. La détermination de cette valeur est un problème ouvert depuis longtemps, remontant aux recherches de Felix Klein, bien avant que la dimension essentielle d'un groupe fini ne soit formellement définie. Nous savons que $\mathrm{ed}_k(\mathrm{S}_n)$ se situe entre $\lfloor n/2 \rfloor$ et $n-3$ pour tout entier $n \geqslant 5$ et tout corps k de caractéristique autre que 2. De plus, si $\mathrm{char}(k) = 0$, on sait que $\mathrm{ed}_k(\mathrm{S}_n) \geqslant \lfloor (n+1)/2 \rfloor$ pour tout $n \geqslant 7$. La valeur de $\mathrm{ed}_k(\mathrm{S}_n)$ est inconnue dès que $n \geqslant 8$ ceci quelque soit le corps k ; bien qu'on estime généralement que $\mathrm{ed}_k(\mathrm{S}_n)$ devrait être $n-3$ pour tout $n \geqslant 5$, au moins en caractéristique 0. Nous démontrons que pour tout nombre premier p, il existe une infinité d'entiers positifs n tels que $\mathrm{ed}_{\mathbb{F}_p}(\mathrm{S}_n) \leqslant n-4$.

Keywords. Essential dimension, symmetric group, general polynomial, group action on an algebraic variety, positive characteristic.

Mots-clés. Dimension essentielle, groupe symétrique, polynôme général, action d'un groupe sur une variété algébrique, caractéristique positive.

2020 Mathematics Subject Classification. 12E05, 14G17, 14L30, 14E05.

Funding. Oakley Edens was partially supported by an Undergraduate Student Research Award (USRA) from the National Sciences and Engineering Research Council of Canada. Zinovy Reichstein was partially supported by an Individual Discovery Grant from the National Sciences and Engineering Research Council of Canada.

Manuscript received 28 August 2023, revised 31 October 2023, accepted 9 October 2023.

[*] Corresponding author

1. Introduction

The essential dimension $\mathrm{ed}_k(\mathrm{S}_n)$ of the symmetric group S_n is the smallest integer d such that the general polynomial $x^n + a_1 x^{n-1} + \cdots + a_n$ can be reduced to a d-parameter form by a Tschirnhaus transformation. The geometric definition of essential dimension and some background material can be found in Section 2; for a comprehensive overview, see [10, 12].

Finding $\mathrm{ed}_k(\mathrm{S}_n)$ is a long-standing open problem, which goes back to F. Klein [8]; cf. also N. Chebotarev [14]. Essential dimension of a finite group was formally defined by J. Buhler and the second author in [5], where the inequalities

$$\mathrm{ed}_k(\mathrm{S}_n) \geqslant \lfloor n/2 \rfloor \qquad \text{and} \qquad \mathrm{ed}_k(\mathrm{S}_n) \leqslant n-3 \quad (n \geqslant 5) \tag{1}$$

were proved. The field k was assumed to be of characteristic 0 in [5], but the proof of the first inequality in (1) given there goes through for any field k of characteristic different from 2. The second inequality is valid over an arbitrary field k. A. Duncan [6] subsequently showed that in characteristic 0, $\mathrm{ed}_k(\mathrm{S}_n) \geqslant \lfloor (n+1)/2 \rfloor$ for any $n \geqslant 7$. The exact value of $\mathrm{ed}_k(\mathrm{S}_n)$ is open for each $n \geqslant 8$ and any field k, though it is widely believed that $\mathrm{ed}_k(\mathrm{S}_n)$ should be $n-3$ for every $n \geqslant 5$, at least in characteristic 0.

The purpose of this paper is to show that $\mathrm{ed}_k(\mathrm{S}_n)$ can be $\leqslant n-4$ in prime characteristic. Our main result is as follows.

Theorem 1. *Let k be a field of characteristic $p > 0$ and let n be a positive integer whose binary presentation is $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_r}$, where $m_1 > m_2 > \cdots > m_r \geqslant 0$. Assume that one of the following conditions holds:*

- (a) *p is odd, p divides n and $r \geqslant 4$. If $r = 4$, assume further that k contains $\mathbb{F}_{p^2}$, a field of p^2 elements.*
- (b) *$p = 2$, 4 divides n, and $r \geqslant 2$.*

Then $\mathrm{ed}_k(\mathrm{S}_n) \leqslant n-4$.

Remark 2.

- (a) If $k \subset k'$ is a field extension, then $\mathrm{ed}_k(\mathrm{S}_n) \geqslant \mathrm{ed}_{k'}(\mathrm{S}_n)$. In particular, Theorem 1 (a) is equivalent to $\mathrm{ed}_{\mathbb{F}_p}(\mathrm{S}_n) \leqslant n-4$ if $r \geqslant 5$ and $\mathrm{ed}_{\mathbb{F}_{p^2}}(\mathrm{S}_n) \leqslant n-4$ if $r = 4$ (assuming $p \mid n$). Theorem 1 (b) is equivalent to $\mathrm{ed}_{\mathbb{F}_2}(S_n) \leqslant n-4$ when n is divisible by 4 and $r \geq 2$.
- (b) It may be possible to weaken the assumptions on p and n in the statement of Theorem 1. Note, however, that these assumptions cannot be dropped entirely. Indeed, $\mathrm{ed}_k(\mathrm{S}_5) = 2$ and $\mathrm{ed}_k(\mathrm{S}_6) = 3$ for any field k of characteristic $\neq 2$; see (1). If $\mathrm{char}(k) = 2$, we still have $\mathrm{ed}_k(\mathrm{S}_5) = 2$. Here the inequality $\mathrm{ed}_k(\mathrm{S}_5) \leqslant 2$ follows from (1), and the opposite inequality from [9, Proposition 7]. We do not know whether $\mathrm{ed}_k(\mathrm{S}_6)$ is 2 or 3 in characteristic 2.
- (c) Suppose l is a field of characteristic 0 and k is a field of characteristic $p > 0$ containing an algebraic closure of $\mathbb{F}_p$. Then $\mathrm{ed}_l(\mathrm{S}_n) \geqslant \mathrm{ed}_k(\mathrm{S}_n)$ for any $n \geqslant 5$; see [4, Corollary 3.4 (b)].
- (d) The smallest n covered by Theorem 1 (a) is $n = 2^3 + 2^2 + 2^1 + 2^0 = 15$ (here $p = 3$ or 5). The smallest n covered by Theorem 1 (b) is $n = 2^3 + 2^2 = 12$. For a fixed p, the density of integers $n \geqslant 1$ to which Theorem 1 applies is positive ($1/p$ if p is odd, and $1/4$ if $p = 2$).

The remainder of this paper will be devoted to proving Theorem 1. In Section 2 we collect the background material on essential dimension that is needed for the proof. In Section 3 we introduce the S_n-invariant subvariety $X_{1,2}$ of $\mathbb{A}^n$. In Section 4 we show that under the assumptions of Theorem 1, the S_n-action on $X_{1,2}$ has maximal possible essential dimension: $\mathrm{ed}_k(X_{1,2}; \mathrm{S}_n) = \mathrm{ed}_k(\mathrm{S}_n)$. Finally, in Section 5 we complete the proof of Theorem 1 by showing that $\mathrm{ed}_k(X_{1,2}, \mathrm{S}_n) \leqslant n-4$.

2. Preliminaries on essential dimension

Throughout this paper k denotes an arbitrary base field, $\overline{k}$ denotes an algebraic closure of k, and G denotes an abstract finite group. Unless otherwise specified, algebraic varieties, morphisms, rational maps, group actions, etc., are assumed to be defined over k. We refer to a variety X with an action of G as a G-variety. We say that the G-action on X (or equivalently, the G-variety X) is

- faithful, if the induced group homomorphism $G \to \mathrm{Aut}(X)$ is injective,
- primitive, if G transitively permutes the irreducible components of $X_{\overline{k}}$,
- generically free, if there exists a dense open subset $U \subset X$ such that for every $\overline{k}$-point $u \in U$, the stabilizer $\mathrm{Stab}_G(u)$ of u in G is trivial.

A generically free action is clearly faithful. The converse holds if X is irreducible, but not in general. For example, the natural permutation action of S_n on the set of n points is primitive and faithful but not generically free. Note also that the term "primitive" is sometimes used in other ways in related contexts, in particular, in finite group theory (see, e.g., [15, §I.8]) and in algebraic dynamics (see, e.g., [16]). In this paper we will only use it in the sense defined above.

Let X be a generically free primitive G-variety. We will refer to a G-equivariant dominant rational map $X \dashrightarrow Y$ as a *G-compression*, if the G-action on Y is also generically free. The minimal dimension of Y, taken over all G-compressions $X \dashrightarrow Y$ is called the *essential dimension* of X and is denoted by $\mathrm{ed}_k(X;G)$. The largest value of $\mathrm{ed}_k(X;G)$, as X ranges over all generically free primitive G-varieties defined over k, is called the essential dimension of G over k and is denoted by $\mathrm{ed}_k(G)$.

We now recall two results about essential dimension that will be needed in the proof of Theorem 1. Note that Proposition 3 shows, in particular, that $\mathrm{ed}_k(G) < \infty$ for any G and k.

Proposition 3. *Let $G \hookrightarrow \mathrm{GL}(V)$ be a faithful finite-dimensional representation of G. Denote the underlying affine space by $\mathbb{A}(V)$. Then $\mathrm{ed}_k(G) = \mathrm{ed}_k(\mathbb{A}(V);G)$.*

For a proof, see [5, Theorem 3.1] or [1, Proposition 4.11] or [10, Propositions 3.1 and 3.11].

Following [4], we will say that a finite group G is weakly tame over a field k of characteristic $p \geqslant 0$ if G has no normal p-subgroups, other than the trivial subgroup $\{1_G\}$. If $p = 0$ (or if p does not divide $|G|$), then G is always weakly tame over k.

Proposition 4. *Suppose that a finite group G is weakly tame over a field k. Let X and Y be generically free primitive G-varieties over k. Assume that there exists a (not necessarily dominant) G-equivariant rational map $f\colon Y \dashrightarrow X^{\mathrm{sm}}$, where X^{sm} denotes the smooth locus of X. Then $\mathrm{ed}_k(X) \geqslant \mathrm{ed}_k(Y)$.*

Note that a rational map $Y \dashrightarrow X^{\mathrm{sm}}$ is the same thing as a rational map $Y \dashrightarrow X$, with the additional assumption that no component of Y maps to the singular locus of X. For a proof of Proposition 4 we refer the reader to [13, Theorem 1.6].

3. Preliminaries on the affine quadric $X_{1,2}$

Let $X_{1,2}$ be the closed S_n-invariant subvariety of $\mathbb{A}^n$ given by

$$s_1(x_1,\dots,x_n) = s_2(x_1,\dots,x_n) = 0,$$

where s_i is the ith elementary symmetric polynomial and S_n acts on $\mathbb{A}^n$ by permuting the variables in the natural way. If $\mathrm{char}(k) \neq 2$, then equivalently,

$$X_{1,2} := \left\{ (x_1,\dots,x_n) \in \mathbb{A}^n \,\middle|\, x_1 + \dots + x_n = x_1^2 + \dots + x_n^2 = 0 \right\}. \tag{2}$$

Let Δ be the discriminant locus in $\mathbb{A}^n$, i.e., the union of the hyperplanes $x_i = x_j$ taken over all pairs (i, j), where $1 \leqslant i < j \leqslant n$. Note that the symmetric group S_n acts freely (i.e., with trivial stabilizers) on $\mathbb{A}^n \setminus \Delta$.

Lemma 5. *Assume $n \geqslant 5$. Then*

(a) *the singular locus of $X_{1,2}$ is $X_{1,2} \cap D$, where D is the small diagonal in $\mathbb{A}^n$ given by $x_1 = \cdots = x_n$.*
(b) *$X_{1,2}$ is absolutely irreducible. In particular, the S_n-action on $X_{1,2}$ is primitive.*
(c) *$X_{1,2} \setminus \Delta$ is a dense open subset of $X_{1,2}$. In particular, the S_n-action on $X_{1,2}$ is generically free.*

Proof. By definition $X_{1,2}$ is the affine cone over the projective variety $\mathbb{P}(X_{1,2}) \subset \mathbb{P}^{n-1}$ given by

$$s_1(x_1,\dots,x_n) = s_2(x_1,\dots,x_n) = 0. \tag{3}$$

Thus it suffices to show that (a) the singular locus of $\mathbb{P}(X_{1,2})$ is $\mathbb{P}(\Delta)$, (b) $\mathbb{P}(X_{1,2})$ is absolutely irreducible, and (c) $\mathbb{P}(X_{1,2})$ is not contained in $\mathbb{P}(\Delta)$. If $\mathrm{char}(k) \neq 2$, then $X_{1,2}$ is cut out by (2), and these assertions are proved in [3, Lemma 2.1(b), (c) and (f), respectively].

In fact, the arguments [3, Lemma 2.1] work in any characteristic. The Jacobian matrix of the system (3) is

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ s_1 - x_1 & s_1 - x_2 & \dots & s_1 - x_n \end{pmatrix}.$$

This matrix has rank $\leqslant 1$ if and only if $x_1 = \cdots = x_n$. This proves (a). Parts (b) and (c) are deduced from (a) in the same way as in the proof of [3, Lemma 2.1]. □

4. Reduction to $X_{1,2}$

The purpose of this section is to prove the following.

Proposition 6. *Assume k and n are as in the statement of Theorem 1. Then*

$$\mathrm{ed}_k(X_{1,2};\mathrm{S}_n) = \mathrm{ed}_k(\mathrm{S}_n).$$

The essential dimension $\mathrm{ed}(X_{1,2};\mathrm{S}_n)$ is well defined because the S_n-action on $X_{1,2}$ is primitive and generically free by Lemma 5. Note that Lemma 5 applies here because our assumptions on n force it to be at least 12; see Remark 2 (d).

Our proof of Proposition 6 will be based on the following.

Lemma 7. *Assume k and n are as in the statement of Theorem 1. Let F be a field containing k and E/F be an n-dimensional étale algebra. Then there exists an element $\alpha \in E \setminus F$ such that $s_1(\alpha) = s_2(\alpha) = 0$. Here $(-1)^i s_i(\alpha)$ denotes the coefficient of λ^{n-i} in the characteristic polynomial $N_{E/F}(\lambda \cdot 1_F - \alpha)$ of α.*

Recall that an étale algebra E over F is a direct product $E_1 \times \cdots \times E_s$, where each E_i is a finite separable field extension of F. The norm function $N_{E/F}\colon E \to F$ is defined as the product $N_{E/F}(\alpha) = N_{E_1/F}(\alpha_1) \cdot N_{E_2/F}(\alpha_2) \cdot \ldots \cdot N_{E_s/F}(\alpha_s)$ for any $\alpha = (\alpha_1,\dots,\alpha_s) \in E$. For background material on étale algebras, see [2, §6].

Proof of Lemma 7. Let E^0 be the kernel of the trace map $s_1\colon E \to F$. It is an $(n-1)$-dimensional F-vector subspace of E. Since n is divisible by $p = \mathrm{char}(k) = \mathrm{char}(F)$, F is contained in E^0. Consider the quadratic form $s_2\colon E^0 \to F$. Substituting $\alpha + t \cdot 1_F$ in place of α into the characteristic polynomial $N_{E/F}(\lambda \cdot 1_F - \alpha)$, we obtain

$$s_2(\alpha + t \cdot 1_F) = s_2(\alpha) + (n-1)\, t s_1(\alpha) + \binom{n}{2} t^2.$$

For any $\alpha \in E^0$ we have $s_1(\alpha) = 0$. Moreover, the assumptions on n and $p = \mathrm{char}(k)$ imply that $\binom{n}{2} = 0$ in k, in either part (a) or part (b). We conclude that $s_2(\alpha + t \cdot 1_F) = s_2(\alpha)$ for any $\alpha \in E^0$ and $t \in F$. In other words, the quadratic form s_2 descends from E^0 to a quadratic form $\overline{s_2}$ on the $(n-2)$-dimensional quotient space $\overline{E^0} = E^0/(F \cdot 1)$.

Elements $\alpha \in E$ such that $s_1(\alpha) = s_2(\alpha) = 0$ are precisely the isotropic vectors of s_2 in E^0. We are looking for an element $\alpha \in E^0 \setminus F$ whose image in $\overline{E^0}$ is an isotropic vector for $\overline{s_2}$. In other words, the lemma is equivalent to the assertion that the quadratic form $\overline{s_2} \colon \overline{E^0} \to F$ is isotropic.

To show that $\overline{s_2}$ is isotropic, we appeal to Springer's theorem: If F'/F is a field extension of odd degree, then $\overline{s_2}$ is isotropic in $\overline{E^0}$ if and only if it becomes isotropic over F'. Note that Springer's Theorem is valid in arbitrary characteristic; see [7, Corollary 18.5]. By [3, Proposition 5.1] we can choose F'/F so that $[F' : F]$ is odd and $E' = E \otimes_F F'$ is an étale algebra of degree n over F' of the form $E' = E_1 \times E_2 \times \cdots \times E_r$, where E_i is an étale algebra of degree 2^{m_i} over F' for each $i = 1, \ldots, r$. After replacing F by F' and E by E', we may assume without loss of generality that, in fact,

$$E = E_1 \times E_2 \times \cdots \times E_r,$$

where E_i is an 2^{m_i}-dimensional étale algebra over F for each $i = 1, \ldots, r$. Now observe that on the r-dimensional F-subalgebra of E,

$$F \times \cdots \times F \ (r \text{ times}) \subset E_1 \times \cdots \times E_r = E,$$

s_1 and s_2 are quite transparent: $s_1(c_1, \ldots, c_r) = 2^{m_1} c_1 + \cdots + 2^{m_r} c_r$ and

$$s_2(c_1, \ldots, c_r) = \sum_{1 \leqslant i < j \leqslant r} 2^{m_i + m_j} c_i c_j + \sum_{i=1}^{r} \binom{2^{m_i}}{2} c_i^2$$

for any $c_1, \ldots, c_r \in F$. We would like to show that $\overline{s_2}$ has an isotropic vector in V/F, where

$$V = \{(c_1, \ldots, c_r) \in F \times \cdots \times F \mid s_1(c_1, \ldots, c_r) = 0\}.$$

Equivalently, we would like to show that s_2 has an isotropic vector in $V \cap H$, where H is a F-hyperplane in $F \times \cdots \times F$ (r times) which does not contain the unit element $(1, \ldots, 1)$. For example, we can take H to be the hyperplane $c_r = 0$. Explicitly, we are looking for a non-trivial solution to the system

$$\begin{cases} 2^{m_1} c_1 + \cdots + 2^{m_{r-1}} c_{r-1} = 0 \\ \sum_{1 \leqslant i < j \leqslant r-1} 2^{m_i + m_j} c_i c_j + \sum_{i=1}^{r-1} \binom{2^{m_i}}{2} c_i^2 = 0 \end{cases} \tag{4}$$

(a) Note that all the coefficients in the system (4) are integers; thus we may look for solutions in the finite field $\mathbb{F}_p$. By a theorem of Chevalley [11, Theorem 5.2.1], finite fields have property C_1. Consequently, the system (4) of two polynomials in the variables $c_1, \ldots, c_{r-1}$ of degree 1 and 2, respectively, has a non-trivial solution over $\mathbb{F}_p$, as long as $r - 1 > 1 + 2$. This completes the proof of part (a) for $r \geqslant 5$.

If $r = 4$, then we may or may not be able to find a non-trivial solution of the system (4) over $\mathbb{F}_p$, but there is certainly one over some quadratic extension of $\mathbb{F}_p$. Since $\mathbb{F}_p$ has a unique quadratic extension, $\mathbb{F}_{p^2}$, and we are assuming that k contains a copy of $\mathbb{F}_{p^2}$, the system (4) has a non-trivial solution over k and hence, over F. This completes the proof of part (a) for $r = 4$.

(b) Now suppose $\mathrm{char}(k) = 2$. By our assumption, n is divisible by 4. Hence, $m_1 > \cdots > m_{r-1} > m_r \geqslant 2$, and all of the coefficients of the system (4) are 0. Consequently, the system (4) has a non-trivial solution, e.g., $(c_1, \ldots, c_{r-1}) = (1, 0, \ldots, 0)$, whenever $r - 1 \geqslant 1$, i.e., $r \geqslant 2$. □

In the proof of Proposition 6 below, we will apply Lemma 7 to the general field extension L_n/K_n defined as follows: $K_n = k(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n$ are independent variables and L_n is an extension of K_n obtained by adjoining a root of the "general polynomial" $f(x) = x^n + a_1 x^{n-1} +$

$\cdots + a_n$ of degree n. Note that $f(x)$ is irreducible over K_n by the Eisentstein criterion. Hence, $L_n = K_n[x]/(f(x))$.

Remark 8. Lemma 7 may be viewed as a "bad characteristic variant" of [3, Corollary 10.1(c)]. When char(k) does not divide n (i.e., in "good characteristic"), Corollary 10.1(c) asserts that every étale algebra E/F has an element α satisfying $\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}_{E/F}(\alpha^2) = 0$ if and only if

$$2^{m_1}c_1 + \cdots + 2^{m_r}c_r = 2^{m_1}c_1^2 + \cdots + 2^{m_r}c_r^2 = 0.$$

for some $(0,\dots,0) \neq (c_1,\dots,c_r) \in k^r$. Here $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_r}$ is the binary presentation of n, as in Theorem 1. When k is algebraically closed, this system has a non-trivial solution if and only if $r \geqslant 3$. Note that in good characteristic the condition that $\mathrm{Tr}_{E/F}(\alpha) = 0$ automatically implies that $\alpha \not\in F$. That is, $E^0 \cap F = \{0\}$. In bad characteristic $F \subset E^0$. This complicates the proof of Lemma 7, compared to the argument in [3], and necessitates the assumption that $r \geqslant 4$ in part (a).

Remark 9. If F is an infinite field, one can always choose α in Lemma 7 so that it generates E over F, i.e., $F[\alpha] = E$. This follows from the fact that if an absolutely irreducible quadric Q defined over K has a smooth K-point, then Q is rational over K (via stereographic projection) and hence, K-points are dense in Q. Since we will not use this assertion, we leave the details of this proof as an exercise for the reader. Note also that we will only use Lemma 7 in the special case, where E/F is the general field extension L_n/K_n defined above. Since there are no intermediate fields, strictly between L_n and K_n, in this case $K_n[\alpha] = L_n$ is automatic for any $\alpha \in L_n \setminus K_n$.

Proof of Proposition 6. Denote the roots of the general polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_0$ by $x_1,\dots,x_n$. Then $a_i = (-1)^i s_i(x_1,\dots,x_n)$, where s_i denotes the ith symmetric polynomial. Since $a_1,\dots,a_n$ are algebraically independent over k, so are $x_1,\dots,x_n$. Identify K_n with $k(x_1,\dots,x_n)^{\mathrm{S}_n}$ and L_n with $K_n(x_1) = k(x_1,\dots,x_n)^{\mathrm{S}_{n-1}}$, where S_n naturally permutes $x_1,\dots,x_n$ and S_{n-1} is the stabilizer of x_1 in S_n.

It is well known that elements of L_n are in bijective correspondence with S_n-equivariant rational maps $\phi\colon \mathbb{A}^n \dashrightarrow \mathbb{A}^n$. Indeed, write $\phi(x_1,\dots,x_n) = \big(\phi_1(x_1,\dots,x_n),\dots,\phi_n(x_1,\dots,x_n)\big)$. A priori the components $\phi_1,\dots,\phi_n$ of ϕ lie in $k(x_1,\dots,x_n)$; however, since ϕ is S_n-equivariant, ϕ_1 actually lies in $k(x_1,\dots,x_n)^{\mathrm{S}_{n-1}} = L_n$. The components $\phi_1,\dots,\phi_n$ are then the S_n-translates of ϕ_1. Conversely, given $\alpha \in L_n$, we can define $\phi\colon \mathbb{A}^n \dashrightarrow \mathbb{A}^n$ by

$$\phi(x) = \big(\alpha_1(x_1,\dots,x_n),\dots,\alpha_n(x_1,\dots,x_n)\big), \tag{5}$$

where $\alpha_1,\dots,\alpha_n$ are the S_n-translates of $\alpha = \alpha_1 \in L_n$. Note that there are exactly n distinct S_n-translates if α does not lie in K_n. If α lies in K_n, then $\alpha_1 = \cdots = \alpha_n$.

Now choose $\alpha \in L_n$ as in Lemma 7, and let $\phi\colon \mathbb{A}^n \dashrightarrow \mathbb{A}^n$ be the rational S_n-equivariant map given by (5). The condition that $s_1(\alpha) = s_2(\alpha) = 0$ is equivalent to the image of ϕ being contained in $X_{1,2} \subset \mathbb{A}^n$. Since $\alpha \not\in K_n$, the general point of $\mathbb{A}^n$ maps to $X_{1,2} \setminus D$, where D is the small diagonal in $\mathbb{A}^n$ given by $x_1 = \cdots = x_n$, as in Lemma 5(c). In other words, we may think of ϕ as an S_n-equivariant map $\mathbb{A}^n \dashrightarrow X_{1,2} \setminus D$. Now recall that since $\mathbb{A}^n$ is an affine space with a linear action of S_n,

$$\mathrm{ed}_k(\mathbb{A}^n;\mathrm{S}_n) = \mathrm{ed}_k(\mathrm{S}_n) \geqslant \mathrm{ed}_k(X_{1,2};\mathrm{S}_n); \tag{6}$$

see Proposition 3. On the other hand, by Proposition 4,

$$\mathrm{ed}_k(\mathbb{A}^n;\mathrm{S}_n) \leqslant \mathrm{ed}_k(X_{1,2};\mathrm{S}_n). \tag{7}$$

Proposition 4 applies here because $X_{1,2}$ is an irreducible generically free S_n-variety, $X_{1,2} \setminus D$ is smooth (see Lemma 5), and the symmetric group S_n is weakly tame at any prime. (Once again, here $n \geqslant 12$; see Remark 2(d).)

Combining (6) and (7), we obtain the desired equality, $\mathrm{ed}_k(\mathrm{S}_n) = \mathrm{ed}_k(X_{1,2};\mathrm{S}_n)$. □

5. Conclusion of the proof of Theorem 1

In this section we complete the proof of Theorem 1 by establishing the following.

Proposition 10. *Let k be a base field of characteristic $p > 0$. Assume that $n \geqslant 5$ and p divides n. If $p = 2$, assume further that 4 divides n. Then $\mathrm{ed}_k(X_{1,2}; \mathrm{S}_n) \leqslant n-4$.*

Note that the assumptions of Theorem 1 that $r \geqslant 4$ and $r \geqslant 2$ in parts (a) and (b), respectively, are not needed here.

Before proceeding with the proof of Proposition 10, we briefly outline our overall strategy. Our goal is to show the existence of an S_n-compression $\pi\colon X_{1,2} \dashrightarrow Y$ defined over k, where $\dim(Y) \leqslant n-4$. Key to our construction is the observation that $X_{1,2}$ admits an action of a certain 2-dimensional linear algebraic group B, which commutes with the S_n-action. This B-action is a characteristic p phenomenon, it only exists when $\mathrm{char}(k)$ divides both n and $\binom{n}{2}$; see Remark 12. The idea is then to define π as the quotient map for this action. The remainder of this section will be devoted to working out the details of this construction.

We begin by introducing the 2-dimensional algebraic group B: it is the group of upper-triangular matrices in PGL_2, i.e., the group of matrices of the form $\left(\begin{smallmatrix} \alpha & \beta \\ 0 & 1 \end{smallmatrix}\right)$. Note that B is a Borel subgroup of PGL_2; this is why we chose the letter "B". Consider the natural action of B on $\mathbb{A}^n$ by

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} : (x_1, \dots, x_n) \to (\alpha x_1 + \beta, \dots, \alpha x_n + \beta).$$

Lemma 11. *Assume $p = \mathrm{char}(k)$ divides n. If $p = 2$, assume further that 4 divides n. Then*

(a) *$X_{1,2} \subset \mathbb{A}^n$ is invariant under the action of B defined above.*

(b) *The stabilizer in B of a point $a = (a_1, \dots, a_n) \in X_{1,2} \setminus \Delta$ is trivial.*

Proof.

(a). For $a = (a_1, \dots, a_n) \in \mathbb{A}^n(\overline{k})$, let $s_i(a)$ be the ith elementary symmetric polynomial in $a_1, \dots, a_n$. By definition, a lies on $X_{1,2}$ if and only if $s_1(a) = s_2(a) = 0$. Thus we need to check that $s_1(a) = s_2(a) = 0$ implies $s_1(g \cdot a) = s_2(g \cdot a) = 0$, for any $a = (a_1, \dots, a_n) \in \mathbb{A}^n(\overline{k})$ and any $g = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & 1 \end{smallmatrix}\right) \in B$. Indeed, assume that $s_1(a) = s_2(a) = 0$. Under our assumptions on $p = \mathrm{char}(k)$ and n,

$$s_1(g \cdot a) = s_1(\alpha a_1 + \beta, \dots, \alpha a_n + \beta) = \alpha s_1(a) + n\beta = 0 + 0 = 0 \tag{8}$$

and

$$s_2(g \cdot a) = s_2(\alpha a_1 + \beta, \dots, \alpha a_n + \beta) = \alpha^2 s_2(a) + \alpha\beta(n-1)s_1(a) + \binom{n}{2}\beta^2 = 0 + 0 + 0 = 0, \tag{9}$$

as desired.

(b). The stabilizer of any point $a = (a_1, \dots, a_n) \in \mathbb{A}^n(\overline{k})$ is the group subscheme of B cut out by the equations

$$\begin{cases} \alpha a_1 + \beta = a_1, \\ \dots \\ \alpha a_n + \beta = a_n. \end{cases} \tag{10}$$

Here $a_1, \dots, a_n \in \overline{k}$ are fixed, and α and β are coordinate functions on B. Rewriting this system in matrix form, we obtain

$$(\alpha - 1, \beta) \cdot \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 1 & \dots & 1 \end{pmatrix} = \begin{pmatrix} 0 & \dots & 0 \end{pmatrix}.$$

If $a \notin D \subset \Delta$, i.e., at least two of the elements $a_1, \ldots, a_n$ of k are distinct, then the $2 \times n$ matrix $\left(\begin{smallmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 1 & \cdots & 1 \end{smallmatrix}\right)$ has rank 2. Hence, the kernel of this matrix is trivial. We conclude that the (scheme-theoretic) solution set to the system (10) consists of a single point, $(\alpha, \beta) = (1, 0)$. In other words, the stabilizer of a in B is trivial. □

Remark 12. For an arbitrary field k, formulas (8) and (9) tell us that $X_{1,2}$ is invariant under the action of B if and only if $n\beta = \binom{n}{2}\beta^2 = 0$ for every $\beta \in \overline{k}$. This condition is satisfied if and only if either $p = \mathrm{char}(k)$ is odd and p divides n or $p = 2$ and 4 divides n.

We now define the S_n-equivariant morphism $\pi\colon (X_{1,2} \setminus \Delta) \to \mathbb{A}^{n(n-1)(n-2)}$ by

$$\pi\colon a = (x_1, \ldots, x_n) \mapsto \left(\frac{x_r - x_s}{x_r - x_t}\right)_{(r,s,t)}$$

where the subscript (r, s, t) ranges over the $n(n-1)(n-2)$ ordered triples of distinct integers in $\{1, 2, \ldots, n\}$, and S_n acts on these triples in the natural way. Clearly, each $\frac{x_r - x_s}{x_r - x_t}$ is a regular function on $X_{1,2} \setminus \Delta$. Letting Y be the Zariski closure of the image of π in $\mathbb{A}^{n(n-1)(n-2)}$, we may view π as an S_n-equivariant dominant rational map $X_{1,2} \dashrightarrow Y$. The following lemma completes the proof of Proposition 10.

Lemma 13. *Assume $n \geqslant 5$, $p = \mathrm{char}(k)$ divides n. If $p = 2$, assume further that 4 divides n. Then*

(a) S_n *acts faithfully on Y, and*
(b) $\dim(Y) \leqslant n - 4$.

Proof.

(a). Assume the contrary. The kernel N of this action is a non-trivial normal subgroup of S_n. Since $n \geqslant 5$, N is either the alternating group A_n or the full symmetric group S_n. In both cases A_n acts trivially on $\pi(a)$ for every $a = (a_1, \ldots, a_n) \in X_{1,2} \setminus \Delta$. In particular, the 3-cycle $\sigma = (2, 4, 5) \in \mathrm{A}_n$ preserves $\pi(a)$. That is,

$$\frac{a_1 - a_2}{a_1 - a_3} = \sigma \cdot \frac{a_1 - a_2}{a_1 - a_3} = \frac{a_1 - a_4}{a_1 - a_3}. \tag{11}$$

This implies $a_2 = a_4$, which contradicts our assumption that $a \notin \Delta$.

(b). Note that π sends every B-orbit to a point. By Lemma 11(b), a general orbit of B in $X_{1,2}$ is 2-dimensional. Hence, a general fiber of π is of dimension $\geqslant 2$. By the Fiber Dimension Theorem, $\dim(Y) \leqslant \dim(X_{1,2}) - 2 = n - 4$. □

Remark 14. As we suggested at the beginning of this section, π is, in fact, a rational quotient for the B-action on $X_{1,2}$. We do not need to know this though; the explicit formula in (11) suffices for the purpose of proving Proposition 10.

Acknowledgements

We are grateful to Serge Cantat and the anonymous referee for helpful comments.

Declaration of interests

The authors do not work for, advise, own shares in, or receive funds from any organization that could benefit from this article, and have declared no affiliations other than their research organizations.

References

[1] G. Berhuy and G. Favi, “Essential dimension: a functorial point of view (after A. Merkurjev)”, *Doc. Math.* **8** (2003), pp. 279–330.

[2] N. Bourbaki, *Éléments de mathématique. XI. Première partie: Les structures fondamentales de l’analyse. Livre II: Algèbre. Chapitre IV: Polynomes et fractions rationnelles. Chapitre V: Corps commutatifs*, Hermann, 1950, pp. ii+219+iii.

[3] M. Brassil and Z. Reichstein, “The Hermite-Joubert problem over p-closed fields”, in *Algebraic groups: structure and actions*, American Mathematical Society, 2017, pp. 31–51.

[4] P. Brosnan, Z. Reichstein and A. Vistoli, “Essential dimension in mixed characteristic”, *Doc. Math.* **23** (2018), pp. 1587–1600.

[5] J. Buhler and Z. Reichstein, “On the essential dimension of a finite group”, *Compos. Math.* **106** (1997), no. 2, pp. 159–179.

[6] A. Duncan, “Essential dimensions of A_7 and S_7”, *Math. Res. Lett.* **17** (2010), no. 2, pp. 263–266.

[7] R. Elman, N. Karpenko and A. Merkurjev, *The algebraic and geometric theory of quadratic forms*, American Mathematical Society, 2008, pp. viii+435.

[8] F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, revised edition, Dover Publications, 1956, pp. xvi+289. English translation of *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom 5ten Grade*, 1884.

[9] A. Ledet, “Finite groups of essential dimension one”, *J. Algebra* **311** (2007), no. 1, pp. 31–37.

[10] A. S. Merkurjev, “Essential dimension: a survey”, *Transform. Groups* **18** (2013), no. 2, pp. 415–481.

[11] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, Cambridge University Press, 1995, pp. viii+179.

[12] Z. Reichstein, “Essential dimension”, in *Proceedings of the International Congress of Mathematicians. Volume II*, Hindustan Book Agency, 2010, pp. 162–188.

[13] Z. Reichstein and F. Scavia, “The behavior of essential dimension under specialization”, *Épijournal de Géom. Algébr., EPIGA* **6** (2022), article no. 21 (28 pages).

[14] N. G. Tschebotaröw, “The problem of resolvents and critical manifolds”, *Izv. Akad. Nauk SSSR, Ser. Mat.* **7** (1943), pp. 123–146.

[15] H. Wielandt, *Finite permutation groups*, Academic Press Inc., 1964, pp. x+114. Translated from the German by R. Bercov.

[16] D.-Q. Zhang, “The g-periodic subvarieties for an automorphism g of positive entropy on a compact Kähler manifold”, *Adv. Math.* **223** (2010), no. 2, pp. 405–415.