Journal of Combinatorial Theory, Series A 171 (2020) 105175

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

On the minimal dimension of a finite simple group ☆,☆☆

Timothy C. Burness [a], Martino Garonzi [b], Andrea Lucchini [c]

[a] *School of Mathematics, University of Bristol, Bristol BS8 1UG, UK*
[b] *Departamento de Matemática, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Brasília-DF, 70910-900, Brazil*
[c] *Dipartimento di Matematica "Tullio Levi-Civita", Università di Padova, Via Trieste 63, 35131 Padova, Italy*

ARTICLE INFO

Article history:
Received 22 March 2019
Received in revised form 10 September 2019
Accepted 7 November 2019
Available online 20 November 2019

Keywords:
Minimal dimension
Finite simple groups
Maximal subgroups
Base size

ABSTRACT

Let G be a finite group and let $\mathcal{M}$ be a set of maximal subgroups of G. We say that $\mathcal{M}$ is irredundant if the intersection of the subgroups in $\mathcal{M}$ is not equal to the intersection of any proper subset. The minimal dimension of G, denoted $\mathrm{Mindim}(G)$, is the minimal size of a maximal irredundant set of maximal subgroups of G. This invariant was recently introduced by Garonzi and Lucchini and they computed the minimal dimension of the alternating groups. In this paper, we prove that $\mathrm{Mindim}(G) \leqslant 3$ for all finite simple groups, which is best possible, and we compute the exact value for all non-classical simple groups. We also introduce and study two closely related invariants denoted by $\alpha(G)$ and $\beta(G)$. Here $\alpha(G)$ (respectively $\beta(G)$) is the minimal size of a set of maximal subgroups (respectively, conjugate maximal subgroups) of G whose intersection coincides with the Frattini subgroup of G. Evidently, $\mathrm{Mindim}(G) \leqslant \alpha(G) \leqslant \beta(G)$. For a

☆ With an appendix by T.C. Burness and R.M. Guralnick.

☆☆ Garonzi acknowledges the support of the Fundação de Apoio à Pesquisa do Distrito Federal (FAPDF) - demanda espontânea 03/2016 and the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) - Grant numbers 302134/2018-2, 422202/2018-5. Guralnick was partially supported by NSF grant DMS-1600056. The authors thank two anonymous referees for helpful comments and suggestions, which have improved the clarity of the paper.

E-mail addresses: t.burness@bristol.ac.uk (T.C. Burness), mgaronzi@gmail.com (M. Garonzi), lucchini@math.unipd.it (A. Lucchini).

https://doi.org/10.1016/j.jcta.2019.105175
0097-3165/© 2019 Elsevier Inc. All rights reserved.

simple group G we show that $\beta(G) \leqslant 4$ and $\beta(G) - \alpha(G) \leqslant 1$, and both upper bounds are best possible.
© 2019 Elsevier Inc. All rights reserved.

1. Introduction

Let G be a finite group and let $\mathcal{M}$ be a set of maximal subgroups of G. We say that $\mathcal{M}$ is *irredundant* if the intersection of the subgroups in $\mathcal{M}$ is not equal to the intersection of any proper subset of $\mathcal{M}$. Following Fernando [19], we define the *maximal dimension* of G, denoted $\mathrm{Maxdim}(G)$, to be the maximal size of an irredundant set of maximal subgroups of G. This definition arises from the study of the maximum size $m(G)$ of an irredundant generating set for G (that is, a generating set that does not properly contain any other generating set). Indeed, it is easy to see that $m(G) \leqslant \mathrm{Maxdim}(G)$, and in [18] it is proved that the difference $\mathrm{Maxdim}(G) - m(G)$ can be arbitrarily large.

As noted in [19], work of Whiston [35] on maximal independent generating sets of the symmetric group implies that $\mathrm{Maxdim}(S_n) = n - 1$ and $\mathrm{Maxdim}(A_n) = n - 2$ for all $n \geqslant 3$. More generally, observe that if G is a nonabelian simple group then

$$3 \leqslant m(G) \leqslant \mathrm{Maxdim}(G)$$

since at least three involutions are needed to generate G. Moreover, it is worth highlighting that the maximal dimension of a simple group of Lie type G can be arbitrarily large. For example, if r denotes the twisted Lie rank of G, then a Borel subgroup is the intersection of precisely r maximal parabolic subgroups and consequently $\mathrm{Maxdim}(G) \geqslant r$.

The dual concept of *minimal dimension* was introduced by Garonzi and Lucchini in [20]. We say that an irredundant set $\mathcal{M}$ of maximal subgroups is *maximal irredundant* if it is not properly contained in any other irredundant set of maximal subgroups. Then the minimal dimension of G, denoted $\mathrm{Mindim}(G)$, is the minimal size of a maximal irredundant set. For example, if $G = S_3$ then $\mathcal{M} = \{\langle(12)\rangle, \langle(13)\rangle\}$ is maximal irredundant and $\mathrm{Mindim}(G) = 2$. Note that $\mathrm{Mindim}(G) = 1$ if and only if G is cyclic of prime-power order.

The main theorem of [20] gives the exact minimal dimension of all alternating groups. More precisely, if we define

$$\mathcal{A} = \{34, 46, 58, 86, 94, 106, 118, 134, 142, 146, \ldots\} \tag{1}$$

to be the set of integers of the form $2p$, where $p \neq 11$ is a prime and $2p - 1$ is not a prime power, then

$$\mathrm{Mindim}(A_n) = \begin{cases} 3 & \text{if } n \in \{6,7,8,11,12\} \cup \mathcal{A} \\ 2 & \text{otherwise} \end{cases}$$

for all $n \geqslant 4$.

The proof of this result relies on earlier work [9,23] on base sizes for primitive actions of alternating groups. To explain the connection, let H be a maximal subgroup of a finite group G and let $H_G = \bigcap_{g \in G} H^g$ be the core of H, so we can view G/H_G as a primitive permutation group on the set $\Omega = G/H$ of cosets of H in G. Then a subset B of Ω is a *base* for G/H_G if the pointwise stabiliser of B in G/H_G is trivial, and we define the *base size* of G, denoted $b(G,H)$, to be the minimal size of a base. Equivalently,

$$b(G,H) = \min\{|S| \,:\, S \subseteq G, \bigcap_{g \in S} H^g = H_G\}.$$

Clearly, we have

$$\mathrm{Mindim}(G/H_G) \leqslant b(G,H),$$

so an upper bound on $b(G,H)$ yields an upper bound on $\mathrm{Mindim}(G/H_G)$. This observation leads us naturally to the following definition.

Definition. Let G be a finite group, let $\mathcal{M}$ be the set of maximal subgroups of G and let $\mathcal{M}^*$ be the set of maximal subgroups H of G with $H_G = \mathrm{Frat}(G)$, the Frattini subgroup of G. Define

$$\begin{aligned} \alpha(G) &= \min\{|\mathcal{T}| \,:\, \mathcal{T} \subseteq \mathcal{M}, \bigcap_{H \in \mathcal{T}} H = \mathrm{Frat}(G)\} \\ \beta(G) &= \begin{cases} \min\{b(G,H) \,:\, H \in \mathcal{M}^*\} & \text{if } \mathcal{M}^* \neq \emptyset \\ \infty & \text{otherwise} \end{cases} \end{aligned} \tag{2}$$

and observe that $\mathrm{Mindim}(G) \leqslant \alpha(G) \leqslant \beta(G)$.

By inspecting the proof of [20, Theorem 1], we see that

$$\mathrm{Mindim}(A_n) = \alpha(A_n) = \beta(A_n)$$

for all $n \geqslant 4$. Our goal in this paper is to study the invariants $\mathrm{Mindim}(G)$, $\alpha(G)$ and $\beta(G)$ for all finite simple groups. A simplified version of our main result is the following (in part (i), we define $\mathcal{A}$ as in (1)).

Theorem 1. *Let G be a nonabelian finite simple group.*

(i) *If G is an alternating, sporadic or exceptional group of Lie type, then*

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) \leqslant 3,$$

with equality if and only if

$$G \in \{A_n,\, \mathrm{M}_{22},\, G_2(2)' \,:\, n \in \{6, 7, 8, 11, 12\} \cup \mathcal{A}\}.$$

(ii) *If G is a classical group, then either*

$$\mathrm{Mindim}(G) \leqslant \alpha(G) \leqslant \beta(G) \leqslant 3,$$

or $G = \mathrm{U}_4(2)$, $\mathrm{Mindim}(G) = \alpha(G) = 3$ and $\beta(G) = 4$.

Remark 1. Let us make some comments on the statement of Theorem 1.

(a) The set $\mathcal{A}$ is infinite. To see this, let p be a prime number such that $p \equiv 2 \pmod 3$ and $2p - 1 = q$ is a prime power. Then q is a 3-power and by combining the prime number theorem with a quantitative version of Dirichlet's theorem on arithmetic progressions, we conclude that $\mathcal{A}$ contains infinitely many numbers of the form $2p$ with $p \equiv 2 \pmod 3$. Therefore, part (i) reveals that there are infinitely many finite simple groups G with $\mathrm{Mindim}(G) = 3$. As noted in [20], it is not feasible to determine $\mathcal{A}$ explicitly (this is a formidably difficult problem in number theory).

(b) For linear groups $G = \mathrm{L}_n(q)$ we can essentially compute all three invariants precisely. Indeed, Theorem 6.4 states that if $G \neq \mathrm{L}_8(2)$ then

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = \begin{cases} 3 & \text{if } G = \mathrm{L}_2(7), \mathrm{L}_2(9), \mathrm{L}_4(2), \mathrm{L}_4(4) \\ 2 & \text{otherwise.} \end{cases}$$

For $G = \mathrm{L}_8(2)$ we have $\alpha(G) = \beta(G) = 3$, but we have been unable to compute the exact value of $\mathrm{Mindim}(G)$.

(c) Similarly, we refer the reader to Theorems 6.5, 6.7, 6.11 and 6.13 for more detailed results for the other classical groups. It is worth noting that if $G = \mathrm{PSp}_4(2^f)'$ and $f \geqslant 1$ is a 2-power, then

$$\mathrm{Mindim}(G) \leqslant \alpha(G) = \beta(G) = 3$$

so there are infinitely many simple classical groups with $\alpha(G) = 3$. Let us also highlight Theorem 6.11, which states that

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 2$$

for all orthogonal groups $G = \Omega_n(q)$ with $n \geqslant 7$ and nq odd.

(d) We have only identified two simple groups with $\alpha(G) < \beta(G)$, namely $G = \mathrm{U}_4(2)$ as noted in Theorem 1, and $G = \mathrm{Sp}_6(4)$ with $\alpha(G) = 2$ and $\beta(G) = 3$.

Corollary 2. *Let G be a nonabelian finite simple group. Then the following hold:*

(i) $\alpha(G) \leqslant 3$, *with equality for infinitely many simple groups G.*
(ii) $\beta(G) \leqslant 4$, *with equality if and only if $G = \mathrm{U}_4(2)$.*
(iii) $\beta(G) - \alpha(G) \leqslant 1$, *with equality if $G = \mathrm{U}_4(2)$ or $\mathrm{Sp}_6(4)$.*
(iv) $\alpha(G) - \mathrm{Mindim}(G) \leqslant 1$.

We do not know if equality is possible in part (iv) of Corollary 2. However, we can show that the situation is completely different for arbitrary finite groups. Indeed, in Section 8 we construct a family of soluble groups G such that the difference $\alpha(G) - \mathrm{Mindim}(G)$ is arbitrarily large.

It is natural to study the finite groups G with $\mathrm{Mindim}(G) = \mathrm{Maxdim}(G)$, which we call *minmax* groups. First observe that all nilpotent groups are minmax. Indeed, if G is nilpotent then

$$\mathrm{Mindim}(G) = \mathrm{Maxdim}(G) = \lambda(|G/\mathrm{Frat}(G)|)$$

is the number of prime divisors of $|G/\mathrm{Frat}(G)|$, counted with multiplicity. This is because if $H, M \leqslant G$ and M is maximal, then either M contains H, or $|H : H \cap M| = |G : M|$ is a prime number, so all maximal irredundant families have the same size. It is also easy to see that there are non-nilpotent minmax groups, such as S_3, A_4 and S_4. In fact, one can show that any direct product of soluble minmax groups is minmax, so there are infinitely many non-nilpotent minmax groups.

By a well-known theorem of Iwasawa [22], all unrefinable chains in the subgroup lattice of a finite group G have the same length if and only if G is supersoluble. In our case, in place of arbitrary unrefinable chains, we restrict our attention to the unrefinable chains in the sublattice generated by the maximal subgroups of G. In the context of Iwasawa's result, it is worth noting that supersoluble does not imply minmax. For instance, let p be a prime such that $p-1$ is a product of at least three distinct primes and consider the affine group $G = \mathrm{AGL}_1(p) = K{:}H$, where $K = C_p$ and $H = C_{p-1}$. Then G is a supersoluble Frobenius group with maximal complement H, so $\mathrm{Mindim}(G) = 2$. However, we have $\mathrm{Maxdim}(G) \geqslant \mathrm{Maxdim}(H) \geqslant 3$.

It seems reasonable to conjecture that every minmax group is soluble, and we see that Theorem 1 has the following corollary in support of this conjecture.

Corollary 3. *If G is a nonabelian finite simple group, then* $\mathrm{Mindim}(G) < \mathrm{Maxdim}(G)$.

Let G be a nonabelian finite simple group. In order to prove Theorem 1, our first goal is to estimate $\beta(G)$. Indeed, if there exists a maximal subgroup H of G with $b(G, H) = 2$,

then

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 2.$$

A complete classification of the simple groups G with $\beta(G) = 2$ remains out of reach, but we can appeal to an extensive literature on base sizes for primitive actions of almost simple groups (see [7,12,10,9,14,15] for example). Along the way, we also establish some new base size results, which may be of independent interest. For example, Lemma 5.7 states that $b(G, H) = 2$ when $G = G_2(q)$ and H is a maximal rank subgroup of type $\mathrm{L}_2(q) \times \mathrm{L}_2(q)$ (the bound $b(G, H) \leqslant 5$ was established in [14]).

The paper is structured as follows. In Section 2 we record some preliminary results that will be needed in the proof of Theorem 1 and we handle the sporadic and alternating groups in Sections 3 and 4, respectively. The exceptional groups of Lie type are studied in Section 5 and we state and prove our main results on classical groups in Section 6. Finally, in Section 7 we prove Corollary 3 and in Section 8 we present an example to demonstrate that there are soluble groups G such that $\alpha(G) - \mathrm{Mindim}(G)$ is arbitrarily large.

In an appendix by Burness and Guralnick, the action of the exceptional group $G_2(k)$ (either finite or algebraic) on cosets of a maximal rank subgroup of type A_1A_1 is studied in the even characteristic setting. Theorem A.1 states that this action admits a base of size 2 when k is finite, which is an essential ingredient in the proof of Lemma 5.7. The second main result, Theorem A.2, considers the case where k is an algebraically closed field and the three base measures for algebraic groups introduced in [11] are computed precisely. In particular, the base size for this action is 2, but it is shown that a generic two-point stabiliser has order 2, containing a short root element.

Finally, let us say a few words on our notation, most of which is standard. We adopt the notation from [25] for simple groups of Lie type, so we write $\mathrm{L}_n^+(q) = \mathrm{L}_n(q) = \mathrm{PSL}_n(q)$ and $E_6^-(q) = {}^2E_6(q)$, etc. We also use $\mathrm{P}\Omega_n^\epsilon(q)$ to denote a simple orthogonal group, which differs from the notation in the Atlas [17]. A cyclic group of order m is denoted by C_m (or just m) and we write $H{:}K$ for a split extension H by K. In addition, (a, b) denotes the greatest common divisor of integers a and b.

2. Preliminaries

In this section we record some preliminary results that will be needed in the proof of Theorem 1. We begin with an elementary observation, which will be used throughout the paper without further comment. Here, and for the remainder of this section, G is a finite group.

Lemma 2.1. *Suppose G has subgroups H and K with $|H||K| > |G|$. Then $H^g \cap K \neq 1$ for all $g \in G$.*

We will also need the following generalisation.

Lemma 2.2. *Suppose G has subgroups H and K and there exists a set $R \subset G$ of distinct (H, K) double coset representatives such that*

(i) $|HxK| < |H||K|$ *for all* $x \in R$*; and*
(ii) $\sum_{x \in R} |HxK| > |G| - |H||K|$.

Then $H^g \cap K \neq 1$ *for all* $g \in G$.

Proof. Consider the action of K on the set Ω of right cosets of H in G. We may identify the K-orbit of Hg with the double coset HgK, so this orbit has length

$$|K : H^g \cap K| = \frac{|HgK|}{|H|}.$$

By (i), the elements in R correspond to distinct non-regular K-orbits and the inequality in (ii) implies that the union of these orbits contains more than $|\Omega| - |K|$ points. We conclude that K does not have a regular orbit on Ω and the result follows. □

Remark 2.3. Given an appropriate group G, we can use Magma [2] to implement the observation in Lemma 2.2. Indeed, this is a straightforward extension of the double coset technique discussed in [15, Section 2.3.3].

Let G be a finite group and let $x_1, \ldots, x_k$ be a set of representatives of the conjugacy classes in G of elements of prime order. Fix a core-free subgroup H of G. For $x \in G$, let

$$\mathrm{fpr}(x, G/H) = \frac{|x^G \cap H|}{|x^G|}$$

denote the *fixed point ratio* of x with respect to the standard action of G on G/H. For a positive integer c we define

$$\widehat{Q}(G, H, c) = \sum_{i=1}^{k} |x_i^G| \, \mathrm{fpr}(x_i, G/H)^c. \tag{3}$$

Now $\widehat{Q}(G, H, c)$ is an upper bound on the probability that a randomly chosen c-tuple of points in G/H does *not* form a base for G (see the proof of Theorem 1.3 in [31], for example). This immediately implies the following result, which is a standard tool for bounding the base size $b(G, H)$ using fixed point ratio estimates.

Lemma 2.4. *If* $\widehat{Q}(G, H, c) < 1$ *then* $b(G, H) \leqslant c$.

We are now ready to begin the proof of Theorem 1, which we partition into four sections according to the type of simple group we are considering. For the remainder of the paper (with the exception of Section 8), G will denote a nonabelian finite simple group and $\mathcal{M}$ is the set of maximal subgroups of G. We define $\alpha(G)$ and $\beta(G)$ as in (2).

3. Sporadic groups

Theorem 3.1. *If G is a sporadic simple group, then*

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = \begin{cases} 3 & \text{if } G = \mathrm{M}_{22} \\ 2 & \text{otherwise.} \end{cases}$$

Proof. From the information on base sizes presented in [15], we immediately deduce that

$$\beta(G) = \begin{cases} 3 & \text{if } G = \mathrm{M}_{22} \\ 2 & \text{otherwise.} \end{cases}$$

For $G = \mathrm{M}_{22}$, one checks that $|H||K| > |G|$ for any two non-conjugate subgroups $H, K \in \mathcal{M}$, so $\alpha(G) \geqslant 3$. Finally, with the aid of Magma [2], it is straightforward to verify that if A, B are distinct maximal subgroups of G, then there exists a third maximal subgroup $C \neq A, B$ such that $\{A, B, C\}$ is irredundant. This implies that $\mathrm{Mindim}(G) \geqslant 3$ and the result follows. □

4. Alternating groups

Theorem 4.1. *If $G = A_n$ with $n \geqslant 5$, then*

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = \begin{cases} 3 & \text{if } n \in \{6, 7, 8, 11, 12\} \cup \mathcal{A} \\ 2 & \text{otherwise,} \end{cases}$$

where $\mathcal{A}$ is the set of integers defined in (1).

Proof. This follows from the proof of [20, Theorem 1], but for the sake of completeness we provide a brief sketch of the main steps.

Firstly, if $5 \leqslant n \leqslant 12$ then the desired result is easily checked using Magma [2] (note that if $n \in \{6, 7, 8, 11, 12\}$, then $|H|^2 > |G|$ for all $H \in \mathcal{M}$), so we may assume $n \geqslant 13$.

By the main theorem of [9], if there exists $H \in \mathcal{M}$ such that the action of H on $\{1, \ldots, n\}$ is primitive, then $b(G, H) = 2$ and thus $\beta(G) = 2$. Therefore, we may assume that every maximal subgroup of G is either intransitive or imprimitive. By applying a theorem of J. James [23] on $b(G, H)$ for H imprimitive, we can reduce to the case where $n = 2p$ and $p \geqslant 7$ is a prime (see the proof of [20, Theorem 1] for the details of this reduction). Moreover, we have $p \neq 11$ (since $\mathrm{M}_{22} < A_{22}$ is maximal and primitive) and

$2p \neq q+1$ for a prime power q (since $\mathrm{L}_2(q) < A_{q+1}$ is maximal and primitive). We have now reduced to the case where $n \in \mathcal{A}$.

By [20, Lemma 1], each $H \in \mathcal{M}$ is either intransitive of the form $(S_k \times S_{n-k}) \cap G$, or imprimitive of the form $(S_p \wr S_2) \cap G$ or $(S_2 \wr S_p) \cap G$. In particular, one can check that $|H|^2 > |G|$ for all $H \in \mathcal{M}$, so $\alpha(G) \geqslant 3$. Moreover, if $H = (S_2 \wr S_p) \cap G$ then $b(G,H) = 3$, as noted in [9, Remark 1.6(ii)], so $\beta(G) \leqslant 3$. Finally, for each pair of subgroups $A, B \in \mathcal{M}$, it is possible to construct an explicit maximal subgroup C such that $\{A, B, C\}$ is irredundant (see the final step in the proof of [20, Theorem 1]). This shows that $\mathrm{Mindim}(G) \geqslant 3$ and the proof is complete. □

5. Exceptional groups

Theorem 5.1. *If G is a finite simple exceptional group of Lie type, then*

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = \begin{cases} 3 & \text{if } G = G_2(2)' \cong \mathrm{U}_3(3) \\ 2 & \text{otherwise.} \end{cases}$$

We will prove Theorem 5.1 in a sequence of lemmas. Base sizes for primitive actions of exceptional groups are studied extensively in [14], typically by combining fixed point ratio estimates with the upper bound in Lemma 2.4 (the parabolic actions are handled using character-theoretic methods). We will make extensive use of these results. We will also appeal to more recent results in [13], and we will apply work of Burness, Guralnick and Saxl [11] on base sizes for exceptional algebraic groups defined over an algebraically closed field. In addition, we establish some new base size results along the way, which may be of independent interest (see Lemmas 5.5 and 5.7). Note that the proof of the latter result, Lemma 5.7, relies on Theorem A.1 in Appendix A.

There is an extensive literature on the semisimple and unipotent conjugacy classes of simple exceptional groups (for example, [32] is a convenient source of detailed information on semisimple classes, and similarly [30] for unipotent classes). In particular, the sizes of these conjugacy classes are known and we will freely use this information in some of the proofs in this section.

Lemma 5.2. *Theorem 5.1 holds if $G = {}^2B_2(q)$ or ${}^2G_2(q)'$.*

Proof. If $G = {}^2B_2(q)$ then [14, Lemma 4.39] gives $b(G,H) = 2$ for $H = D_{2(q-1)}$. Similarly, if $G = {}^2G_2(q)$ with $q \geqslant 27$ then $b(G,H) = 2$ for $H = C_{q+1}{:}C_6$ (see [14, Lemma 4.37]). Finally, it is easy to check that $\beta(G) = 2$ when $G = {}^2G_2(3)' \cong \mathrm{L}_2(8)$. □

Lemma 5.3. *Theorem 5.1 holds if $G = E_6^{\epsilon}(q)$ or $E_7(q)$.*

Proof. First assume $G = E_6^{\epsilon}(q)$. Here $\mathcal{M}$ contains a maximal rank subgroup $H = \mathrm{L}_3^{\epsilon}(q^3).3$ (see [29, Table 5.1]) and [13, Lemma 6.6] gives $b(G,H) = 2$. Similarly, if $G = E_7(q)$ then [13, Lemma 6.5] states that $b(G,H) = 2$ for $H = (\mathrm{L}_2(q^3) \times {}^3D_4(q)).3$. □

Lemma 5.4. *Theorem 5.1 holds if $G = {}^2F_4(q)'$, ${}^3D_4(q)$ or $E_8(q)$.*

Proof. Suppose $G = E_8(q)$ and let $H = C_m{:}C_{30} \in \mathcal{M}$, where $m = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$ (see [29, Table 5.2]). Since $|x^G| > q^{58}$ for all nontrivial $x \in G$, we deduce that

$$\widehat{Q}(G, H, 2) < |H|^2 q^{-58} < 1$$

for all $q \geqslant 2$ and thus $b(G, H) = 2$ by Lemma 2.4 (see (3) for the definition of $\widehat{Q}(G, H, 2)$).

Next assume $G = {}^2F_4(q)'$, where $q = 2^{2m+1}$ and $m \geqslant 0$. If $m = 0$ then $\beta(G) = 2$ (as noted in [14, Table 11], we have $b(G, H) = 2$ for $H = A_6.2^2$), so let us assume $m \geqslant 1$ and consider $H = (C_{q+1})^2{:}\mathrm{GL}_2(3) \in \mathcal{M}$. Since $|x^G| > (q-1)q^{10}$ for all $1 \neq x \in G$, it follows that

$$\widehat{Q}(G, H, 2) < |H|^2 (q-1)^{-1} q^{-10} < 1$$

and thus $b(G, H) = 2$.

The case $G = {}^3D_4(q)$ is similar. Here we take $H = C_m{:}C_4 \in \mathcal{M}$, where $m = q^4 - q^2 + 1$. If $q = 2$ then $b(G, H) = 2$ (see [14, Table 12]), so let us assume $q \geqslant 3$. Now $|x^G| \geqslant (q^8 + q^4 + 1)(q^2 - 1) = a$ for all $1 \neq x \in G$, so $\widehat{Q}(G, H, 2) < |H|^2 a^{-1}$, which is less than 1 for $q \geqslant 4$. Finally, if $q = 3$ then $H = C_{19}{:}C_4$ and thus every element in H is semisimple. This implies that $|x^G| \geqslant q^8(q^8 + q^4 + 1) = b$ for all $x \in H$ of prime order and we deduce that $\widehat{Q}(G, H, 2) < |H|^2 b^{-1} < 1$. $\square$

Lemma 5.5. *Let $G = F_4(q)$ and let $H \in \mathcal{M}$ be a subgroup of type $\mathrm{L}_3^\epsilon(q) \times \mathrm{L}_3^\epsilon(q)$, where $(3, q - \epsilon) = 1$. Then $b(G, H) = 2$.*

Proof. By [29, Table 5.1] we have

$$H = (\mathrm{L}_3^\epsilon(q) \times \mathrm{L}_3^\epsilon(q)).2 = B.2$$

and it suffices to show that $\widehat{Q}(G, H, 2) < 1$ (see Lemma 2.4). To do this, it will be convenient to write

$$\widehat{Q}(G, H, 2) = \mathcal{U} + \mathcal{S},$$

where $\mathcal{U}$ (respectively, $\mathcal{S}$) is the contribution from unipotent (respectively, semisimple) elements.

Let $\bar{G} = F_4$ be the ambient simple algebraic group over the algebraic closure of $\mathbb{F}_q$ and let $\bar{H} = A_2\tilde{A}_2$ be the connected component of the corresponding maximal closed subgroup of $\bar{G}$ (here our notation indicates that the second A_2 factor of $\bar{H}$ is generated by short root subgroups). Let M be the natural module for A_2. It will be useful to consider the restriction of the Lie algebra $V = \mathcal{L}(\bar{G})$ to $\bar{H}$, which decomposes as follows

$$V \downarrow \bar{H} = \mathcal{L}(\bar{H}) \oplus (M \otimes S^2(M)^*) \oplus (M^* \otimes S^2(M)) = U \oplus W \oplus W^* \tag{4}$$

(see [33, Chapter 12], for example) where $S^2(M)$ denotes the symmetric-square of M. In addition, let us write $q = p^f$ with p a prime.

We begin by estimating $\mathcal{U}$. Let $x \in H$ be an element of order p. First assume $p = 2$ and $x^G \cap (H \setminus B)$ is nonempty. Here we may assume that x acts as a graph automorphism on the two A_2 factors of $\bar{H}$ and we can use the decomposition in (4) to determine the Jordan form of x on V. Indeed, we calculate that x has Jordan form $[J_2^6, J_1^4]$ on U and it interchanges W and W^*, so it has Jordan form $[J_2^{24}, J_1^4]$ on V (here J_i denotes a standard unipotent Jordan block of size i). By inspecting [26, Table 4], we conclude that x is in the G-class labelled $A_1\tilde{A}_1$ in [30, Table 22.2.4]. Now $\mathrm{L}_3^\epsilon(q)$ has a unique class of involutions (comprising root elements) and the G-class of each involution in B is transparent. For example, if x is in the G-class labelled A_1 (that is, x is a long root element in G), then $x^G \cap H$ comprises the set of involutions in the first $\mathrm{L}_3^\epsilon(q)$ factor of B and thus

$$|x^G \cap H| = \frac{|\mathrm{SL}_3^\epsilon(q)|}{q^3(q-\epsilon)} = (q+\epsilon)(q^3-\epsilon) < 2q^4 = a_1 = a_2$$

and $|x^G| > q^{16} = b_1 = b_2$. The same bounds apply if x is in the $\tilde{A}_1$ class. Finally, for x in the class labelled $A_1\tilde{A}_1$ we get

$$|x^G \cap H| = \left(\frac{|\mathrm{SL}_3^\epsilon(q)|}{|\mathrm{Sp}_2(q)|}\right)^2 + \left(\frac{|\mathrm{SL}_3^\epsilon(q)|}{q^3(q-\epsilon)}\right)^2 < 2q^{10} = a_3$$

and $|x^G| > q^{28} = b_3$.

Now assume p is odd, so $x^G \cap H \subseteq B$. By inspecting [27, Section 4.7], we deduce that the contribution to $\mathcal{U}$ from the unipotent elements in the classes A_1, $\tilde{A}_1$ and $A_1\tilde{A}_1$ is at most $\sum_{i=1}^3 a_i^2 b_i^{-1}$, where the a_i and b_i terms are defined as above. For the remaining elements $x \in G$ of order p, we have $|x^G| > \frac{1}{4}q^{30} = b_4$ and we note that B contains precisely $q^{12} = a_4$ unipotent elements. Therefore, for any p, we conclude that

$$\mathcal{U} < \sum_{i=1}^{4} a_i^2 b_i^{-1}.$$

Now let us turn to $\mathcal{S}$ and let $x \in H$ be an element of prime order $r \neq p$. Set $\bar{D} = C_{\bar{G}}(x)$. First assume $r = 2$, so $\bar{D} = B_4$ or A_1C_3. Suppose $x^G \cap (H \setminus B)$ is nonempty. As before, at the level of algebraic groups, we may assume x induces a graph automorphism on the two A_2 factors of $\bar{H}$ and by considering the decomposition in (4), we can determine the dimension of the 1-eigenspace of x on V, which coincides with the dimension of $\bar{D}$ (see [16, Section 1.14]). Indeed, x interchanges W and W^*, and it has a 6-dimensional 1-eigenspace on $\mathcal{L}(\bar{H})$ (since the centraliser of a graph automorphism of A_2 is 3-dimensional). It follows that $\dim C_V(x) = 24$ and thus $\bar{D} = A_1C_3$. Similarly, we can use (4) to determine the

G-class of each involution in B, noting that $\mathrm{L}_3^\epsilon(q)$ has a unique class of involutions, with size

$$\frac{|\mathrm{GL}_3^\epsilon(q)|}{|\mathrm{GL}_2^\epsilon(q)||\mathrm{GL}_1^\epsilon(q)|} = q^2(q^2+\epsilon q+1).$$

In this way, we deduce that if $\bar{D} = B_4$, then

$$|x^G \cap H| = q^2(q^2+\epsilon q+1) < 2q^4 = c_1, \quad |x^G| > q^{16} = d_1.$$

Similarly, if $\bar{D} = A_1C_3$, then

$$|x^G \cap H| = \left(\frac{|\mathrm{SL}_3^\epsilon(q)|}{|\mathrm{SO}_3(q)|}\right)^2 + q^2(q^2+\epsilon q+1)(1+q^2(q^2+\epsilon q+1)) < 2q^{10} = c_2$$

and $|x^G| > q^{28} = d_2$.

Finally, let us assume $r \geqslant 3$, so $x^G \cap H \subseteq B$. If $\dim x^{\bar{G}} \geqslant 36$, then $|x^G| > (q-1)q^{35} = d_3$ and we note that $|B| < q^{16} = c_3$. Now assume $\dim x^{\bar{G}} < 36$, in which case $\bar{D} = B_3T_1$ or C_3T_1, and $|x^G| > (q-1)q^{29} = d_4$. Note that $\dim C_V(x) = 22$. Write $x = x_1x_2 \in \bar{H}$, where $x_1 \in A_2$ and $x_2 \in \tilde{A}_2$. If both x_1 and x_2 are nontrivial, then using [31, Lemma 3.7], we deduce that $\dim C_W(x) = \dim C_{W^*}(x) \leqslant 6$, whence $\dim C_V(x) \leqslant 16$, a contradiction. Therefore, one of x_1 or x_2 is trivial and there are fewer than $2|\mathrm{L}_3^\epsilon(q)| < 2q^8 = c_4$ such elements in H.

Putting all of the above estimates together, we conclude that

$$\widehat{Q}(G,H,2) < \sum_{i=1}^{4} a_i^2 b_i^{-1} + \sum_{i=1}^{4} c_i^2 d_i^{-1} < 1$$

and thus $b(G,H) = 2$ as claimed. □

Corollary 5.6. *Theorem 5.1 holds if $G = F_4(q)$.*

To complete the proof of Theorem 5.1 we may assume $G = G_2(q)'$. The key result is the following lemma, which states that $b(G,H) = 2$ for a maximal rank subgroup H of type $\mathrm{L}_2(q) \times \mathrm{L}_2(q)$. Here $\widehat{Q}(G,H,2) > 1$ so the probabilistic approach via Lemma 2.4 is ineffective and we need to argue differently. For q odd we can appeal to [11] where the corresponding action of the ambient simple algebraic group is studied (here it is important to note that H is the centraliser of an involution). For q even, this technique is not available and an entirely different approach is required (see Theorem A.1 in Appendix A).

Lemma 5.7. *Let $G = G_2(q)$, $q \geqslant 3$ and let $H \in \mathcal{M}$ be a subgroup of type $\mathrm{L}_2(q) \times \mathrm{L}_2(q)$. Then $b(G,H) = 2$.*

Proof. The case q even is handled in Appendix A (see Theorem A.1), so let us assume q is odd, in which case $H = C_G(x)$ for an involution $x \in G$. Let $\bar{G} = G_2(k)$ be the ambient simple algebraic group, where k is the algebraic closure of $\mathbb{F}_q$, and let σ be a Frobenius morphism of $\bar{G}$ such that $\bar{G}_\sigma = G$. Similarly, let $\bar{H} = A_1\tilde{A}_1$ be a σ-stable subgroup of $\bar{G}$ such that $H = \bar{H}_\sigma$ (here the notation indicates that the second A_1 factor is generated by short root elements). Set $\bar{\Omega} = \bar{G}/\bar{H}$ and $\Omega = G/H$. Now σ acts on $\bar{\Omega}$ and the natural map from Ω to $\bar{\Omega}_\sigma$ is an isomorphism of H-sets, so it suffices to show that H has a regular orbit on $\bar{\Omega}_\sigma$.

By [11, Theorem 8], $\bar{H}$ has a unique regular orbit on $\bar{\Omega}$, say $\bar{\Lambda}$, and this is σ-stable by uniqueness. Since $\bar{H}$ is connected, the Lang-Steinberg theorem implies that $H = \bar{H}_\sigma$ acts transitively on $\bar{\Lambda}_\sigma$, whence $\bar{\Lambda}_\sigma$ is a regular H-orbit on $\bar{\Omega}_\sigma$ and thus $b(G, H) = 2$. □

Lemma 5.8. *Theorem 5.1 holds if $G = G_2(q)'$.*

Proof. By Lemma 5.7, we immediately deduce that

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 2$$

if $q \geqslant 3$. Finally, the case $G = G_2(2)' \cong \mathrm{U}_3(3)$ can be handled using Magma. □

This completes the proof of Theorem 5.1.

6. Classical groups

In this section we complete the proof of Theorem 1. A simplified version of our main result for classical groups is the following.

Theorem 6.1. *Let G be a finite simple classical group. Then either*

$$\mathrm{Mindim}(G) \leqslant \alpha(G) \leqslant \beta(G) \leqslant 3,$$

or $G = \mathrm{U}_4(2)$, $\mathrm{Mindim}(G) = \alpha(G) = 3$ and $\beta(G) = 4$.

Let G be a finite simple classical group with natural module V. The main result on the subgroup structure of G is due to Aschbacher [1], which states that each maximal subgroup of G belongs to one of nine subgroup collections, denoted $\mathcal{C}_1, \ldots, \mathcal{C}_8, \mathcal{S}$. The members of the $\mathcal{C}_i$ collections are defined in terms of the underlying geometry of G. For example, they include the stabilisers of appropriate subspaces of V, and suitable direct sum and tensor product decompositions. The subgroups in the collection $\mathcal{S}$ are almost simple groups acting irreducibly on V. We refer the reader to [25] for detailed information on the structure, conjugacy and maximality of the geometric subgroups comprising the $\mathcal{C}_i$ collections. A complete classification of the maximal subgroups of the low-dimensional classical groups (with $\dim V \leqslant 12$) is presented in [3]. Following [25], it

will be convenient to refer to the *type* of a maximal subgroup H of G, which gives an approximate description of the group-theoretic structure of H.

In studying the base sizes of primitive actions of a classical group it is natural to make a distinction between so-called *subspace* and *non-subspace* actions. Roughly speaking, a subspace action corresponds to the action of G on an appropriate set of subspaces of the natural module (equivalently, a point stabiliser H is contained in the $\mathcal{C}_1$ collection of reducible maximal subgroups). In this situation, the base size can be arbitrarily large. On the other hand, all non-subspace actions admit small bases. Indeed, the main theorem of [7] states that $b(G,H) \leqslant 5$ for all non-subspace actions of a simple classical group and this bound is best possible. Some additional results for certain non-subspace actions are presented in [10,24], and work to extend these results is in progress (see [12]). The ultimate aim is to determine the base size of every primitive action of an almost simple classical group.

A key tool in the proof of Theorem 6.1 is the following result from [12] on the primitive actions with the property that a point stabiliser is a field extension subgroup in Aschbacher's $\mathcal{C}_3$ collection (see [25, Table 4.3.A] for a description of the subgroups in $\mathcal{C}_3$).

Proposition 6.2. *Let G be a finite simple classical group with natural module V such that $\dim V \geqslant 6$. Let $H \in \mathcal{C}_3$ be a maximal subgroup corresponding to a field extension of prime degree k. Then $b(G,H) \leqslant 3$. More precisely, if $k \geqslant 3$ then*

$$b(G,H) = \begin{cases} 3 & \text{if } G = \mathrm{PSp}_6(q) \text{ and } H \text{ is of type } \mathrm{Sp}_2(q^3) \\ 2 & \text{otherwise.} \end{cases}$$

Proof. This is [12, Theorem 4.1]. □

We will also need the following result.

Proposition 6.3. *Let G be a finite simple classical group with natural module V such that $\dim V \geqslant 6$. Let H be a maximal subgroup of G and suppose there is a constant $\epsilon > 0$ such that*

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\epsilon}$$

for all $x \in G$ of prime order. Then $b(G,H) \leqslant \lceil \frac{4}{3\epsilon} \rceil$.

Proof. Set $c = \lceil \frac{4}{3\epsilon} \rceil$ and let $x_1, \ldots, x_k$ be representatives of the conjugacy classes in G of elements of prime order. Then Lemma 2.4 implies that

$$\widehat{Q}(G,H,c) < \sum_{i=1}^{k} |x_i^G|^{1-c\epsilon} \leqslant \sum_{i=1}^{k} |x_i^G|^{-\frac{1}{3}}$$

and this upper bound is less than 1 by [7, Proposition 2.2]. The result follows. □

6.1. Linear groups

Theorem 6.4. *Let $G = \mathrm{L}_n(q)$, where $n \geqslant 2$. If $G \neq \mathrm{L}_8(2)$ then*

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = \begin{cases} 3 & \text{if } G = \mathrm{L}_2(7), \mathrm{L}_2(9), \mathrm{L}_4(2), \mathrm{L}_4(4) \\ 2 & \text{otherwise.} \end{cases}$$

For $G = \mathrm{L}_8(2)$ we have $\mathrm{Mindim}(G) \leqslant \alpha(G) = \beta(G) = 3$.

Proof. First assume $n = 2$. If q is even, then $b(G, H) = 2$ for $H = D_{2(q-1)} \in \mathcal{M}$ (see [8, Example 2.5]), so let us assume q is odd. The cases $q \in \{5, 7, 9\}$ can be checked directly, and for $q \geqslant 11$ we have $b(G, H) = 2$ with $H = D_{q+1} \in \mathcal{M}$ (see [13, Lemma 7.10]).

Next suppose $n = 3$. The cases with $q < 5$ can be handled directly, so let us assume $q \geqslant 5$. By [3, Table 8.3], G contains a maximal $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_3$ and [24, Theorem 1.4] gives $b(G, H) = 2$. A very similar argument applies if $n = 4$ or 5 (note that the groups $\mathrm{L}_4(2) \cong A_8$ and $\mathrm{L}_4(4)$ can be handled using Magma).

Now assume $n \geqslant 6$. If n is divisible by an odd prime k, then G has a maximal $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_{n/k}(q^k)$ and Proposition 6.2 states that $b(G, H) = 2$. We have now reduced to the case where $n = 2^m$ and $m \geqslant 3$. If $m \geqslant 4$ then a $\mathcal{C}_2$-subgroup H of type $\mathrm{GL}_4(q) \wr S_{n/4}$ is maximal (see [25, Table 3.5.A]) and [24, Theorem 1.4] gives $b(G, H) = 2$. Now assume $m = 3$. Here we take a $\mathcal{C}_2$-subgroup H of type $\mathrm{GL}_2(q) \wr S_4$, which is maximal if $q \geqslant 3$ (see [3, Table 8.44]) and once again the result follows via [24, Theorem 1.4].

Finally, let us assume $G = \mathrm{L}_8(2)$ and H is a maximal subgroup of G. If H is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_4(2) \wr S_2$, then one can use Magma to show that $b(G, H) = 3$ (more precisely, we identify sufficiently many distinct (H, H) double cosets to rule out the existence of a regular H-orbit on G/H; see Lemma 2.2). If H is any other maximal subgroup, then one checks that $|H|^2 > |G|$, so $b(G, H) \geqslant 3$ and we conclude that $\beta(G) = 3$. In view of Lemma 2.1, to see that $\alpha(G) = 3$ it suffices to show that there is no $g \in G$ with $H^g \cap K = 1$, where H and K are of type $\mathrm{GL}_4(2) \wr S_2$ and $\mathrm{GL}_4(4)$, respectively (indeed, if A and B are any other non-conjugate maximal subgroups of G, then $|A||B| > |G|$). To do this, we use Magma to find sufficiently many distinct (H, K) double cosets to rule out the existence of a regular orbit of K on G/H (see Lemma 2.2). We have not been able to determine the exact value of $\mathrm{Mindim}(G)$ in this case (this is difficult since G contains 7,595,740,589 maximal subgroups). $\square$

6.2. Unitary groups

Theorem 6.5. *Let $G = \mathrm{U}_n(q)$, where $n \geqslant 3$.*

(i) *If n is divisible by an odd prime, then*

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = \begin{cases} 3 & \textit{if } G = \mathrm{U}_3(3), \mathrm{U}_3(5) \\ 2 & \textit{otherwise.} \end{cases}$$

(ii) *If n is a 2-power, then either*
  (a) $G = \mathrm{U}_4(2)$, $\mathrm{Mindim}(G) = \alpha(G) = 3$ *and* $\beta(G) = 4$, *or*
  (b) $\mathrm{Mindim}(G) \leqslant \alpha(G) \leqslant \beta(G) \leqslant 3$.

In order to prove Theorem 6.5, we will need the following technical result.

Lemma 6.6. *Let $G = \mathrm{U}_n(q)$, where $n = 2^m$ and $m \geqslant 3$. Let H be a $\mathcal{C}_2$-subgroup of G of type $\mathrm{GU}_1(q) \wr S_n$. Then*

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{4}{9}}$$

for all $x \in G$ of prime order.

Proof. Let $x \in G$ be an element of prime order r and observe that

$$H = ((C_{q+1})^{n-1}/Z).S_n = B.S_n,$$

where $Z = C_{(n,q+1)}$ is the centre of $\mathrm{SU}_n(q)$ (see [25, Proposition 4.2.9]). By the main theorem of [4], we have

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{1}{2}+\frac{1}{n}}$$

so we may assume $n \in \{8, 16\}$. In addition, we may also assume that r divides $|H|$ (otherwise $\mathrm{fpr}(x, G/H) = 0$). The cases $(n, q) = (8, 2), (8, 3)$ can be handled using Magma, so we can assume $q \geqslant 4$ if $n = 8$.

Suppose $(r, q + 1) = 1$. Then there exists a positive integer h such that $hr \leqslant n$ and

$$|x^G \cap H| \leqslant \frac{n!}{h!(n-hr)!r^h}(q+1)^{h(r-1)}, \quad |x^G| > \frac{1}{4}\left(\frac{q}{q+1}\right)^{r-1} q^a,$$

where $a = nh(r-1)(2-hr/n)$ (see the proof of [6, Proposition 2.5]). It is straightforward to check that these bounds are sufficient.

For the remainder, we may assume r divides $q+1$. In particular, x is semisimple. Let $\nu(x)$ be the codimension of the largest eigenspace of x on the natural module of G. We refer the reader to [5, Sections 3.3 and 3.4] for an explanation of the bounds on $|x^G|$ presented below.

First assume $x^G \cap H \subseteq B$. If $\nu(x) = 1$ then

$$|x^G \cap H| \leqslant n, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right) q^{2n-2}$$

and the result follows. Similarly, if $\nu(x) \geqslant 2$ then the bounds

$$|x^G \cap H| < |B| = \frac{(q+1)^{n-1}}{(n, q+1)}, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right) q^{4n-8}$$

are sufficient.

To complete the proof, we may assume r divides $q+1$ and $x^G \cap (H \setminus B)$ is nonempty. Notice that each primitive r-th root of unity occurs as an eigenvalue of x with positive multiplicity. If $\nu(x) = 1$ then $r = 2$ and the result follows since

$$|x^G \cap H| \leqslant n + (q+1)\binom{n}{2}, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right) q^{2n-2}.$$

Next assume $\nu(x) = 2$, so $r \in \{2, 3\}$. If $r = 3$ then

$$|x^G \cap H| \leqslant 2\binom{n}{2} + 2\binom{n}{3}(q+1)^2, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^2 q^{4n-6}$$

and similarly,

$$|x^G \cap H| \leqslant \binom{n}{2} + 3\binom{n}{4}(q+1)^2 + \binom{n}{2}(n-2)(q+1), \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right) q^{4n-8}$$

if $r = 2$. In both cases, one checks that the given bounds are sufficient.

Finally, let us assume $\nu(x) \geqslant 3$. Here the bounds

$$|x^G \cap H| < |H| = n!\left(\frac{(q+1)^{n-1}}{(n, q+1)}\right), \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right) q^{6n-18}$$

are sufficient unless $n = 16$ and $q = 2, 3$ (recall that we may assume $q \geqslant 4$ if $n = 8$). Suppose $(n, q) = (16, 2)$, so $r = 3$ and we note that S_n contains $b = 1191911840$ elements of order 3. For $\nu(x) \geqslant 4$ we have

$$|x^G \cap H| \leqslant (b+1).3^{n-1}, \quad |x^G| > \frac{1}{2}\left(\frac{2}{3}\right) 2^{8n-32}$$

and the result follows. Similarly, if $\nu(x) = 3$ then the bounds

$$|x^G \cap H| \leqslant (c+1).3^{n-1}, \quad |x^G| > \frac{1}{2}\left(\frac{2}{3}\right) 2^{6n-18}$$

are sufficient, where $c = 1120$ is the number of 3-cycles in S_n. Finally, if $(n, q) = (16, 3)$ then $r = 2$ and

$$|x^G \cap H| \leqslant (d+1).4^{n-2}, \quad |x^G| > \frac{1}{2}\left(\frac{3}{4}\right)3^{6n-18}$$

where $d = 46206735$ is the number of involutions in S_n. Once again, it is straightforward to check that these bounds are sufficient. $\square$

We are now ready to prove Theorem 6.5.

Proof of Theorem 6.5. First assume $n \in \{3, 5\}$. The cases $(n, q) = (3, 3)$, $(3, 5)$ and $(5, 2)$ can be handled directly. In the remaining cases, G has a maximal subgroup $H \in \mathcal{C}_3$ of type $\mathrm{GU}_1(q^n)$ (see [3, Tables 8.5 and 8.20]) and we have $b(G, H) = 2$ (see [7, Tables 2 and 3]). Similarly, if $n \geqslant 6$ is divisible by an odd prime k, then G has a maximal subgroup $H \in \mathcal{C}_3$ of type $\mathrm{GU}_{n/k}(q^k)$ and Proposition 6.2 gives $b(G, H) = 2$.

For the remainder, we may assume $n = 2^m$ with $m \geqslant 2$. Suppose $m = 2$. If $q \geqslant 4$ then G has a maximal $\mathcal{C}_2$-subgroup of type $\mathrm{GU}_1(q) \wr S_4$ and $b(G, H) = 2$ (see [7, Table 2]). The cases $q \leqslant 3$ can be checked directly with the aid of Magma. In particular, for $q = 2$ one checks that $\beta(G) = 4$, but there exist subgroups $H, K \in \mathcal{M}$ of type $\mathrm{GU}_3(q) \times \mathrm{GU}_1(q)$ and $\mathrm{GU}_1(q) \wr S_4$, respectively, such that $H \cap H^x \cap K = 1$ for some $x \in G$. Therefore, $\alpha(G) = 3$ in this case (and similarly, one checks that $\mathrm{Mindim}(G) = 3$).

Finally, let us assume $n = 2^m$ with $m \geqslant 3$ and let H be a $\mathcal{C}_2$-subgroup of type $\mathrm{GU}_1(q) \wr S_n$. By Lemma 6.6, we have

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{4}{9}}$$

for all $x \in G$ of prime order and thus $\widehat{Q}(G, H, 3) < 1$ by Proposition 6.3. In view of Lemma 2.4, we conclude that $b(G, H) \leqslant 3$. $\square$

6.3. Symplectic groups

Theorem 6.7. *Let $G = \mathrm{PSp}_n(q)'$, where $n \geqslant 4$.*

(i) *If $n = 4$ then either*
  (a) *$q = 2^f$, $f \geqslant 1$ a 2-power and $\mathrm{Mindim}(G) \leqslant \alpha(G) = \beta(G) = 3$, or*
  (b) *$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 2$.*
(ii) *If $G = \mathrm{Sp}_6(2)$ then $\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 3$.*
(iii) *If $G = \mathrm{Sp}_6(4)$ then $\mathrm{Mindim}(G) = \alpha(G) = 2$ and $\beta(G) = 3$.*
(iv) *If $n > 6$ is divisible by an odd prime, then $\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 2$.*
(v) *In all other cases, $\mathrm{Mindim}(G) \leqslant \alpha(G) \leqslant \beta(G) \leqslant 3$.*

Remark 6.8. Part (i) shows that there are infinitely many finite simple classical groups G with $\alpha(G) = \beta(G) = 3$. It also worth noting that $\mathrm{Mindim}(G) = 3$ for $G = \mathrm{Sp}_4(2)'$ and $\mathrm{Sp}_4(4)$, but we have not been able to compute the precise minimal dimension of the other groups arising in part (i)(a).

Lemma 6.9. *Theorem 6.7 holds if $n = 4$.*

Proof. Write $q = p^f$ with p a prime. First assume q is odd. The case $q = 3$ can be handled directly, so let us assume $q \geqslant 5$. Let H be a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_2(q)$ and note that H is maximal in G (see [3, Table 8.12]). We claim that $b(G, H) = 2$.

To justify the claim, first identify G/H with the set Ω of pairs $\{U, W\}$, where U and W are 2-dimensional totally isotropic subspaces such that $V = U \oplus W$ for the natural module V. Fix a symplectic basis $\{e_1, e_2, f_1, f_2\}$ for V and set $\alpha = \{U, W\} \in \Omega$, where $U = \langle e_1, e_2 \rangle$ and $W = \langle f_1, f_2 \rangle$. Working in $L = \mathrm{Sp}_4(q)$, it suffices to show that there exists $\beta = \{U', W'\} \in \Omega$ with $L_\alpha \cap L_\beta = \{\pm I_4\}$. Note that

$$L_\alpha = \left\{ \begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix}, \begin{pmatrix} 0 & -A^{-T} \\ A & 0 \end{pmatrix} : A \in \mathrm{GL}_2(q) \right\}.$$

Define

$$U' = \langle e_1, e_2 + f_2 \rangle, \quad W' = \langle e_1 + f_2, e_2 + f_1 \rangle$$

and observe that $\beta = \{U', W'\} \in \Omega$. It is now a straightforward exercise to show that $L_\alpha \cap L_\beta = \{\pm I_4\}$ and this justifies the claim.

Finally, let us assume $q = 2^f$ is even. If $q = 2$ then $G \cong A_6$ and the result follows from Theorem 4.1, so we may assume $f > 1$. If f is divisible by an odd prime k, then we can consider a subfield subgroup H of type $\mathrm{Sp}_4(q^{1/k})$ and it is straightforward to show that $b(G, H) = 2$ via Lemma 2.4 (see [7, Table 3]).

Now assume $f = 2^m$ with $m \geqslant 1$. The cases $m \in \{1, 2\}$ can be handled using Magma, so we can assume $m \geqslant 3$. Let H be a subfield subgroup of type $\mathrm{Sp}_4(q^{1/2})$. By applying Lemma 2.4, we deduce that $b(G, H) \leqslant 3$. In [28], Lawther and Saxl compute the subdegrees for the action of G on G/H (see [28, Table 2]) and we immediately deduce that H does not have a regular orbit, whence $b(G, H) \geqslant 3$ and we conclude that $b(G, H) = 3$. By inspecting [3, Table 8.14], we see that $|K|^2 > |G|$ for all other maximal subgroups $K \in \mathcal{M}$, which proves that $\beta(G) = 3$. In addition, one checks that $|H||K| > |G|$ and thus $\alpha(G) = 3$. □

Lemma 6.10. *Theorem 6.7 holds if $n \geqslant 6$.*

Proof. First assume $n = 6$. The groups with $q \leqslant 4$ can be checked directly and the case $q = 4$ merits special attention. Indeed, for $G = \mathrm{Sp}_6(4)$ we have $\beta(G) = 3$ and $\alpha(G) = 2$ since there exists $x \in G$ such that $H \cap K^x = 1$, where $H = \mathrm{Sp}_6(2)$ is a subfield subgroup and K is a $\mathcal{C}_3$-subgroup of type $\mathrm{Sp}_2(4^3)$. If $q \geqslant 5$ then G has a maximal $\mathcal{C}_3$-subgroup H of type $\mathrm{Sp}_2(q^3)$ and Proposition 6.2 gives $b(G, H) = 3$.

Now assume $n > 6$. If n is divisible by an odd prime k then G has a maximal $\mathcal{C}_3$-subgroup of type $\mathrm{Sp}_{n/k}(q^k)$ with $b(G, H) = 2$. Finally, if $n = 2^m$ with $m \geqslant 3$, then Proposition 6.2 gives $b(G, H) \leqslant 3$ for H of type $\mathrm{Sp}_{n/2}(q^2)$. The result follows. □

6.4. Orthogonal groups

Theorem 6.11. *Let $G = \Omega_n(q)$, where $n \geqslant 7$ and nq is odd. Then*

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 2.$$

Proof. Let V be the natural module for G and let $(\ ,\ )$ be the corresponding nondegenerate symmetric bilinear form on V. To begin with let us assume $n = 4m + 1$. Let

$$\{e_1, \ldots, e_m, f_1 \ldots, f_m, e_1^*, \ldots, e_m^*, f_1^*, \ldots, f_m^*, x\}$$

be a standard basis for V, where $(x, x) = 1$, $(e_i, f_i) = 1$, $(e_i^*, f_i^*) = 1$. We claim that the action of G on the set Ω of $2m$-dimensional nondegenerate subspaces of V of plus-type has a base of size 2 (recall that an orthogonal $2m$-space is of *plus-type* if it has a totally singular subspace of dimension m).

To see this, set

$$\begin{aligned} U &= \langle e_1, \ldots, e_m, f_1, \ldots, f_m \rangle \\ W &= \langle e_1 + x, f_1 + e_1^*, e_2 + f_1^*, f_2 + e_2^*, e_3 + f_2^*, \ldots, e_m + f_{m-1}^*, f_m + e_m^* \rangle \end{aligned}$$

and note that $U, W \in \Omega$. Suppose $g \in G$ stabilises U and W, so g also stabilises

$$\begin{aligned} U^\perp &= \langle x, e_1^*, \ldots, e_m^*, f_1^*, \ldots, f_m^* \rangle \\ W^\perp &= \langle f_1 - x, e_1 - f_1^*, f_2 - e_1^*, e_2 - f_2^*, f_3 - e_2^*, \ldots, f_m - e_{m-1}^*, e_m - f_m^*, e_m^* \rangle. \end{aligned}$$

Our goal is to prove that $g = 1$. Set $Z = U^\perp \cap W^\perp = \langle e_m^* \rangle$.

With respect to the basis $\{e_1, f_1, \ldots, e_m, f_m, x, e_1^*, f_1^*, \ldots, e_m^*, f_m^*\}$, we claim that g is represented by a block matrix of the form

$$\begin{pmatrix} A & 0 & 0 \\ 0 & A & \lambda \\ 0 & 0 & \mu \end{pmatrix} \tag{5}$$

for some $A \in O_{2m}^+(q)$. To see this, let us view the elements of V as column vectors and set $Y = (U + W) \cap U^\perp = \langle x, e_1^*, f_1^*, \ldots, e_m^* \rangle$. Since g stabilises U and Y, and it sends f_m^* into $U^\perp$, it follows that g is represented by a block matrix of the form

$$\begin{pmatrix} A & 0 & 0 \\ 0 & B & \lambda \\ 0 & 0 & \mu \end{pmatrix}$$

for some $A, B \in O_{2m}^+(q)$. We may define an invertible linear map $\sim$ from U to Y setting $\tilde{e}_1 = x$, $\tilde{f}_1 = e_1^*, \tilde{e}_2 = f_1^*, \ldots, \tilde{e}_m = f_{m-1}^*, \tilde{f}_m = e_m^*$. Notice that if $u \in U$ and $y \in Y$, then

$u + y \in W$ if and only if $y = \tilde{u}$. Since g stabilises W, we have $(u + \tilde{u})^g = Au + B\tilde{u} \in W$ for every $u \in U$ and this implies that $A = B$. This justifies the claim.

We record some useful observations:

(a) There exist $b_0, b_1, \ldots, b_m \in \mathbb{F}_q$ such that

$$(f_i)^g = \sum_{j=i}^{m} b_{j-i} f_j \text{ for all } i = 1, \ldots, m$$
$$(e_i^*)^g = \sum_{j=i}^{m} b_{j-i} e_j^* \text{ for all } i = 0, \ldots, m$$

where $e_0^* = x$. To prove this we apply descending induction on i.
Suppose $i = m$. Since g stabilises Z, there exists a nonzero scalar $a = b_0 \in \mathbb{F}_q$ such that $(e_m^*)^g = ae_m^*$, whence $f_m^g = af_m$. Now assume $i < m$. By induction, we have $f_{i+1}^g = \sum_{j=i+1}^{m} b_{j-i-1} f_j$, so

$$(e_i^* - f_{i+1})^g - \sum_{j=i+1}^{m} b_{j-i-1}(e_{j-1}^* - f_j) = (e_i^*)^g - \sum_{j=i+1}^{m} b_{j-i-1} e_{j-1}^* \in Z \tag{6}$$

and thus there exists $b_{m-i} \in \mathbb{F}_q$ such that the above vector equals $b_{m-i} e_m^*$, implying

$$(e_i^*)^g = \sum_{j=i}^{m} b_{j-i} e_j^*.$$

By the block matrix form of g in (5), it follows that

$$f_i^g = \sum_{j=i}^{m} b_{j-i} f_j.$$

(b) We have

$$x^g = ax + b_1 e_1^* + \ldots + b_{m-1} e_{m-1}^* + b_m e_m^*$$
$$e_1^g = ae_1 + b_1 f_1 + \ldots + b_{m-1} f_{m-1} + b_m f_m$$

(c) There exist $c_1, \ldots, c_{m-1} \in \mathbb{F}_q$ such that

$$e_i^g = \sum_{j=i}^{m} b_j f_{j-i+1} + ae_i + \sum_{j=1}^{i-1} c_j f_{m-i+j+1}$$
$$(f_{i-1}^*)^g = \sum_{j=i-1}^{m} b_j e_{j-i+1}^* + af_{i-1}^* + \sum_{j=1}^{i-1} c_j e_{m-i+j+1}^*$$

for all $i = 2, \ldots, m$. The proof is very similar to the argument in item (a).

Using $(e_i^g, e_i^g) = (e_i, e_i) = 0$ and $((f_i^*)^g, (f_i^*)^g) = (f_i^*, f_i^*) = 0$ we quickly deduce that $b_j = 0$ for all $1 \leqslant j \leqslant m$ and $c_j = 0$ for all $1 \leqslant j < m$. In addition, by applying the argument in (6) to the vector $f_m^* - e_m$ we deduce that $\lambda = 0$ and $\mu = a$ in (5), hence $g = aI_n$ and thus $a = 1$.

Now assume $n = 4m + 3$. Here a very similar argument applies and we provide a sketch. Fix a standard basis

$$\{e_1, \ldots, e_m, f_1 \ldots, f_m, e_1^*, \ldots, e_m^*, f_1^*, \ldots, f_m^*, e, f, x\}$$

for V, where $(x, x) = 1$, $(e, f) = 1$, $(e_i, f_i) = 1$, $(e_i^*, f_i^*) = 1$. Let Ω be the set of $(2m + 1)$-dimensional nondegenerate subspaces X of V with the property that $X^\perp$ has plus-type. Then G acts primitively on Ω and we claim that there is a base of size 2.

Set

$$\begin{aligned} U &= \langle x, e_1, \ldots, e_m, f_1, \ldots, f_m \rangle \\ W &= \langle x + e_1^*, e_1 + f_1^*, f_1 + e_2^*, \ldots, e_m + f_m^*, f_m + e \rangle \end{aligned}$$

and observe that $U, W \in \Omega$. Suppose $g \in G$ stabilises U and W, in which case g also stabilises

$$\begin{aligned} U^\perp &= \langle e_1^*, \ldots, e_m^*, f_1^*, \ldots, f_m^*, e, f \rangle \\ W^\perp &= \langle x - f_1^*, f_1 - e_1^*, e_1 - f_2^*, \ldots, f_m - e_m^*, e_m - f, e \rangle. \end{aligned}$$

With respect to the basis

$$\{x, e_1, f_1, \ldots, e_m, f_m, e_1^*, f_1^*, \ldots, e_m^*, f_m^*, e, f\},$$

the element g is represented by the same block matrix as in (5), where $A \in O_{2m+1}(q)$. Set $e_{m+1}^* = e$. We have the following facts:

(a) There exist $b_1, \ldots, b_m \in \mathbb{F}_q$ such that

$$(e_i^*)^g = ae_i^* + \sum_{j=1}^{m-i+1} b_j e_{i+j}^*, \quad f_{i-1}^g = af_{i-1} + \sum_{j=1}^{m-i+1} b_j f_{i+j-1}$$

for $i = 2, \ldots, m$.

(b) There exist $b_{m+1}, \ldots, b_{2m} \in \mathbb{F}_q$ such that

$$e_i^g = ae_i + \sum_{j=1}^{i-1} b_j e_{i-j} + b_i x + \sum_{j=i+1}^{m+i} b_j f_{j-i}$$

$$(f_i^*)^g = af_i^* + \sum_{j=1}^{i-1} b_j f_{i-j}^* + b_i e_1^* + \sum_{j=i+1}^{m+i} b_j e_{j-i+1}^*$$

for $i = 1, \ldots, m$.

Using $0 = (e_i, e_i) = (e_i^g, e_i^g)$ and $0 = (f_i^*, f_i^*) = ((f_i^*)^g, (f_i^*)^g)$ we deduce that $b_j = 0$ for all j. Finally, by applying the argument in (6) to the vector $f - e_m \in W^\perp$, we see that $\lambda = 0$ and $\mu = a$. Therefore $g = aI_n$ and thus $a = 1$ and $g = 1$. $\square$

For the even-dimensional orthogonal groups, we will need the following technical result. In the statement of the lemma, we work with a standard basis

$$\mathcal{B} = \{e_1, \ldots, e_m, e_1^*, \ldots, e_m^*, f_1, \ldots, f_m, f_1^*, \ldots, f_m^*\} \tag{7}$$

for the natural module V of $G = \Omega_{4m}^+(q)$, where $Q(e_i) = Q(e_i^*) = Q(f_i) = Q(f_i^*) = 0$ and $(e_i, f_j) = (e_i^*, f_j^*) = \delta_{i,j}$ (here Q is the defining quadratic form on V and $(\ ,\ )$ is the corresponding symmetric bilinear form). In addition, for a vector $e = \sum_i a_i e_i$ we define $e^* = \sum_i a_i e_i^*$, and similarly if $f = \sum_i a_i f_i$ then $f^* = \sum_i a_i f_i^*$.

Lemma 6.12. *Let $G = \Omega_{4m}^+(q)$, where $m \geqslant 2$ and q is even, and set*

$$\begin{array}{lll} E = \langle e_1, \ldots, e_m \rangle & F = \langle f_1, \ldots, f_m \rangle & W = \langle E, F \rangle \\ E^* = \langle e_1^*, \ldots, e_m^* \rangle & F^* = \langle f_1^*, \ldots, f_m^* \rangle & W^* = \langle E^*, F^* \rangle \end{array}$$

with respect to the basis $\mathcal{B}$. Fix $A, B \in \mathrm{GL}_m(q)$ such that $\langle A, B \rangle = \mathrm{GL}_m(q)$ and $I_m + A$ is invertible. Set

$$\begin{aligned} W_1 &= \langle e + (Ae)^*,\ f + f^* \ :\ e \in E,\ f \in F \rangle \\ W_2 &= \langle e + (Be)^*, f \ :\ e \in E,\ f \in F \rangle. \end{aligned}$$

Then every element of G stabilising W, W_1 and W_2 has the form

$$T_a = \begin{pmatrix} aI_{2m} & 0 \\ 0 & a^{-1}I_{2m} \end{pmatrix}$$

with respect to the basis $\mathcal{B}$, for some nonzero $a \in \mathbb{F}_q$.

Proof. First observe that W, W_1 and W_2 are nondegenerate $(2m)$-spaces of plus-type (note that W_1 is nondegenerate since $I_m + A$ is invertible). Suppose $g \in G$ stabilises W, W_1 and W_2. Then g stabilises $W \cap W_2 = F$ and the radical of $W + W_2 = \langle E, F, E^* \rangle$, which is E^*. Moreover, since g stabilises W it also stabilises $W^* = W^\perp$. Writing g in block form using the ordered basis $\mathcal{B}$ in (7) we deduce that for some $m \times m$ matrices R, S, X_1, X_2, X_3, X_4, with the X_i invertible, we have

$$g = \begin{pmatrix} X_1 & 0 & 0 & 0 \\ 0 & X_2 & 0 & S \\ R & 0 & X_3 & 0 \\ 0 & 0 & 0 & X_4 \end{pmatrix}.$$

Since g stabilises W_1 we quickly deduce that $X_3 = X_4$, $X_2 = AX_1A^{-1}$ and $R = S = 0$. Moreover, since g preserves the underlying symplectic form on V, it follows that $X_3 = X_1^{-T}$ and $X_4 = X_2^{-T}$. But $X_3 = X_4$ and we deduce that $X_1 = X_2 = AX_1A^{-1}$, in other words $X_1 = X_2$ commutes with A. Since g stabilises W_2 we quickly deduce that $X_2B = BX_2$, so $X_1 = X_2$ also commutes with B. Finally, since $\langle A, B\rangle = \mathrm{GL}_m(q)$, it follows that $X_1 = X_2 = aI_m$ for some nonzero scalar $a \in \mathbb{F}_q$ and the result follows. $\square$

We can now establish our main result for even-dimensional orthogonal groups.

Theorem 6.13. *Let $G = \mathrm{P}\Omega_n^\epsilon(q)$, where $n \geqslant 8$ is even.*

(i) *If n is divisible by an odd prime k with $n/k \geqslant 4$, then*

$$\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 2.$$

(ii) *If $G = \Omega_8^+(2)$, then* $\mathrm{Mindim}(G) = \alpha(G) = \beta(G) = 3$.

(iii) *In all other cases,* $\mathrm{Mindim}(G) \leqslant \alpha(G) \leqslant \beta(G) \leqslant 3$.

Proof. First assume n is divisible by an odd prime k with $n/k \geqslant 4$. Then G has a maximal $\mathcal{C}_3$-subgroup H of type $O_{n/k}^\epsilon(q^k)$ and Proposition 6.2 gives $b(G, H) = 2$. Therefore, we may assume that $n = 2^m$ or $2k$, where $m \geqslant 3$ and $k \geqslant 5$ is a prime.

If $n = 2^m$ with $m \geqslant 3$ then G has a maximal $\mathcal{C}_3$-subgroup H of type $O_{n/2}^\epsilon(q^2)$ and $b(G, H) \leqslant 3$ by Proposition 6.2. The special case $G = \Omega_8^+(2)$ in part (ii) of the theorem can be checked directly (here we find that $|H|^2 > |G|$ for all $H \in \mathcal{M}$).

Finally, let us assume $n = 2k$, where $k \geqslant 5$ is a prime. If $\epsilon = -$ then we can take a $\mathcal{C}_3$-subgroup H of type $\mathrm{GU}_{n/2}(q)$, in which case Proposition 6.2 gives $b(G, H) \leqslant 3$. Now assume $\epsilon = +$. If q is odd then G has a maximal $\mathcal{C}_3$-subgroup H of type $O_{n/2}(q^2)$ and the bound $b(G, H) \leqslant 3$ follows from Proposition 6.2. Now assume q is even. Let $\widetilde{V}$ be the natural module for G and let Ω be the set of nondegenerate plus-type subspaces of dimension $k+1$. Then G acts primitively on Ω and we claim that there is a base of size 3.

To see this, write $k = 2m + 1$ and $\widetilde{V} = V \perp \langle \widetilde{e}, \widetilde{f}\rangle$, where V is a nondegenerate $4m$-space of plus-type and $Q(\widetilde{e}) = Q(\widetilde{f}) = 0$ and $(\widetilde{e}, \widetilde{f}) = 1$. Fix a standard basis for V as in (7) and define the subspaces $W_0 = W$, W_1 and W_2 of V as in Lemma 6.12. Set

$$\widetilde{W_0} = W \perp \langle \widetilde{e}, \widetilde{f}\rangle, \quad \widetilde{W_1} = W_1 \perp \langle \widetilde{e}, \widetilde{f}\rangle, \quad \widetilde{W_2} = W_2 \perp \langle e_1^* + \widetilde{e}, e_2^* + \widetilde{f}\rangle$$

and observe that $\widetilde{W_i} \in \Omega$ for $i = 1, 2, 3$.

Suppose $g \in G$ stabilises $\widetilde{W}_0$, $\widetilde{W}_1$ and $\widetilde{W}_2$. We claim that $g = 1$. To see this, first observe that g stabilises the nondegenerate 2-space $\widetilde{W}_0 \cap \widetilde{W}_1 = \langle \widetilde{e}, \widetilde{f} \rangle$, so g also stabilises its orthogonal complement, namely V. Moreover g stabilises $\widetilde{W}_i \cap V = W_i$, so Lemma 6.12 implies that g acts on V as T_a for some nonzero scalar $a \in \mathbb{F}_q$, and it acts on $\langle \widetilde{e}, \widetilde{f} \rangle$ as a matrix $A \in O_2^+(q)$. There are two possibilities to consider.

(a) Suppose $A = \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}$. Here

$$(e_1^* + \widetilde{e})^g + (e_2^* + \widetilde{f})^g - a(e_1^* + \widetilde{e}) - a(e_2^* + \widetilde{f}) = (b - a)\widetilde{e} + (b^{-1} - a)\widetilde{f} \in \widetilde{W}_2,$$

which implies that $b = a = b^{-1}$, and consequently $a = b = 1$ and $g = 1$.

(b) Otherwise, $A = \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}$. In this case,

$$(e_1^* + \widetilde{e})^g + (e_2^* + \widetilde{f})^g - a(e_1^* + \widetilde{e}) - a(e_2^* + \widetilde{f}) = (b^{-1} - a)\widetilde{e} + (b - a)\widetilde{f} \in \widetilde{W}_2$$

and we deduce that $b = a = b^{-1}$ and thus $a = b = 1$. But then

$$g = \begin{pmatrix} I_{4m} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \notin \Omega_n^+(q).$$

We conclude that $g = 1$ as required. $\square$

This completes the proof of Theorem 1.

7. Proof of Corollary 3

Suppose G is a nonabelian finite simple group with $\mathrm{Maxdim}(G) = \mathrm{Mindim}(G)$. As we observed in the introduction,

$$\mathrm{Maxdim}(G) \geqslant m(G) \geqslant 3,$$

so Theorem 1 implies that $\mathrm{Maxdim}(G) = \mathrm{Mindim}(G) = m(G) = 3$.

Since $\mathrm{Maxdim}(A_n) = n-2$ and $\mathrm{Mindim}(A_5) = 2$, it follows that G is not an alternating group. If G is sporadic, then the condition $\mathrm{Mindim}(G) = 3$ implies that $G = \mathrm{M}_{22}$. However M_{22} has a maximal subgroup $H = \mathrm{L}_3(4)$ with $b(\mathrm{M}_{22}, H) = 5$ (see [15, Table 1]) and we deduce that $\mathrm{Maxdim}(\mathrm{M}_{22}) \geqslant 5$. If G is an exceptional group of Lie type, then Theorem 1 implies that $G = G_2(2)' \cong \mathrm{U}_3(3)$. By a theorem of Wagner [34], G can be generated by 4 involutions and no fewer, so $m(G) \geqslant 4$ and thus $\mathrm{Maxdim}(G) \geqslant 4$.

Finally, let us assume G is a classical group with natural module V of dimension n. Let $g \in G$ be a long root element and let $\nu(g)$ be the codimension of the 1-eigenspace of g on V. Clearly, we need at least $n/\nu(g)$ conjugates of g in order to generate G. If G

is orthogonal, then $\nu(g) = 2$ and we may assume that $n \geqslant 7$, so $\mathrm{Maxdim}(G) \geqslant m(G) \geqslant \lceil n/2 \rceil \geqslant 4$. For the remaining classical groups we have $\nu(g) = 1$, so $\mathrm{Maxdim}(G) \geqslant n$ and by applying Theorems 6.4 and 6.5 it follows that G is one of $\mathrm{L}_2(7)$, $\mathrm{L}_2(9)$ and $\mathrm{U}_3(5)$. The first two possibilities can be ruled out since $m(\mathrm{L}_2(7)) = m(\mathrm{L}_2(9)) = 4$ (see [36]). Finally, $G = \mathrm{U}_3(5)$ has a maximal subgroup $H = A_7$ and it is easy to check that $b(G, H) = 4$ (note that $|H|^3 > |G|^2$).

This completes the proof of Corollary 3.

8. A soluble example

Recall that if G is a nonabelian finite simple group, then $\alpha(G) - \mathrm{Mindim}(G) \leqslant 1$. In stark contrast, in this final section we construct a family of finite soluble groups G with the property that $\alpha(G) - \mathrm{Mindim}(G)$ can be arbitrarily large.

Let F be the free group of rank 2 and let X be the intersection of the normal subgroups N of F with $F/N \cong D_8$. It turns out that X is a 2-generated group of order 32. A concrete construction of X can be given in the following way. Let $D_8 = \langle a, b \mid a^4, b^2, abab \rangle$ and consider the subgroup X of $D_8 \times D_8 \times D_8$ generated by $x_1 = (a, b, b)$ and $x_2 = (b, ab, a)$. Note that the Frattini subgroup of X is generated by the elements

$$y_1 = x_1^2 = (a^2, 1, 1), \quad y_2 = x_2^2 = (1, 1, a^2), \quad y_3 = [x_1, x_2] = (a^2, a^2, a^2).$$

Also notice that $N_1 = \langle y_1, y_2 \rangle$, $N_2 = \langle y_1, y_1 y_2 y_3 \rangle$ and $N_3 = \langle y_2, y_1 y_2 y_3 \rangle$ are normal subgroups of X contained in $\mathrm{Frat}(X)$, with $X/N_i \cong D_8$ for all i. The dihedral group D_8 can be viewed as an irreducible subgroup of $\mathrm{GL}_2(3)$, so there exist three irreducible X-modules A_1, A_2, A_3 with $|A_i| = 9$ and $C_X(A_i) = N_i$ for all i.

Consider the semidirect product $G = (A_1 \times A_2 \times A_3){:}X$. Clearly $\mathrm{Frat}(G) = 1$. The maximal subgroups of G are divided into four families:

- $\mathcal{M}_0$, the maximal subgroups of G containing $A_1 \times A_2 \times A_3$;
- $\mathcal{M}_i$, the maximal subgroups of G supplementing A_i, for $i = 1, 2, 3$.

Claim. $\alpha(G) \geqslant 6$.

To see this, let $\mathcal{A}$ be a set of maximal subgroups of G with $\bigcap_{M \in \mathcal{A}} M = 1$. Now $\mathcal{A} \cap \mathcal{M}_i$ must be nonempty for $i = 1, 2, 3$, say $\mathcal{A}$ contains $M_i \in \mathcal{M}_i$.

We claim that there exists $a_i \in A_i$ such that $M_i = \left(\prod_{j \neq i} A_j\right) X^{a_i}$. We will do this for $i = 1$, the other cases being similar. Write $G = A{:}X$ with $A = A_1 A_2 A_3$ and let M be a maximal subgroup of G with $MA_1 = G$. Since A_1 is an abelian minimal normal subgroup of G, it follows that M is a complement of A_1. Moreover, $A_1(M \cap A) = A_1 M \cap A = G \cap A = A$ and $M \cap A \trianglelefteq G$, since $M \cap A$ is normal in M, and also in A (since A is abelian). Next observe that $[A_i, N_j] = A_i$ if $i \neq j$, which implies that $A_2 A_3 = [A, N_1] = [A_1(M \cap A), N_1] = [M \cap A, N_1] \leqslant M$. Now the quotient $G/A_2 A_3$ is a primitive soluble

group of the form $(A/A_2A_3){:}(M/A_2A_3)$ and it also equals $(A/A_2A_3){:}(A_2A_3X/A_2A_3)$. Since any two complements of the socle of a primitive soluble group are conjugate, it follows that there exists $a_1 \in A_1$ such that $M^{a_1^{-1}} = A_2A_3X$. Therefore, $M = A_2A_3X^{a_1}$. This justifies the claim.

Set $Y = M_1 \cap M_2 \cap M_3$ and observe that $Y = X^{a_1a_2a_3}$. For $i = 1, 2, 3$, let $Z_i = \bigcap_{M \notin \mathcal{M}_i} M$ be the intersection of all the maximal subgroups of G which do not belong to $\mathcal{M}_i$, and let $R_i = \bigcap_{j \neq i} N_j$. Notice that $Z_i = A_iR_i$, so $Z_i \cap M_i = R_i^{a_i} \neq 1$. Therefore, we must have $|\mathcal{A} \cap \mathcal{M}_i| \geqslant 2$ for $i = 1, 2, 3$ and consequently $\alpha(G) \geqslant 6$ as required.

Next we claim that $\mathrm{Mindim}(G) \leqslant 5$. Set $B = A_1 \times A_2 \times A_3$ and $B_i = \prod_{j \neq i} A_j$ and consider the set $\mathcal{M} = \{M_1, M_2, M_3, M_4, M_5\}$ of maximal subgroups of G, where

$$M_1 = B_1X,\ M_2 = B_2X,\ M_3 = B_3X,\ M_4 = BK_1,\ M_5 = BK_2$$

and K_1, K_2 are two different maximal subgroups of X. We claim that $\mathcal{M}$ is a maximal irredundant set of maximal subgroups of G. It is clearly irredundant, so let us focus on maximality. Let H be a maximal subgroup of G with $H \notin \mathcal{M}$. If $H \in \mathcal{M}_0$ then $H \cap M_4 \cap M_5 = M_4 \cap M_5 = B\mathrm{Frat}(X)$, so $\mathcal{M} \cup \{H\}$ is redundant. If $H \in \mathcal{M}_i$ with $i > 0$ then $M_1 \cap M_2 \cap M_3 \cap H = C_X(a)$ for some $a \in A_i$, and one of $C_X(a) \cap K_1$ and $C_X(a) \cap K_2$ is contained in $\mathrm{Frat}(X)$. So once again $\mathcal{M} \cup \{H\}$ is redundant. This proves that $\mathrm{Mindim}(G) \leqslant 5$.

Finally, let k be a positive integer and consider the direct product $\Gamma_k = G_1 \times \cdots \times G_k$ with $G_i \cong G$ for each i. By repeating the above argument, it can be easily seen that $\alpha(\Gamma_k) \geqslant 6k$ and $\mathrm{Mindim}(\Gamma_k) \leqslant 5k$, so

$$\alpha(\Gamma_k) - \mathrm{Mindim}(\Gamma_k) \geqslant k$$

can be arbitrarily large.

Appendix A. On a primitive action of G_2 (by Timothy C. Burness and Robert M. Guralnick[1])

Let $\bar{G} = G_2(k)$, where k is an algebraically closed field of characteristic $p = 2$, and let σ be a Frobenius morphism of $\bar{G}$ such that $\bar{G}_\sigma = G_2(2)$ and $\bar{G}_{\sigma^e} = G = G_2(q)$ for some positive integer $e \geqslant 2$ (so $q = 2^e$). Let $\bar{H} = A_1\tilde{A}_1$ be a σ-stable subgroup of $\bar{G}$, where the second A_1 factor is generated by short root elements, and set $H = \bar{H}_{\sigma^e}$. Up to conjugacy, we may assume that

$$H = \langle X_{3a+2b}, X_{-(3a+2b)}, X_a, X_{-a} \rangle = \mathrm{L}_2(q) \times \mathrm{L}_2(q)$$

[1] Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA.
E-mail address: guralnic@usc.edu.

where a and b are simple roots for G, with a short, b long, and $X_r = \{x_r(t) : t \in \mathbb{F}_q\}$ is the root subgroup corresponding to the root r.

Our first result settles the case q even in Lemma 5.7.

Theorem A.1. *If $g = x_b(1)x_{a+b}(1)x_{-b}(1) \in G$, then $H \cap H^g = 1$ and thus $b(G, H) = 2$.*

Proof. Set $L = H \cap H^g$ and note that $g \in \bar{G}_\sigma$. Suppose the result is false and choose e minimal so that $L \neq 1$. With the aid of Magma [2], one checks that $L = 1$ when $q = 4$, so we have $q = 2^e$ with $e \geqslant 3$. Since e is minimal, it follows that σ acts semiregularly on L, so $|L| \equiv 1 \pmod{e}$. In particular, some power of σ acts on L as a fixed point free automorphism of prime order and thus L is nilpotent.

It will be convenient to write $\bar{H} = \bar{H}_1\bar{H}_2$, where $\bar{H}_1$ and $\bar{H}_2$ are the A_1 factors of $\bar{H}$, with $\bar{H}_2$ generated by the short root subgroups X_a and X_{-a}. Observe that the σ-stable subgroup $\bar{H} \cap \bar{H}^g$ is finite. Indeed, if it is infinite, then [21, Proposition 8.1] would imply that $H \cap H^g$ is nontrivial when $q = 4$, which is not the case.

First we reduce to the case where L is a 2-group. Suppose L is not a 2-group and let $x \in L$ be a semisimple element of order $r \geqslant 3$. Suppose $r \geqslant 5$, or $r = 3$ and $C_{\bar{G}}(x) \neq A_2$. Then $Z(C_{\bar{G}}(x)) = T$ is a positive dimensional torus and $C_{\bar{G}}(x) = C_{\bar{G}}(T)$. Let S be a maximal torus of $\bar{H}$ containing x. Then $T, S \leqslant C_{\bar{G}}(T)$ and thus $T^y \leqslant S$ for some $y \in C_{\bar{G}}(T)$ (since T is contained in a maximal torus of $C_{\bar{G}}(T)$, and all such maximal tori are conjugate). Therefore, $T \leqslant S < \bar{H}$. Similarly, since $x \in \bar{H}^g$ we deduce that $T < \bar{H}^g$ and thus $T \leqslant \bar{H} \cap \bar{H}^g$. But this is not possible since $\bar{H} \cap \bar{H}^g$ is finite.

Now assume each nontrivial semisimple element $x \in L$ has order 3 with $C_{\bar{G}}(x) = A_2$. By considering the restriction

$$\mathcal{L}(\bar{G}) \downarrow \bar{H} = \mathcal{L}(\bar{H}) \oplus (M_1 \otimes S^3(M_2)),$$

where $\mathcal{L}(X)$ denotes the Lie algebra of X and M_i is the natural module for $\bar{H}_i$ (see [33, Chapter 12], for example), it is easy to see that $x \in \bar{H}_2$. Let P be the unique Sylow 3-subgroup of L. Then P is contained in a Sylow 3-subgroup of the second $\mathrm{L}_2(q)$ factor of H, which is cyclic, so $|P| = 3$ and thus $P \leqslant \bar{G}_{\sigma^2}$. It follows that

$$P \leqslant (\bar{H} \cap \bar{H}^g)_{\sigma^2},$$

but this contradicts the fact that $H \cap H^g = 1$ when $q = 4$. We have now reduced to the case where L is a 2-group. Note that $e \geqslant 3$ is odd and $|L| \geqslant 4$.

Let V be the natural 6-dimensional irreducible module for $\bar{G}$ and recall that $\bar{G}$ preserves a symplectic form on V, so we can view $\bar{G}$ as a subgroup of $\mathrm{Sp}_6(k)$. In this setting, $\bar{H}$ is the stabiliser in $\bar{G}$ of a 2-dimensional nondegenerate subspace W of V and one checks that $\langle W, W^g \rangle$ is a nondegenerate 4-space (it suffices to work over $\mathbb{F}_2$ to verify this). It follows that L fixes an orthogonal decomposition

$$V = W \perp W' \perp W'' \tag{8}$$

of V into 2-dimensional nondegenerate subspaces. Set $M = W^{\perp}$ and note that $\bar{H}$ acts irreducibly on M, whence $M = M_1 \otimes M_2$, where M_i is the natural module for $\bar{H}_i$. In particular, $\bar{H}$ acts as $\mathrm{SO}_4(k)$ on M. Therefore, the stabiliser in $\bar{H}$ of both W' and W'' is of the form $T.2$, where T is a maximal torus. But since $L < \bar{H}$ stabilises both subspaces, it follows that $|L| = 2$. This final contradiction completes the proof. $\square$

Let us consider the action of $\bar{G}$ on $\bar{\Omega} = \bar{G}/\bar{H}$ and define the base measures

$$b(\bar{G}, \bar{H}),\ b^0(\bar{G}, \bar{H}),\ b^1(\bar{G}, \bar{H})$$

as in [11]. Here $b(\bar{G}, \bar{H})$ is the *exact base size* of $\bar{G}$, which is the smallest integer c such that $\bar{\Omega}$ contains c points with trivial pointwise stabiliser. Similarly, the *connected base size*, denoted $b^0(\bar{G}, \bar{H})$, is the smallest c such that $\bar{\Omega}$ contains c points with finite pointwise stabiliser, and the *generic base size* $b^1(\bar{G}, \bar{H})$ is the minimal c such that the product variety $\bar{\Omega}^c$ contains a nonempty open subvariety U with the property that every c-tuple in U is a base for $\bar{G}$. Evidently,

$$b^0(\bar{G}, \bar{H}) \leqslant b(\bar{G}, \bar{H}) \leqslant b^1(\bar{G}, \bar{H}).$$

By [11, Lemma 3.21] we have $b^0(\bar{G}, \bar{H}) = 2$ and $b^1(\bar{G}, \bar{H}) \leqslant 3$, but $b(\bar{G}, \bar{H})$ and $b^1(\bar{G}, \bar{H})$ were not determined precisely in [11]. The following theorem resolves this ambiguity. Since the statement only involves algebraic groups, we will choose to suppress the bar notation used above.

Theorem A.2. *Let $G = G_2(k)$ defined over an algebraically closed field k of characteristic 2 and let H be a maximal rank subgroup of type $A_1\tilde{A}_1$. Consider the natural action of G on the quotient variety $\Omega = G/H$.*

(i) *There exists a nonempty open subvariety $U \subseteq \Omega \times \Omega$ such that $G_\alpha \cap G_\beta$ has order 2 and contains a short root element for all $(\alpha, \beta) \in U$.*
(ii) *We have $b(G, H) = b^0(G, H) = 2$ and $b^1(G, H) = 3$.*

Proof. Without loss of generality, we may assume that k is the algebraic closure of the field of two elements. Let H be the subgroup of G generated by the root subgroups corresponding to the roots $\pm a$, $\pm(3a + 2b)$ and let $g \in G_2(2)$ be the element defined in the statement of Theorem A.1. Set $J = H \cap H^g$ and let $J(q)$ be the set of $\mathbb{F}_q$-points in J. By Theorem A.1 we have $J(2^e) = 1$ for all positive integers e and thus $J = 1$. Therefore, $b(G, H) = 2$ and we deduce that $G_\gamma \cap G_\delta$ is finite on an open subvariety of $\Omega \times \Omega$, whence $b^0(G, H) = 2$. If (i) holds then $b^1(G, H) > 2$ and by [11, Proposition 2.5(iv)] we have $b^1(G, H) \leqslant b^0(G, H) + 1$, whence $b^1(G, H) = 3$. Thus, part (ii) follows once we have proved (i).

Let V denote the natural 6-dimensional module for G and recall that H is the stabiliser of a nondegenerate 2-space (with respect to a G-invariant symplectic form on V). Since

G acts transitively on such spaces, we can identify Ω with the set of nondegenerate 2-dimensional subspaces of V. Write $H = G_\alpha$ and let X be the 2-space corresponding to α under this identification.

Fix a diagonal involution $x \in H$ and note that x is a short root element of G. Since $x^G \cap H$ is a union of two H-classes (those in a short root subgroup of H and the diagonal involutions), it follows that $\Omega(x)$, the set of fixed points of x on Ω, is a union of two $C_G(x)$ orbits. More precisely, the two orbits are $C_G(x)\alpha$ and $C_G(x)g\alpha$, where $g \in G$ is such that $y = x^g$ is contained in a short root subgroup R of H. Note that $C_G(x)$ is a 6-dimensional irreducible variety, whence the two $C_G(x)$ orbits are irreducible varieties of dimensions 4 and 2, respectively. Let $\Omega_0(x)$ denote the 4-dimensional orbit.

Let $\beta \in C_G(x)g\alpha$ and let Y be the 2-space corresponding to β. Since $C_G(y) = C_G(R)$, it follows that $G_\alpha \cap G_\beta$ contains R and thus $\langle X, Y\rangle$ cannot be a 4-dimensional nondegenerate space (for then R would stabilise this space and its orthogonal complement, as well X and Y, whence R would act quadratically on V, which it does not). On the other hand, there is clearly a 2-dimensional nondegenerate x-invariant space W such that $\langle X, W\rangle$ is a nondegenerate 4-space. It follows that W must correspond to an element in $\Omega_0(x)$, and since the nondegeneracy of $\langle X, W\rangle$ is an open condition, we conclude that this is true for a nonempty open subvariety of $\Omega_0(x)$.

Next we claim that $H \cap G_\gamma = \langle x\rangle$ for a generic $\gamma \in \Omega_0(x)$ (that is, for all γ in a nonempty open subvariety of $\Omega_0(x)$). Let W be the 2-space corresponding to γ. Then $\langle X, W\rangle$ is nondegenerate and thus $H \cap G_\gamma$ acts quadratically on V. More precisely, we can write

$$V = X \perp V_2 \perp V_3, \tag{9}$$

where the summands are nondegenerate 2-spaces with $V_2 \subseteq \langle X, W\rangle$ and $V_3 \subseteq \langle X, W\rangle^\perp$.

Since H acts on $X^\perp$ as $\mathrm{SO}_4(k)$, any subgroup of H stabilising a decomposition as in (9) is contained in $\langle T, x\rangle$, where T is a maximal torus of H. Therefore, to justify the claim, it suffices to show that $H \cap G_\gamma$ contains no semisimple elements. If this intersection contains a semisimple element of order $r > 3$, or an element of order 3 whose centraliser is not $\mathrm{SL}_3(k)$, then the argument in the proof of Theorem A.1 shows that $H \cap G_\gamma$ contains a torus S (namely, the centre of the centraliser of such a semisimple element). However, the set of fixed points of S on Ω is at most 2-dimensional (since $C_H(S)$ has codimension at most 2 in $C_G(S)$). So for a generic $\gamma \in \Omega_0(x)$, the intersection $H \cap G_\gamma$ is either $\langle x\rangle$ as claimed, or it is isomorphic to the symmetric group S_3 (note that any elementary abelian subgroup of order 9 in H contains elements of order 3 with centraliser not equal to $\mathrm{SL}_3(k)$). The centraliser in G of such an S_3 subgroup is 3-dimensional (indeed, the centraliser of the element of order 3 is $\mathrm{SL}_3(k)$ and the involution x induces a graph automorphism on this subgroup). Since there are only finitely many H-classes of S_3 subgroups, it follows that the set of fixed points of S_3 on Ω is at most 3-dimensional and this completes the proof of the claim.

To complete the proof of the theorem, let us consider the morphism of varieties

$$f : G \times \Omega_0(x) \times \Omega_0(x) \to \Omega \times \Omega$$

given by $f(g, \beta, \gamma) = (g\beta, g\gamma)$. Consider the fibre $f^{-1}(\beta, \gamma)$, where $(\beta, \gamma) \in \Omega_0(x) \times \Omega_0(x)$. For a generic pair (β, γ), the previous claim implies that $G_\beta \cap G_\gamma = \langle x \rangle$ and so if $(g, \delta, \epsilon) \in f^{-1}(\beta, \gamma)$ then $g \in C_G(x)$. Therefore, the dimension of the fibre coincides with the dimension of $C_G(x)$, which is 6. In particular, the minimal dimension of a fibre of f is at most 6 and thus the dimension of the image of f is at least

$$14 + 4 + 4 - 6 = 16 = \dim(\Omega \times \Omega).$$

Therefore, f is dominant and for $(\delta, \epsilon) = (g\beta, g\gamma) \in \Omega \times \Omega$ we have $G_\delta \cap G_\epsilon = \langle x^g \rangle$. The result follows. □

By combining Theorem A.2 with [11, Theorem 3.13], we get the following corollary.

Corollary A.3. *Let $G = G_2(k)$ defined over an algebraically closed field k and let H be a maximal rank subgroup of type $A_1\tilde{A}_1$. Consider the natural action of G on the quotient variety $\Omega = G/H$. Then $b(G, H) = b^0(G, H) = 2$ and $b^1(G, H) = 3$.*

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, Invent. Math. 76 (1984) 469–514.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, J. Symbolic Comput. 24 (1997) 235–265.

[3] J.N. Bray, D.F. Holt, C.M. Roney-Dougal, The Maximal Subgroups of the Low-dimensional Finite Classical Groups, London Math. Soc. Lecture Note Series, vol. 407, Cambridge University Press, 2013.

[4] T.C. Burness, Fixed point ratios in actions of finite classical groups I, J. Algebra 309 (2007) 69–79.

[5] T.C. Burness, Fixed point ratios in actions of finite classical groups II, J. Algebra 309 (2007) 80–138.

[6] T.C. Burness, Fixed point ratios in actions of finite classical groups III, J. Algebra 314 (2007) 693–748.

[7] T.C. Burness, On base sizes for actions of finite classical groups, J. Lond. Math. Soc. 75 (2007) 545–562.

[8] T.C. Burness, M. Giudici, On the Saxl graph of a permutation group, Math. Proc. Cambridge Philos. Soc. (2019), https://doi.org/10.1017/S0305004118000610, in press.

[9] T.C. Burness, R.M. Guralnick, J. Saxl, On base sizes for symmetric groups, Bull. Lond. Math. Soc. 44 (2011) 386–391.

[10] T.C. Burness, R.M. Guralnick, J. Saxl, Base sizes for $\mathcal{S}$-actions of finite classical groups, Israel J. Math. 199 (2014) 711–756.

[11] T.C. Burness, R.M. Guralnick, J. Saxl, On base sizes for algebraic groups, J. Eur. Math. Soc. (JEMS) 19 (2017) 2269–2341.

[12] T.C. Burness, R.M. Guralnick, J. Saxl, Base sizes for geometric actions of finite classical groups, in preparation.

[13] T.C. Burness, S. Harper, Finite groups, 2-generation and the uniform domination number, Israel J. Math. (2019), in press.

[14] T.C. Burness, M.W. Liebeck, A. Shalev, Base sizes for simple groups and a conjecture of Cameron, Proc. Lond. Math. Soc. 98 (2009) 116–162.

[15] T.C. Burness, E.A. O'Brien, R.A. Wilson, Base sizes for sporadic groups, Israel J. Math. 177 (2010) 307–333.
[16] R.W. Carter, Finite Groups of Lie Type: Conjugacy Classes and Complex Characters, John Wiley and Sons, New York, 1985.
[17] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups, Oxford University Press, 1985.
[18] E. Detomi, A. Lucchini, Maximal subgroups of finite soluble groups in general position, Ann. Mat. Pura Appl. 195 (2016) 1177–1183.
[19] R. Fernando, On an inequality of dimension-like invariants for finite groups, preprint, arXiv:1502.00360, 2015.
[20] M. Garonzi, A. Lucchini, Maximal irredundant families of minimal size in the alternating group, Arch. Math. (Basel) 113 (2019) 119–126.
[21] D. Goldstein, R.M. Guralnick, Alternating forms and self-adjoint operators, J. Algebra 308 (2007) 330–349.
[22] K. Iwasawa, Über die endlichen Gruppen und die Verbände ihrer Untergruppen, J. Fac. Sci., Imp. Univ. Tokyo, Sect. I 4 (1941) 171–199.
[23] J.P. James, Partition actions of symmetric groups and regular bipartite graphs, Bull. Lond. Math. Soc. 38 (2006) 224–232.
[24] J.P. James, Two point stabilisers of partition actions of linear groups, J. Algebra 297 (2006) 453–469.
[25] P.B. Kleidman, M.W. Liebeck, The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.
[26] R. Lawther, Jordan block sizes of unipotent elements in exceptional algebraic groups, Comm. Algebra 23 (1995) 4125–4156.
[27] R. Lawther, Unipotent classes in maximal subgroups of exceptional algebraic groups, J. Algebra 322 (2009) 270–293.
[28] R. Lawther, J. Saxl, On the actions of finite groups of Lie type on the cosets of subfield subgroups and their twisted analogues, Bull. Lond. Math. Soc. 21 (1989) 449–455.
[29] M.W. Liebeck, J. Saxl, G.M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, Proc. Lond. Math. Soc. 65 (1992) 297–325.
[30] M.W. Liebeck, G.M. Seitz, Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras, Mathematical Surveys and Monographs, vol. 180, Amer. Math. Soc., 2012.
[31] M.W. Liebeck, A. Shalev, Simple groups, permutation groups, and probability, J. Amer. Math. Soc. 12 (1999) 497–520.
[32] F. Lübeck, Centralizers and numbers of semisimple classes in exceptional groups of Lie type, http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/CentSSClasses.
[33] A.R. Thomas, The irreducible subgroups of exceptional algebraic groups, Mem. Amer. Math. Soc. (2019), in press.
[34] A. Wagner, The minimal number of involutions generating some finite three-dimensional groups, Boll. Unione Mat. Ital. 15 (1978) 431–439.
[35] J. Whiston, Maximal independent generating sets of the symmetric group, J. Algebra 232 (2000) 255–268.
[36] J. Whiston, J. Saxl, On the maximal size of independent generating sets of $\mathrm{PSL}_2(q)$, J. Algebra 258 (2002) 651–657.