Monatshefte für Mathematik
https://doi.org/10.1007/s00605-021-01599-5

Base sizes of primitive permutation groups

Mariapia Moscatiello[1] · **Colva M. Roney-Dougal**[2]

Received: 2 June 2021 / Accepted: 22 June 2021

Abstract
Let G be a permutation group, acting on a set Ω of size n. A subset $\mathcal{B}$ of Ω is a *base* for G if the pointwise stabilizer $G_{(\mathcal{B})}$ is trivial. Let $b(G)$ be the minimal size of a base for G. A subgroup G of $\mathrm{Sym}(n)$ is *large base* if there exist integers m and $r \geq 1$ such that $\mathrm{Alt}(m)^r \trianglelefteq G \leq \mathrm{Sym}(m) \wr \mathrm{Sym}(r)$, where the action of $\mathrm{Sym}(m)$ is on k-element subsets of $\{1, \ldots, m\}$ and the wreath product acts with product action. In this paper we prove that if G is primitive and not large base, then either G is the Mathieu group M_{24} in its natural action on 24 points, or $b(G) \leq \lceil \log n \rceil + 1$. Furthermore, we show that there are infinitely many primitive groups G that are not large base for which $b(G) > \log n + 1$, so our bound is optimal.

Keywords Primitive groups · Base size · Classical groups · Simple groups

Mathematics Subject Classification 20B15 · 20B10

1 Introduction

Let the permutation group G act on a set Ω of size n. A subset $\mathcal{B}$ of Ω is a *base* for G if the pointwise stabilizer $G_{(\mathcal{B})}$ is trivial. Let $b(G, \Omega)$, or just $b(G)$ when the meaning is clear, be the minimal size of a base for G.

In the 19th century, a problem that attracted a lot of attention was that of bounding the order of a finite primitive permutation group. It is easy to show that $|G| \leq n^{b(G)}$,

Communicated by John S. Wilson.

✉ Colva M. Roney-Dougal
colva.roney-dougal@st-andrews.ac.uk

Mariapia Moscatiello
mariapia.moscatiello@unibo.it

[1] Dipartimento di Matematica, Universitá di Bologna, Piazza di Porta San Donato 5, 40126 Bologna, Italy

[2] School of Mathematics and Statistics, The University of St Andrews, North Haugh, St Andrews, Fife KY16 9SS, Scotland

Published online: 05 August 2021

so one can find an upper bound on the order of a permutation group by bounding the minimal base size. One of the earliest results in this direction is a theorem of Bochert [2] from 1889, which states that if G is a primitive permutation group of degree n not containing the alternating group $\mathrm{Alt}(n)$, then $b(G) \leq n/2$.

Bases also arise naturally in other contexts, which also benefit from good upper bounds on base size. For example, they have been used extensively in the computational study of finite permutation groups, where the problem of calculating base sizes has important practical applications. The knowledge of how an element g of G acts on a base $\mathcal{B}$ completely determine the action of g on Ω, so once a base and a related data-structure called a strong generating set are known for G, we may store elements of G as $|\mathcal{B}|$-tuples, rather than as permutations, of Ω.

A permutation group G is *large base* if there exist integers m and $r \geq 1$ such that

$$\mathrm{Alt}(m)^r \trianglelefteq G \leq \mathrm{Sym}(m) \wr \mathrm{Sym}(r),$$

where the action of $\mathrm{Sym}(m)$ is on k-element subsets of $\{1, \ldots, m\}$ for some k, and if $r > 1$ then G has product action. Note that this includes the natural actions of $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$.

Using the Classification of Finite Simple Groups (CFSG), and building on earlier work by Cameron [12], in 1984 Liebeck [20] proved the remarkable result that if G is a primitive group of degree n that is not large base, then $b(G) \leq 9 \log n$. (In this paper, all logarithms are to base 2, unless otherwise indicated.) Much more recently, Liebeck, Halasi and Maróti showed in [18] that for most non-large-base primitive groups G, the base size $b(G) \leq 2\lfloor \log n \rfloor + 26$; the second author and Siccha then noted in [22] that this bound applies to all primitive groups that are not large base.

The main result of this paper is as follows.

Theorem 1 *Let G be a primitive permutation group of degree n. If G is not large base, then either G is the Mathieu group M_{24} in its 5-transitive action of degree 24, or $b(G) \leq \lceil \log n \rceil + 1$. Furthermore, there are infinitely many such groups G for which $b(G) > \log n + 1$.*

If G is M_{24} in its 5-transitive action of degree 24 then $b(G) = 7$. In Theorem 5 we shall completely classify the non-large-base primitive groups G for which the base size $b(G) > \log n + 1$: there is one infinite family, and three Mathieu groups.

Our notation for groups is generally standard: for the orthogonal groups, by $\mathrm{GO}^{\varepsilon}_d(q)$ we denote the full isometry group of our standard quadratic form of type ε, as given in Definition 4.

Definition 1 Let G be almost simple with socle G_0, a classical group with natural module V over a field of characteristic p. A subgroup H of G not containing G_0 is a *subspace* subgroup if for each maximal subgroup M of G_0 containing $H \cap G_0$ one of the following holds.

1. $M = G_U$ for some proper nonzero subspace U of V, where U is either totally singular, or non-degenerate, or, if G is orthogonal and $p = 2$, a nonsingular 1-space. If $G_0 = \mathrm{PSL}_d(q)$ then we shall consider all subspaces of V to be totally singular.

2. $G_0 = \mathrm{Sp}_d(2^f)$ and $M \cap G_0 = \mathrm{GO}_d^{\pm}(2^f)$.

A transitive action of G is a *subspace action* if the point stabiliser is a subspace subgroup of G.

Definition 2 Let G be almost simple with socle G_0. A transitive action of G on Ω is *standard* if, up to equivalence of actions, one of the following holds, and is *non-standard* otherwise.

1. $G_0 = \mathrm{Alt}(\ell)$ and Ω is an orbit of subsets or partitions of $\{1, \ldots, \ell\}$;
2. G is a classical group in a subspace action.

Cameron and Kantor conjectured in [12,13] that there exists an absolute constant c such that if G is almost simple with a faithful primitive non-standard action on a finite set Ω then $b(G) \leq c$. In [9, Theorem 1.3], Liebeck and Shalev proved this conjecture, but without specifying the constant c. Later, in a series of papers [5,7,10], Burness and others proved that $b(G) \leq 7$, with equality if and only if G is M_{24} in its 5-transitive action of degree 24; that is, the Cameron-Kantor conjecture is true with the constant $c = 7$.

In stark contrast with the non-standard case, the base size of a group with a standard action can be arbitrarily large. The bulk of this article therefore concerns such actions. For many of the standard actions we shall use results due to Halasi, Liebeck and Maróti [18], however we sometimes require more precise bounds.

Notation 3 Let G be a classical group, with natural module V. We shall write $\mathcal{S}(G, k)$ for a G-orbit of totally singular subspaces of V of dimension k, and $\mathcal{N}(G, k)$ for a G-orbit of non-degenerate or non-singular subspaces of V of dimension k. For the orthogonal groups, let W be a space in the orbit if dk is even, and the orthogonal complement of such a space if dk is odd. Then we write $\mathcal{N}^{\epsilon}(G, k)$, with $\epsilon \in \{+, -\}$, to indicate that the restriction of the form to W is of type ϵ: if d is odd then the symbol $\mathcal{N}(G, k)$ is not used, since k or $d - k$ is even.

The next result is a key tool in the proof of Theorem 1, but may be of independent interest. It will follow immediately from the results in Sect. 2: bounds for smaller dimensions may be found there.

Theorem 2 *Let G be one of $\mathrm{PGL}_d(q)$, $\mathrm{PGU}_d(q)$, $\mathrm{PSp}_d(q)$, or $\mathrm{PGO}_d^{\varepsilon}(q)$. Let $k \in \{1, 2\}$, and let Ω be $\mathcal{S}(G, k)$ or $\mathcal{N}^{\epsilon}(G, k)$, with ϵ either $+$, $-$, or blank.*

1. *Assume that $d \geq 5$, that G is $\mathrm{PGL}_d(q)$, and that $k = 2$. Then $b(G) \leq \lceil d/2 \rceil + 2$.*
2. *Assume that $d \geq 3$, that G is $\mathrm{PGU}_d(q)$ or $\mathrm{PSp}_d(q)$, and that $k = 1$. Then $b(G) \leq d$.*
3. *Assume that $d \geq 6$, that G is $\mathrm{PGO}_d^{\varepsilon}(q)$, and that $k = 1$. Then $b(G) = d - 1$.*
4. *Assume that $d \geq 7$, that G is not $\mathrm{PGL}_d(q)$, and that $k = 2$. Then $b(G) \leq \lceil d/2 \rceil$.*

Additionally, if q is even, $d \geq 6$, and Ω is the right coset space of $\mathrm{GO}_d^{\pm}(q)$ in $G = \mathrm{Sp}_d(q)$, then $b(G) = d$.

We shall prove this result by giving explicit bases of the stated size. These bounds are very similar to those proved by Burness, Guralnick and Saxl in [8] for algebraic groups, although we consider the full projective isometry group. Unfortunately we

were not able to directly transfer many of their proofs over to the finite case, but we have taken some inspiration from their arguments.

We notice in passing that the value of $b(G, \Omega)$ for Ω the right coset space of $\mathrm{GO}_d^{\pm}(q)$ in $G = \mathrm{Sp}_d(q)$ is only one less than the value of the largest irredundant base size for this action, as proved in [16]: in general these two quantities can be very different.

2 Explicit bases for some subspace actions

Let G be a finite almost simple classical group with natural module V. In this section we present explicit bases for the action of G on a G-orbit of totally singular, non-degenerate, or non-singular one- or two-dimensional subspaces of V, and for the action of $\mathrm{Sp}_d(q)$ on the right cosets of $\mathrm{GO}_d^{\pm}(q)$, with q even.

Definition 4 Let $\mathbb{F} = \mathbb{F}_{q^2}$ in the unitary case, and $\mathbb{F} = \mathbb{F}_q$ otherwise, and let σ be the automorphism of $\mathbb{F}$ mapping $x \mapsto x^q$. Write $\mathbb{F}^*$ for the non-zero elements of $\mathbb{F}$.

We fix our standard classical forms and bases on $V = \mathbb{F}^d$. Our standard basis for $\mathrm{GL}_d(q)$ will be $(v_1, \ldots, v_d)$. If $d = 2a$ then our standard unitary and symplectic forms B have basis $(e_1, \ldots, e_a, f_1, \ldots, f_a)$, whilst our standard unitary form for $d = 2a+1$ has basis $(e_1, \ldots, e_a, f_1, \ldots, f_a, x)$. In both cases, for all i and j we set $B(e_i, e_j) = B(f_i, f_j) = 0$, $B(e_i, f_j) = \delta_{i,j}$ (the Kronecker δ), $B(e_i, x) = B(f_i, x) = 0$, and $B(x, x) = 1$.

Our standard quadratic form Q, with symmetric bilinear form B, has basis

$$\begin{cases} (e_1, \ldots, e_a, f_1, \ldots, f_a) & \text{if } d = 2a \text{ and } Q \text{ is of } + \text{ type}, \\ (e_1, \ldots, e_a, f_1, \ldots, f_a, x, y) & \text{if } d = 2a+2 \text{ and } Q \text{ is of } - \text{ type}, \\ (e_1, \ldots, e_a, f_1, \ldots, f_a, x) & \text{if } d = 2a+1, \end{cases}$$

where for all i and j we set $Q(e_i) = Q(f_i) = 0$, $B(e_i, f_j) = \delta_{i,j}$, $B(e_i, x) = B(f_i, x) = B(e_i, y) = B(f_i, y) = 0$, $Q(x) = B(x, y) = 1$ and $Q(y) = \zeta$, where $X^2 + X + \zeta \in \mathbb{F}[X]$ is irreducible. We will work, at times, with orthogonal groups of odd dimension in characteristic two, and this is our standard form in this case as well: see, for example, [23, p139] for more information.

A pair (u, v) of vectors in V is a *hyperbolic pair* if $B(u, u) = B(v, v) = 0$, $B(u, v) = 1$, and (in the orthogonal case) $Q(u) = Q(v) = 0$.

We now collect a pair of elementary lemmas. The first two parts of the following are well known, and the third is easy. By the *support* of a vector v, denoted $\mathrm{Supp}(v)$, we mean the set of basis vectors for which the coefficient is nonzero.

Lemma 1 *Let $W = \mathbb{F}_q^d$ with basis $w_1, \ldots, w_d$, let $H = \mathrm{GL}_d(q)$, and let the set $\mathcal{A} = \{\langle w_1 \rangle, \ldots, \langle w_d \rangle\}$.*

1. *$H_{(\mathcal{A})}$ is a group of diagonal matrices, and is trivial when $q = 2$.*
2. *For all $\mu := (\mu_1, \ldots, \mu_d) \in (\mathbb{F}_q^*)^d$, let $\mathcal{A}(\mu) = \mathcal{A} \cup \{\langle \mu_1 w_1 + \cdots + \mu_d w_d \rangle\}$. Then $H_{(\mathcal{A}(\mu))} = Z(\mathrm{GL}_d(q))$.*

3. *Let $T = \langle u, v\rangle \leq W$, and let $g \in H$ be such that $T^g = T$. If there exists an $s \in \mathrm{Supp}(v)$ such that for all $t \in \mathrm{Supp}(u)$, the vector $s \notin \mathrm{Supp}(tg)$, then $\langle u\rangle^g = \langle u\rangle$.*

In the presence of a non-degenerate form, we can make stronger statements.

Lemma 2 *Let B be a non-degenerate sesquilinear form on $V = \mathbb{F}^d$, with $d > 2$. Let $u, v \in V$ be such that $\langle u, v\rangle$ is non-degenerate, and let g be an isometry of V such that $ug = \alpha u$ for some $\alpha \in \mathbb{F}^*$.*

1. *Assume that $vg = \beta v$, for some $\beta \in \mathbb{F}^*$. If (u, v, w) are such that $0 \neq w \in \langle u, v\rangle^\perp$, and g stabilises $\langle \gamma_1 u + \gamma_2 v + \gamma_3 w\rangle$ for some $\gamma_i \in \mathbb{F}$ with $\gamma_1\gamma_3 \neq 0$, then $wg = \alpha w$. Furthermore, if $\gamma_2 \neq 0$ then $\beta = \alpha$, and if, in addition, $B(u, v) \neq 0$ then $\alpha = \alpha^{-q}$.*
2. *Assume instead that B is symmetric, and that (u, v) are a hyperbolic pair. If the vector $vg \in \langle u, v\rangle$, then $vg = \alpha^{-1}v$.*

Proof (1). Since $\langle u, v\rangle$ is non-degenerate, the matrix g preserves the decomposition $V = \langle u, v\rangle \oplus \langle u, v\rangle^\perp$. Fix a basis $\{w = w_3, w_4, \ldots, w_d\}$ of $\langle u, v\rangle^\perp$. Then there exist $\lambda_3, \ldots, \lambda_d$ such that $wg = \sum_{i=3}^{d} \lambda_i w_i$. Furthermore, there exists $\mu \in \mathbb{F}_q$ such that

$$\mu\left(\gamma_1 u + \gamma_2 v + \gamma_3 w\right) = \left(\gamma_1 u + \gamma_2 v + \gamma_3 w\right) g = \gamma_1\alpha u + \gamma_2\beta v + \gamma_3 \left(\sum_{i=3}^{d} \lambda_i w_i\right).$$

Hence $\mu = \alpha = \lambda_3$ and $\lambda_i = 0$ for $4 \leq i \leq d$. Furthermore, if $\gamma_2 \neq 0$ then $\beta = \alpha$. The final claim is clear.
(2). Let $vg = \beta u + \gamma v$. From $1 = B(u, v) = B(ug, vg) = \alpha\gamma$, we deduce that $\gamma = \alpha^{-1} \neq 0$. Then

$$0 = Q(v) = Q(vg) = Q(\beta u + \gamma v) = \beta\gamma$$

implies that $\beta = 0$. □

2.1 Totally singular subspaces

In this subsection we consider the unitary, symplectic and orthogonal groups acting on $\mathcal{S}(G, k)$ for $k \in \{1, 2\}$, where $\mathcal{S}(G, k)$ is as in Notation 3. We shall use without further comment the fact that the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$, given by $\mathrm{tr}(\alpha) = \alpha + \alpha^q$, is surjective.

Lemma 3 *Let G be $\mathrm{PGU}_d(q)$, $\mathrm{PSp}_d(q)$, $\mathrm{PGO}^\varepsilon_d(q)$, with $d \geq 5$ if G is orthogonal, and $d \geq 3$ otherwise, and let $\Omega = \mathcal{S}(G, 1)$. Then the set $\mathcal{B}$ in Table 1 is a base for the action of G on Ω. In particular, $b(G) \leq d$ and if G is orthogonal then $b(G) \leq d - 1$.*

Proof Let $H = \mathrm{GU}_d(q)$, $\mathrm{Sp}_d(q)$, or $\mathrm{GO}^\varepsilon_d(q)$. First let $\mathcal{B}$ be one of the sets listed in Table 1. A straightforward calculation shows that each subspace in $\mathcal{B}$ is singular, so $\mathcal{B} \subseteq \Omega$. Let $g \in H_{(\mathcal{B})}$. We shall show that g is scalar, from which the result will

Table 1 Bases for $\mathcal{S}(G, 1)$

Let $V_i = \langle e_1 + e_i \rangle$, $W_i = \langle e_1 + f_i \rangle$, and $T = \langle -e_1 + f_1 + x \rangle$		
G	$\mathcal{B}$	Comments
$\mathrm{PGU}_{2a+1}(q)$	$\{\langle e_1 \rangle, \langle f_1 \rangle, V_i, W_i, \langle e_1 + \mu f_1 + x \rangle \mid 2 \leq i \leq a\}$	$\mathrm{tr}(\mu) = -1$
$\mathrm{PGU}_{2a}(q), \mathrm{PSp}_{2a}(q)$	$\{\langle e_1 \rangle, \langle f_1 \rangle, V_i, W_i \mid 2 \leq i \leq a\}$	
$\mathrm{PGO}^+_{2a}(q)$	$\{\langle e_1 \rangle, \langle f_1 \rangle, V_i, W_j \mid 2 \leq i \leq a, 2 \leq j \leq a-1\}$	
$\mathrm{PGO}_{2a+1}(q)$	$\{\langle e_1 \rangle, \langle f_1 \rangle, V_i, W_j, T \mid 2 \leq i \leq a, 2 \leq j \leq a-1\}$	
$\mathrm{PGO}^-_{2a+2}(q)$	$\{\langle e_1 \rangle, \langle f_1 \rangle, V_i, W_j, \langle -\zeta e_1 + f_1 + y \rangle T \mid 2 \leq i \leq a, 2 \leq j \leq a-1\}$	ζ from Definition 4

follow. To do so, we shall repeatedly apply Lemma 2(1), with (u, v, w) set to be equal to various triples of vectors.

For $\mathrm{PGU}_3(q)$ it suffices to apply Lemma 2(1) to (e_1, f_1, x). So we can assume that $d \geq 4$. Apply Lemma 2(1), first to (e_1, f_1, e_i) and then to (e_1, f_1, f_j) to see that there exists $\alpha \in \mathbb{F}$ such that

$$e_i g = \alpha e_i, \quad f_j g = \alpha f_j, \quad \text{for } 1 \leq i \leq a \text{ and } \begin{cases} 2 \leq j \leq a & \text{if } H \text{ is } \mathrm{GU}_d(q) \text{ or } \mathrm{Sp}_d(q), \\ 2 \leq j \leq a-1 & \text{if } H \text{ is orthogonal.} \end{cases} \tag{1}$$

Now, $B(e_1 g, f_1 g) = 1$ yields

$$f_1 g = \alpha^{-q} f_1. \tag{2}$$

For $\mathrm{PGU}_{2a+1}(q)$ the result follows by applying Lemma 2(1) to (e_1, f_1, x). For $\mathrm{PGU}_{2a}(q), \mathrm{PSp}_{2a}(q)$ and $\mathrm{PGO}^+_{2a}(q)$, we deduce from $B(e_2 g, f_2 g) = 1$ that $\alpha = \alpha^{-q}$, hence if G is not orthogonal then g is scalar.

For $\mathrm{PGO}_{2a+1}(q)$, applying Lemma 2(1) to (e_1, f_1, x) shows that $xg = \alpha x = \pm x$. Similarly, for $\mathrm{PGO}^-_{2a+2}(q)$, applying Lemma 2(1) to both (e_1, f_1, x) and (e_1, f_1, y) yields $xg = \alpha x = \pm x$ and $yg = \alpha y$. Combining these with (1) and (2), we deduce that if H is orthogonal then g stabilizes $\langle e_a, f_a \rangle^\perp$, and so stabilizes $\langle e_a, f_a \rangle$. Then Lemma 2(2) shows that $f_a g = \alpha f_a$, so g is scalar. □

Lemma 4 *Let $G = \mathrm{PGL}_d(q)$ and let $\Omega = \mathcal{S}(G, 2)$. Then the set $\mathcal{B}$ in Table 2 is a base for the action of G on Ω. In particular $b(G) \leq \lceil \frac{d}{2} \rceil + 2$ when $d \geq 5$, and $b(G) \leq 5$ when $d = 4$.*

Proof Let $g \in \mathrm{GL}_d(q)_{(\mathcal{B})}$: we shall show that g is scalar. The arguments for $d = 4$ are similar to, but easier than, those that follow, so let $d \geq 5$, and let $X = X_1 \oplus \cdots \oplus X_{a-1}$. Then g stabilises $Y_1 \cap X = \langle v_2 + v_4 + \cdots + v_{2a-2} \rangle$. Hence there exists $\alpha \in \mathbb{F}_q$ such that

$$v_{2j} g = \alpha v_{2j}, \text{ for } 1 \leq j \leq a-1.$$

Furthermore, g stabilises $X_1 \cap Y_2 = \langle v_1 \rangle$, and hence $v_1 g = \beta v_1$ for some $\beta \in \mathbb{F}$. Now, this and the fact that g stabilizes $X_2 \oplus \cdots \oplus X_a = \langle v_3, v_4, \ldots, v_{2a-1}, v_{2a} \rangle$ means that we may apply Lemma 1(3), with the vectors $u = v_1 + v_3 + \cdots + v_{2a-1}$, $v = v_2 + v_4 + \cdots + v_{2a-2}$, and $s = v_2$ to deduce that

$$v_{2i-1} g = \beta v_{2i-1}, \text{ for } 1 \leq i \leq a.$$

Now, $v_d g \in \langle v_{d-1}, v_d \rangle$ if $d = 2a$ is even (and $v_d g = \beta v_d$ otherwise), so once again applying Lemma 1(3), this time with $T = Y_2$, $u = v_3 + v_{2a-2} + v_d$ and $s = v_1$ yields $\langle u \rangle^g = \langle u \rangle$, so $\alpha = \beta$ and g is scalar. □

Lemma 5 *Let $G \in \{\mathrm{PGU}_d(q), \mathrm{PSp}_d(q), \mathrm{PGO}^{\varepsilon}_d(q)\}$ with $d \geq 4$, and $d \geq 7$ if G is orthogonal, let $\Omega = \mathcal{S}(G, 2)$ and let $b = b(G)$. Then the set $\mathcal{B}$ in Table 2 is a base for the action of G on Ω. In particular, if $d \geq 7$ then $b \leq \lceil \frac{d}{2} \rceil$, if $G = \mathrm{PGU}_4(q)$ then $b \leq 5$, whilst otherwise, if $d \leq 6$ then $b \leq 4$.*

Proof The arguments for $d \leq 6$ are similar to, but more straightforward than, those that follow, so we shall assume that $d \geq 7$, so that $a = \lceil d/2 \rceil \geq 4$.

Let H be $\mathrm{GU}_d(q)$, $\mathrm{Sp}_d(q)$ or $\mathrm{GO}^{\varepsilon}_d(q)$, and let $g \in H_{(\mathcal{B})}$. It is straightforward to verify that $\mathcal{B} \subseteq \Omega$. Since $V_i^g = V_i$ for $i \in \{1, 2\}$, there exist $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{F}$ such that

$$\begin{aligned} e_1 g &= \alpha_1 e_1 + \alpha_2 e_2, \;\; e_2 g = \beta_1 e_1 + \beta_2 e_2 \\ f_1 g &= \gamma_1 f_1 + \gamma_2 f_2, \;\; f_2 g = \delta_1 f_1 + \delta_2 f_2. \end{aligned} \tag{3}$$

Let $\mathcal{A}$ be as in Table 2, and let $X = \langle \mathcal{A} \rangle$. We shall first show that

$$e_i g = \alpha_1 e_i \text{ and } f_i g = \beta_2 f_i \;\; \text{for } i = \{1, 3, 4, \ldots, a-1\}, \quad e_2 g = \beta_2 e_2, \quad f_2 g = \alpha_1 f_2. \tag{4}$$

Let $U = V_1 \oplus V_2$, and let $W = U^{\perp}$, so that $W^g = W$. For $3 \leq i \leq a-1$, the element g stabilises $U_i := \langle V_1, V_2, W_i \rangle$, and so stabilises $U_i \cap W = \langle e_i, f_i \rangle$. Then Lemma 1(3), with $u = e_1 + e_i$, $v = e_2 - f_1 + f_i$, and $s = f_1$ shows that there exists $\eta \in \mathbb{F}$ such that $(e_1 + e_i)g = \eta(e_1 + e_i) = \alpha_1 e_1 + \alpha_2 e_2 + e_i g$, where the last equality holds by (3). Hence (4) holds for e_i for $i \neq 2$. Similarly, for $3 \leq i \leq a-1$, there exist $\eta, \rho \in \mathbb{F}$ such that

$$\begin{aligned} (e_2 - f_1 + f_i)\, g &= \eta\,(e_1 + e_i) + \rho\,(e_2 - f_1 + f_i) \\ &= \beta_1 e_1 + \beta_2 e_2 - \gamma_1 f_1 - \gamma_2 f_2 + f_i g. \end{aligned}$$

Equating coefficients, we deduce from $f_i g \in \langle e_i, f_i \rangle$ that $\gamma_2 = 0$ and $\beta_2 = \gamma_1$, so that $f_1 g = \beta_2 f_1$, and also deduce that $f_i g = \beta_1 e_i + \beta_2 f_i$ for $3 \leq i \leq a-1$. For $i \in \{1, 2\}$, let $A_i = \langle e_i, f_i \rangle$. Then $A_1^g = A_1$, so g stabilises $A_1^{\perp} \cap U = A_2$, and consequently stabilizes $V_1 \cap A_2 = \langle e_2 \rangle$ and $V_2 \cap A_2 = \langle f_2 \rangle$, and so $\beta_1 = \delta_1 = 0$. Finally, $B(e_1 g, f_1 g) = B(e_2 g, f_2 g) = 1$ yields

$$\alpha_1 = \beta_2^{-q}, \text{ and } \beta_2 = \delta_2^{-q},$$

Table 2 Bases for $\mathcal{S}(G, 2)$

Let $a = \lceil d/2 \rceil$, $X_i = \langle v_{2i-1}, v_{2i} \rangle$ with $v_{d+1} = v_1$, $Y_1 = \langle v_1 + v_3 + \cdots + v_{2a-1}, v_2 + v_4 + \cdots + v_{2a-2} \rangle$, $V_1 = \langle e_1, e_2 \rangle$, $V_2 = \langle f_1, f_2 \rangle$, $W_i = \langle e_1 + e_i, e_2 - f_1 + f_i \rangle$, and $\mathcal{A} = \{V_1, V_2, W_i \ : \ 3 \leq i \leq a-1\}$

G	$\mathcal{B}$	Notes
$\mathrm{PGL}_4(q)$	$\{X_1, X_2, Y_1, \langle v_2, v_4 \rangle, \langle v_1 + v_2, v_3 \rangle\}$	
$\mathrm{PGL}_d(q)$	$\{X_i, Y_1, Y_2 = \langle v_1, v_3 + v_{2a-2} + v_d \rangle \ : \ 1 \leq i \leq a\}$	$d \geq 5$
$\mathrm{PGU}_4(q)$	$\{V_1, V_2, \langle e_1 + \mu f_1, e_2 + \mu f_2 \rangle, \langle e_1, f_2 \rangle, \langle e_1 - e_2, f_1 + f_2 \rangle\}$	$\mathrm{tr}(\mu) = 0$
$\mathrm{PSp}_4(q)$	$\{V_1, V_2, \langle e_1 + f_1 + f_2, e_2 + f_1 \rangle, \langle e_1 + f_2, e_2 + f_1 + f_2 \rangle\}$	q even
	$\{V_1, V_2, \langle e_1 + f_1 + f_2, e_2 + f_1 \rangle, \langle e_1 + f_2, e_2 + f_1 \rangle\}$	q odd
$\mathrm{PGU}_5(q)$	$\{V_1, V_2, \langle -e_2 + \lambda f_2 + x, f_1 \rangle, \langle -e_1 + \lambda f_1 + x, f_2 \rangle\}$	$\mathrm{tr}(\lambda) = 1$
$\mathrm{PSp}_6(q)$, $\mathrm{PGU}_6(q)$	$\{V_1, V_2, \langle e_1 + e_3, e_2 - f_1 + f_3 \rangle, \langle e_1 - e_2, f_1 + f_2 \rangle\}$	
$\mathrm{PGU}_{2a}(q)$, $\mathrm{PSp}_{2a}(q)$, $\mathrm{PGO}^+_{2a}(q)$	$\mathcal{A} \cup \{V_3 = \langle e_1 + e_a, e_2 - e_a - f_1 + f_2 + f_a \rangle\}$	$a \geq 4$
$\mathrm{PGU}_{2a-1}(q)$	$\mathcal{A} \cup \{V_4 = \langle -e_1 + \lambda f_1 + x, e_3 + f_2 \rangle\}$	$\mathrm{tr}(\lambda) = 1$, $a \geq 4$
$\mathrm{PGO}_{2a-1}(q)$	$\mathcal{A} \cup \{V_5 = \langle -e_1 + f_1 + x, e_3 + f_2 \rangle\}$	$a \geq 4$
$\mathrm{PGO}^-_{2a}(q)$	$\mathcal{A} \cup \{V_6 = \langle -e_1 + e_2 + f_1 + x, -\zeta e_1 + f_1 + \zeta f_2 + y \rangle\}$	$a \geq 4$

hence $\alpha_1 = \delta_2$, and so (4) follows.

We now complete the proof that $g = \alpha_1 I_d$, so $\mathcal{B}$ is a base for G. If $d = 2a - 1$ then (4) yields $(X^\perp)^g = \langle x \rangle^g = \langle x \rangle$. Let $u = -e_1 + f_1 + x$ if G is orthogonal and $u = -e_1 + \lambda f_1 + x$ otherwise. Then Lemma 1(3), with $v = e_3 + f_2$ and $s = f_2$, shows that $\langle u \rangle^g = \langle u \rangle$, and so $g = \alpha_1 I_d$, as required.

If $H = \mathrm{GO}^-_{2a}(q)$ then $(X^\perp)^g = \langle x, y \rangle^g = \langle x, y \rangle$. We deduce from (4) and Lemma 1(3), with $T = V_6$, $u = -e_1 + e_2 + f_1 + x$ and $s = f_2$, that $\langle u \rangle^g = \langle u \rangle$, and so $\alpha_1 = \beta_2$ and $xg = \alpha_1 x$. Now considering $u = -\zeta e_1 + f_1 + \zeta f_2 + y$ and $s = e_2$ shows that g is scalar.

Finally, consider $\mathrm{PGU}_{2a}(q)$, $\mathrm{PSp}_{2a}(q)$ and $\mathrm{PGO}^+_{2a}(q)$. From (4) we see that $\langle e_a, f_a \rangle^g = \langle e_a, f_a \rangle$. Then, by Lemma 1(3), with $T = V_3$, $u = e_1 + e_a$, and $s = e_2$, we deduce that $e_a g = \alpha_1 e_a$. Finally, if we instead let $u = e_2 - e_a - f_1 + f_2 + f_a$, $v = e_1 + e_a$, and $s = e_1$, then we see that $\langle u \rangle^g = \langle u \rangle$, and so $g = \alpha_1 I_{2a}$, as required. □

2.2 Non-degenerate subspaces

In this subsection we consider $\mathcal{N}^\epsilon(G, k)$, where $k \leq 2$ and $\mathcal{N}^\epsilon(G, k)$ is as in Notation 3.

Lemma 6 *Let $d \geq 3$, let $G = \mathrm{PGU}_d(q)$, and let $\Omega = \mathcal{N}(G, 1)$. Then the set $\mathcal{B}$ in Table 3 is a base for the action of G on Ω, so $b(G) \leq d$.*

Proof First assume that either d is odd or $q > 2$. Let α be a primitive element of $\mathbb{F}^*$. Then for at least one value of μ in $\{\alpha, \alpha^{-1}, \alpha^2\}$ the vector $v(\mu) = v_1 + \cdots + v_{d-1} + \mu v_d$ is non-degenerate, so $\mathcal{B} \subseteq \Omega$. Let $g \in \mathrm{GU}_d(q)_{(\mathcal{B})}$ and $U = \langle v_1, \ldots, v_{d-1} \rangle$. Since U is non-degenerate, $(U^\perp)^g = \langle v_d \rangle^g = \langle v_d \rangle$, and hence g is diagonal by Lemma 1(1). Then g also stabilises $\langle v(\mu) \rangle$, and so is scalar, by Lemma 1(2).

For $q = 2$ and d even, g stabilises $\langle v_1, v_2 \rangle^\perp = \langle v_3, \ldots, v_d \rangle$. Therefore Lemma 2(1), applied to (v_1, v_2, v_i), for $3 \leq i \leq d$, shows that $\mathrm{GU}_d(q)_{(\mathcal{B})}$ is scalar. □

When q is odd, $\mathrm{PGO}^\varepsilon_d(q)$ has two orbits of non-degenerate 1-spaces. If d is even then the orbits can be distinguished by considering the discriminant of the restriction of the quadratic form to the subspace, and the actions on the two orbits are equivalent, so it is enough to consider one of them. If d is odd then the orbits can be distinguished by the sign of the restriction of the form to the orthogonal complement.

Lemma 7 *Let $d \geq 4$, let $G = \mathrm{PGO}^\varepsilon_d(q)$ with $\varepsilon = -$ if $d = 4$, and let Ω be a G-orbit of non-degenerate or non-singular 1-spaces. Then, up to equivalence, the set $\mathcal{B}$ in Table 3 is a base for the action of G on Ω. In particular, if $d \geq 6$ then $b(G) \leq d - 1$, $b(\mathrm{PGO}^-_4(q)) \leq 3$ if $q \neq 3$, and $b(\mathrm{PGO}_5(q)) \leq 5$. In addition, $b(\mathrm{PGO}^-_4(3)) = 4$.*

Proof The result for $\mathrm{PGO}^-_4(3)$ is an easy calculation. Let $H = \mathrm{GO}^\varepsilon_d(q)$. We start with $d \leq 5$, and show first that $\mathcal{B}$ is contained in a single G-orbit of the appropriate type. For $\mathrm{GO}^-_4(q)$, all 1-spaces in $\langle x, y \rangle$ are non-degenerate. For q odd, they are partitioned into $(q + 1)/2$ spaces $\langle v \rangle$ such that $Q(v)$ is square, and $(q + 1)/2$ with $Q(v)$ non-square. Thus for $q \neq 3$, we may find $v_1, v_2 \in \langle x, y \rangle$ that are linearly independent, not multiples of x, and such that $Q(v_i)$ is square, so that $\mathcal{B}$ is a subset of a G-orbit.

Table 3 Bases for $\mathcal{N}(\mathrm{PGU}_d(q), 1)$ and $\mathcal{N}^\epsilon(\mathrm{PGO}^\varepsilon_d(q), 1)$

For $\mathrm{PGU}_d(q)$, let $(v_1, \ldots, v_d)$ be an orthonormal basis of V.		
d and q	$\mathcal{B}$	Comments
d odd or $q > 2$	$\{\langle v_1\rangle, \ldots, \langle v_{d-1}\rangle, \langle v(\mu)\rangle\}$	$v(\mu)$ as in proof
d even and $q = 2$	$\{\langle v_1\rangle, \langle v_2\rangle, \langle v_1 + v_2 + v_i\rangle \mid 3 \leq i \leq d\}$	
For $\mathrm{PGO}^\varepsilon_d(q)$, let a be the Witt index, let $w_k(v) = e_k - v f_k$, and let $-\alpha \in \mathbb{F}$ be non-square		
$(d, \epsilon, \varepsilon)$	$\mathcal{B}$	Notes
$(4, \circ, -)$	$\{\langle x\rangle, \langle v_1\rangle, \langle e_1 + v_2\rangle \mid v_1, v_2 \in \langle x, y\rangle,\ Q(v_1)$ and $Q(v_2)$ square, $\lvert\{\langle x\rangle, \langle v_1\rangle, \langle v_2\rangle\}\rvert = 3\}$	$q \neq 3$
$(5, +, \circ)$	$\{\langle x\rangle, \langle e_1 + x\rangle, \langle f_1 + x\rangle, \langle e_2 + x\rangle\}$	
$(5, -, \circ)$	$\{\langle w_1(\alpha)\rangle, \langle w_1(\alpha) + e_2\rangle, \langle w_1(\alpha) + f_2\rangle, \langle w_2(\alpha) + e_1\rangle, \langle w_2(1+\alpha) + f_1 + x\rangle\}$	
$(\geq 6, \circ, +)$	$\{\langle w_1(-1)\rangle, \langle w_1(-1) + e_i\rangle, \langle w_1(-1) + f_j\rangle, \langle e_1 + w_2(-1)\rangle \mid 2 \leq i \leq a,\ 2 \leq j \leq a-1\}$	
$(\geq 6, \circ, -)$	$\{\langle x\rangle, \langle v_1\rangle, \langle e_i + v_2\rangle, \langle f_j + x\rangle \mid v_1$ and v_2 as in $d = 4,\ 1 \leq i \leq a,\ 1 \leq j \leq a-1\}$	$q \neq 3$
	$\{\langle x\rangle, \langle e_i + x\rangle, \langle w_1(1) + y\rangle, \langle f_j + x\rangle \mid 1 \leq i \leq a, 1 \leq j \leq a-1\}$	$q = 3$
$(\geq 7, +, \circ)$	$\{\langle x\rangle, \langle e_i + x\rangle, \langle f_j + x\rangle \mid 1 \leq i \leq a,\ 1 \leq j \leq a-1\}$	
$(\geq 7, -, \circ)$	$\{\langle w_1(\alpha)\rangle, \langle w_1(\alpha) + e_i\rangle, \langle w_1(\alpha) + f_j\rangle, \langle e_1 + w_2(\alpha)\rangle, \langle w_2(1+\alpha) + f_1 + x\rangle \mid 2 \leq i \leq a,\ 2 \leq j \leq a-1\}$	

For $(d, \epsilon) = (5, +)$, notice that $\langle e_1 + x\rangle^\perp = \langle e_1, x - 2f_1, e_2, f_2\rangle$ is of plus type, and similarly for the rest of $\mathcal{B}$, so $\mathcal{B} \subseteq \Omega$.

For $(d, \epsilon) = (5, -)$, notice that $\langle w_1(\alpha)\rangle^\perp = \langle e_1 - \alpha f_1\rangle^\perp = \langle e_1 + \alpha f_1, x\rangle \oplus \langle e_2, f_2\rangle$, and the determinant of the restriction of the bilinear form B to $\langle e_1 + \alpha f_1, x\rangle$ is 4α, which is square if and only if α is square. Since $-\alpha$ is non-square, α is a square if and only if $q \equiv 3 \bmod 4$, so $\langle w_1(\alpha)\rangle \in \Omega$ by [19, Prop 2.5.10]. Similarly, the restriction of B to $\langle w_1(\alpha) + e_2\rangle^\perp = \langle e_1 - \alpha f_1 + e_2\rangle^\perp = \langle e_1 + \alpha f_1, x, f_1 - f_2, e_2\rangle$ has determinant -4α, which is always non-square, so $\langle w_1(\alpha) + e_2\rangle \in \Omega$. Notice also that

$$\begin{aligned}\langle w_2(1+\alpha) + f_1 + x\rangle^\perp &= \langle e_2 - (1+\alpha)f_2 + f_1 + x\rangle^\perp \\ &= \langle e_2 + (1+\alpha)f_2, x - 2e_1, f_1, x - 2f_2\rangle,\end{aligned}$$

so a short calculation shows that this 1-space is also in Ω. The argument for the remaining 1-spaces is similar, so $\mathcal{B} \subseteq \Omega$.

We show next that $\mathcal{B}$ is a base, so let $g \in H_{(\mathcal{B})}$. If $d = 4$ then the assumption that v_2 is not a multiple of either x or v_1 combines with Lemma 2(1) applied to (x, v_1, e_1) to show that $g|_{\langle x, y, e_1\rangle} = \pm I_3$. Since g stabilises $\langle x, y\rangle^\perp = \langle e_1, f_1\rangle$, Lemma 2(2) shows that $g = \pm I_4$. For $d = 5$ and $\epsilon = -$, it is straightforward to see that $\mathcal{B}$ forms a base for G. For $d = 5$ and $\epsilon = +$, notice that g stabilises both $\langle x\rangle^\perp$ and $\langle x, e_1 + x, f_1 + x\rangle$, so stabilises $\langle e_i, f_i\rangle$ for $i = 1, 2$. It is then easy to see that $g|_{\langle x, e_1, e_2, f_1\rangle} = \pm I_4$, from which Lemma 2(2) shows that $g = \pm I_5$.

For the rest of the proof, assume that $d \geq 6$. In cases $(\epsilon, \varepsilon) = (+, \circ)$ and $\varepsilon = -$ with $q \neq 3$, the arguments that $\mathcal{B}$ is contained in a single G-orbit of the appropriate type, and that $\mathcal{B}$ is a base for $H = \mathrm{GO}_d^\varepsilon(q)$, are identical to those for $d \leq 5$, so we will omit them. In the other cases, let $g \in H_{(\mathcal{B})}$. We shall show that $\mathcal{B}$ is contained in a single G-orbit and that g is scalar.

First consider $\varepsilon = +$. Then $Q(z) = 1$ for all $\langle z\rangle \in \mathcal{B}$, so $\mathcal{B}$ is contained in a single G-orbit. Let $\mu \in \mathbb{F}_q$ be such that $(w_1(-1))g = (e_1 + f_1)g = \mu(e_1 + f_1)$. Then $\mu \in \{\pm 1\}$. For $2 \leq i \leq a$, there exists $v_i \in \mathbb{F}_q$ such that

$$(w_1(-1) + e_i)\, g = v_i\, (w_1(-1) + e_i) = \mu\, (w_1(-1)) + e_i g.$$

Hence

$$e_i g = (v_i - \mu)(w_1(-1)) + v_i e_i,$$

and $Q(e_i g) = 0$ yields $v_i = \mu$, so $e_i g = \mu e_i$ for $i \geq 2$. Similarly, $f_i g = \mu f_i$ for $2 \leq i \leq a - 1$, and Lemma 2(2) then yields $f_a g = \mu f_a$. Since $\langle (w_2(-1)) + e_1\rangle \in \mathcal{B}$, we deduce in the same way that $e_1 g = \mu e_1$, and then $(w_1(-1))g = \mu e_1 + f_1 g$ shows that $f_1 g = \mu f_1$, as required.

Next consider $\varepsilon = -$ and $q = 3$. Then $Q(y) = 2$, so it follows that $Q(y + w_1(1)) = Q(y + e_1 - f_1) = 1$. It is clear that $Q(z) = 1$ for all other $\langle z\rangle$ in $\mathcal{B}$, so $\mathcal{B}$ is contained in a single G-orbit. Notice that g stabilises

$$W_1 := \langle x, e_1 + x, f_1 + x\rangle = \langle x, e_1, f_1\rangle$$

and also stabilises

$$W_2 := \langle W_1, w_1(1) + y \rangle = \langle e_1, f_1, x, y \rangle.$$

Hence g stabilises $W_1^\perp \cap W_2 = \langle x + y \rangle$, and so stabilises $U := \langle x, y \rangle$ and $U^\perp$. Then g stabilises $\langle w_1(1) + y \rangle$ and $w_1(1)g \in U^\perp$, so g stabilizes $\langle y \rangle$. Lemma 2(1), applied to both (x, y, e_i) and (x, y, f_j), yields $e_i g = \mu e_i$ and $f_j g = \mu f_j$ for $1 \leq i \leq a$ and $1 \leq j \leq a - 1$. The result follows from Lemma 2(1) applied to $(y, x, w_1(1))$ and Lemma 2(2) applied to (e_a, f_a).

Finally, consider $(\epsilon, \varepsilon) = (-, \circ)$. First notice that g stabilises

$$V_2 := \langle w_1(\alpha) \rangle^\perp = \langle e_1 + \alpha f_1, x, e_2, \ldots, e_a, f_2, \ldots, f_a \rangle.$$

In particular $e_i g = u_i$ for some $u_i \in V_2$ for $2 \leq i \leq a$. Hence there exist $\mu \in \{\pm 1\}$ and $\nu_i \in \mathbb{F}_q^*$ such that

$$(w_1(\alpha) + e_i)\, g = \nu_i\, (w_1(\alpha) + e_i) = \mu\, (w_1(\alpha)) + u_i,$$

and so $u_i = e_i g = \mu e_i$ for $2 \leq i \leq a$. Similarly, $f_j g = \mu f_j$ for $2 \leq j \leq a - 1$. Then applying Lemma 2(1) to $(e_2, f_2, e_1 + w_2(\alpha))$ shows that $e_1 g = \mu e_1$ and then $f_1 g = \mu f_1$, by Lemma 2(2). We now deduce that $xg \in \langle e_a, f_a, x \rangle$, and so from $\langle w_2(1+\alpha) + f_1 + x \rangle \in \mathcal{B}$ we see that $xg = \mu x$. The result follows from Lemma 2(2). □

We now prove that the bound for even-dimensional orthogonal groups in Lemmas 3 and 7 is tight.

Lemma 8 *Let $d \geq 6$ be even, and let $G = \mathrm{PGO}_d^\pm(q)$. Let $\mathcal{A} = \{\langle v_1 \rangle, \ldots, \langle v_{d-2} \rangle\}$ be a set of $d - 2$ one-dimensional subspaces of the natural module V for G. Then $G_{(\mathcal{A})}$ is nontrivial. In particular, if Ω is a G-orbit of 1-dimensional subspaces, then $b(G, \Omega) = d - 1$.*

Proof Let $H = \mathrm{GO}_d^\pm(q)$, let W be any $(d-2)$-space containing $\langle \mathcal{A} \rangle$, and let K denote the subgroup of H that acts as scalars on W. We shall show that there exists a nonscalar element of K, from which the result will follow.

If W is non-degenerate, then K contains a subgroup which acts as $\mathrm{GO}(W^\perp) \neq 1$ on $W^\perp$, so the result is immediate. Thus we may assume that W is degenerate, so $U := \mathrm{Rad}(W) = W \cap W^\perp$ is a non-zero subspace of W, of dimension 1 or 2.

First assume that there exists a $u \in U$ such that $Q(u) \neq 0$. This implies that q is even, so H has a single orbit on non-singular 1-spaces, and without loss of generality we can assume that $u = e_1 + f_1$. This implies that $e_1, f_1 \notin W$. We define $g \in \mathrm{GL}(V)$ by

$$e_1 g = f_1, \quad f_1 g = e_1, \quad zg = z \text{ for all } z \in \langle e_1, f_1 \rangle^\perp.$$

Let $v \in V$. Then $v = \alpha e_1 + \beta f_1 + z$, for some $\alpha, \beta \in \mathbb{F}_q$ and $z \in \langle e_1, f_1 \rangle^\perp$, and it is easy to verify that $Q(vg) = Q(v)$, and so $g \in H$. Furthermore, if $w \in W$ then

$B(w, e_1 + f_1) = 0$, so $w = \gamma e_1 + \gamma f_1 + z$, for some $\gamma \in \mathbb{F}_q$ (recalling that q is even) and $z \in \langle e_1, f_1 \rangle^\perp$. Hence $wg = w$, so $g \in K$, as required.

Assume instead that $Q(u) = 0$ for all $u \in U$, and consider first $\dim(U) = 1$. Then we can write $W = \langle u \rangle \perp W'$, with $\mathrm{Rad}(W') = 0$. If q is even this contradicts the fact that $\dim W = d - 2$ is even, so q is odd. There exists a $u' \in V \setminus W$ such that $B(u, u') \neq 0$, and we let $W_1 = \langle W, u' \rangle$. Then W_1 is non-degenerate, and $\dim(W_1) = d - 1$, so $\dim(W_1^\perp) = 1$. Let $\langle z \rangle = W_1^\perp$, and define $g \in \mathrm{GL}(V)$ by

$$zg = -z, \quad wg = w \text{ for all } w \in W_1.$$

Let $v \in V$. Then $v = w + \alpha z$, for some $w \in W_1$ and $\alpha \in \mathbb{F}_q$, so

$$Q(vg) = Q(w - \alpha z) = Q(w) + (-\alpha)^2 Q(z) = Q(v),$$

so $g \in K$, as required.

Finally consider the case $\dim(U) = 2$. We fix $u_1 \in U \setminus \{0\}$. There exists a vector $t_1 \in V \setminus W$ such that (u_1, t_1) is a hyperbolic pair. Furthermore, $\langle u_1, t_1 \rangle^\perp \cap U$ is 1-dimensional, with basis u_2, say, and there exists $t_2 \in \langle u_1, t_1 \rangle^\perp \setminus W$ such that (u_2, t_2) is a hyperbolic pair. Since $t_1, t_2 \notin W$, we may define an element $g \in \mathrm{GL}(V)$ by

$$t_1 g = t_1 + u_2, \quad t_2 g = t_2 - u_1, \quad wg = w \text{ for all } w \in W.$$

Let $v \in V$. Then $v = \alpha t_1 + \beta t_2 + w$ for some $\alpha, \beta \in \mathbb{F}_q$ and $w \in W$, and so

$$\begin{aligned} Q(vg) &= Q(\alpha(t_1 + u_2) + \beta(t_2 - u_1)) + Q(w) + B(\alpha(t_1 + u_2) + \beta(t_2 - u_1), w) \\ &= -\alpha\beta + \alpha\beta + Q(w) + B(\alpha t_1 + \beta t_2, w) = Q(v), \end{aligned}$$

so $g \in K$, as required. □

Lemma 9 *Let $G \in \{\mathrm{PGU}_d(q), \mathrm{PSp}_d(q), \mathrm{PGO}_d^\varepsilon(q)\}$ with $d \geq 5$, and $d \geq 7$ if G is orthogonal, let $\Omega = \mathcal{N}^+(G, 2)$ when G is orthogonal and $\Omega = \mathcal{N}(G, 2)$ otherwise, and let $b = b(G, \Omega)$. Then the set $\mathcal{B}$ in Table 4 is a base for the action of G on Ω. In particular, if $d \neq 6$ then $b \leq \lceil \frac{d}{2} \rceil$, and if $d = 6$ then $b \leq 4$.*

Proof It is straightforward to verify that the given basis of each space in $\mathcal{B}$ is a hyperbolic pair, so $\mathcal{B} \subseteq \Omega$ in each case. The arguments for $d \leq 6$ are similar to, but more straightforward than, those that follow, so we shall assume that $d \geq 7$, so that $a = \lceil d/2 \rceil \geq 4$. Let H be $\mathrm{GU}_d(q)$, $\mathrm{Sp}_d(q)$ or $\mathrm{GO}_d^\varepsilon(q)$ and let $g \in H_{(\mathcal{B})}$.

From $V_2^g = V_2$, it follows that $(f_1 + f_2)g = \beta(f_1 + f_2) + \gamma e_2 = f_1 g + f_2 g$ for some $\beta, \gamma \in \mathbb{F}$. Then $f_1 g \in V_1$ and $f_2 g \in V_1^\perp$, so equating coefficients yields

$$f_1 g = \beta f_1 \text{ and } \; f_2 g = \beta f_2 + \gamma e_2.$$

Next, notice that g stabilises $V_1^\perp \cap V_2 = \langle e_2 \rangle$, so $e_2 g = \alpha e_2$, where $\beta = \alpha^{-q}$ since $B(e_2 g, f_2 g) = 1$.

Table 4 Bases for $\mathcal{N}(G, 2)$ and $\mathcal{N}^+(G, 2)$

Let $V_1 = \langle e_1, f_1\rangle$, $V_2 = \langle e_2, f_1 + f_2\rangle$, $W_i = \langle e_1 + e_i, f_2 + f_i\rangle$, $\mathcal{A} = \{V_1, V_2, W_i \ : \ 3 \leq i \leq a-1\}$		
G	$\mathcal{B}$	Notes
$\mathrm{PSp}_6(q)$, $\mathrm{PGU}_6(q)$	$\{V_1, V_2, W_3, \langle e_1 + e_2, e_1 + f_2 + f_3\rangle\}$	q odd
$\mathrm{PGU}_{2a}(q)$, $\mathrm{PSp}_{2a}(q)$, $\mathrm{PGO}^+_{2a}(q)$	$\mathcal{A} \cup \{\langle e_2 + e_a + f_1, e_1 + f_2 + f_a\rangle\}$	q even, $a \geq 4$
	$\mathcal{A} \cup \{\langle e_a + f_1, e_2 + f_1 + f_a\rangle\}$	q odd, $a \geq 4$
$\mathrm{PGO}^-_{2a}(q)$	$\mathcal{A} \cup \{\langle e_1 - f_1 + x, \zeta e_2 - f_2 + y\rangle\}$	$a \geq 4$
$\mathrm{PGU}_{2a-1}(q)$	$\mathcal{A} \cup \{\langle \lambda e_1 - f_1 + x, \lambda e_2 - f_2 + x\rangle\}$	$\mathrm{tr}(\lambda) = 1$, $a \geq 3$
$\mathrm{PGO}_{2a-1}(q)$	$\mathcal{A} \cup \{\langle e_1 - f_1 + x, e_2 - f_2 + x\rangle\}$	$a \geq 4$

Table 5 Bases for $\mathcal{N}^-(G,2)$

Let $V_1 = \langle e_1 + f_1, e_2 + f_1 + \zeta f_2\rangle$. If $\zeta \neq 1$ then let $V_2 = \langle e_2 + f_1 + f_2, e_1 + \zeta f_1\rangle$, otherwise let $V_2 = \langle e_1 + f_1 + f_2, e_2 + f_2\rangle$. Let $W_i = \langle e_1 + e_i + f_1, e_2 + \zeta e_i + f_i\rangle$ and $\mathcal{A} = \{V_1, V_2, W_i \ : \ 3 \leq i \leq a-1\}$	
G	$\mathcal{B}$
$\mathrm{PGO}_{2a-1}(q)$	$\mathcal{A} \cup \{V_3 = \langle e_2 + f_1 + x, e_1 + e_3 + \zeta f_3\rangle\}$
$\mathrm{PGO}^+_{2a}(q)$	$\mathcal{A} \cup \{V_4 = \langle e_1 + e_2 + f_2 + f_a, e_3 + f_1 + \zeta f_3\rangle\}$
$\mathrm{PGO}^-_{2a}(q)$	$\mathcal{A} \cup \{V_5 = \langle e_1 - e_3 + x, f_1 + f_3 + y\rangle\}$

We shall show next that

$$e_i g = \alpha e_i \text{ and } f_i g = \alpha^{-q} f_i \quad \text{for } 1 \leq i \leq a-1. \tag{5}$$

For $3 \leq i \leq a-1$, the element g stabilises $\langle V_1, V_2, W_i\rangle \cap \langle V_1, V_2\rangle^\perp = \langle e_i, f_i\rangle$. Then Lemma 1(3), applied to $T = W_i$, first with $u = e_1 + e_i$ and $s = f_2$, since $f_2 g \in \langle e_2, f_2\rangle$, and then with $u = f_2 + f_i$ and $s = e_1$, since $e_1 g \in V_1$, shows that there exist $\nu_i, \eta_i, \eta, \delta \in \mathbb{F}$ such that

$$\begin{aligned}(e_1 + e_i)\, g &= \nu_i\, (e_1 + e_i) = (\eta e_1 + \delta f_1) + e_i g\\ (f_2 + f_i)\, g &= \eta_i\, (f_2 + f_i) = \left(\alpha^{-q} f_2 + \gamma e_2\right) + f_i g.\end{aligned}$$

By equating coefficients, we deduce that $e_1 g = \eta e_1$, $e_i g = \eta e_i$, $f_2 g = \alpha^{-q} f_2$, and $f_i g = \alpha^{-q} f_i$. Finally, $B(e_1 g, f_1 g) = 1$ yields $\eta = \alpha$, and so (5) follows.

Finally, we apply Lemma 1(3) to the final subspace, $T = \langle a, b\rangle$ say, in Table 4. When d is odd, setting $u = a$ and $s = e_2$ shows that $\langle a\rangle^g = \langle a\rangle$, so $\alpha = \alpha^{-q}$ and $xg = \alpha x$. If d is even, we deduce both that $\langle a\rangle^g = \langle a\rangle$ and $\langle b\rangle^g = \langle b\rangle$, and hence $g = \alpha I_d$. □

A pair (u, v) of vectors is an *elliptic pair* if $Q(u) = 1$, $Q(v) = \zeta$, for some $\zeta \in \mathbb{F}$ such that $X^2 + X + \zeta$ is irreducible, and $B(u, v) = 1$. Any elliptic pair spans a 2-space of minus type.

Lemma 10 *Let $G = \mathrm{PGO}^\varepsilon_d(q)$, with $\varepsilon \in \{\circ, +, -\}$ and $d \geq 7$, and let $\Omega = \mathcal{N}^-(G,2)$. Then the set $\mathcal{B}$ in Table 5 is a base for the action of G on Ω, and consequently, $b(G,\Omega) \leq \lceil \frac{d}{2} \rceil$.*

Proof Fix ζ such that $X^2 + X + \zeta$ is irreducible, with $\zeta = Q(y)$ if $\varepsilon = -$. Let $a = \lceil d/2 \rceil \geq 4$. One may check that the given ordered basis vectors for each 2-space in $\mathcal{B}$ form an elliptic pair, and so $\mathcal{B} \subseteq \Omega$. For example, $Q(e_1 + f_1) = 1$, $Q(e_2 + f_1 + \zeta f_2) = B(e_2, \zeta f_2) = \zeta$, and $B(e_1 + f_1, e_2 + f_1 + \zeta f_2) = B(e_1, f_1) = 1$. Let $H = \mathrm{GO}^\varepsilon_d(q)$, and let $g \in H_{(\mathcal{B})}$. To show that $\mathcal{B}$ is a base for G, it suffices to show that g is scalar.

We shall show first that there exists $\alpha = \pm 1$ such that

$$(e_1 + f_1)\, g = \alpha\, (e_1 + f_1)\,, \quad e_i g = \alpha e_i \text{ for } 2 \leq i \leq a-1, \quad f_i g = \alpha f_i \quad \text{for } 3 \leq i \leq a-1. \tag{6}$$

Let $U = \langle V_1, V_2 \rangle = \langle e_1, e_2, f_1, f_2 \rangle$. Then g stabilises the subspace $U_i := \langle U, W_i \rangle$ for $3 \leq i \leq a-1$, and so stabilises $U_i \cap U^\perp = \langle e_i, f_i \rangle$. Since g stabilises W_i and V_1, there exist $\mu_i, \nu_i, \alpha, \nu \in \mathbb{F}$ such that

$$\begin{aligned}(e_1 + e_i + f_1)\, g &= \mu_i\,(e_1 + e_i + f_1) + \nu_i\,(e_2 + \zeta e_i + f_i) \in W_i \\ &= (e_1 + f_1)\, g + e_i g = \alpha\,(e_1 + f_1) + \nu\,(e_2 + f_1 + \zeta f_2) + e_i g.\end{aligned}$$

Since $e_i g \in \langle e_i, f_i \rangle$, looking at f_2, we see that $\nu = 0$. Hence $\nu_i = 0$, and we deduce that $(e_1 + f_1)g = \alpha(e_1 + f_1)$ and $e_i g = \alpha e_i$ for $3 \leq i \leq a-1$. We now apply Lemma 2(2) to (e_i, f_i) to see that $f_i g = \alpha^{-1} f_i$ for $3 \leq i \leq a-1$.

To prove (6), it remains to prove that $e_2 g = \alpha e_2 = \pm e_2$. Considering W_3 shows that

$$\begin{aligned}(e_2 + \zeta e_3 + f_3)\, g &= e_2 g + \zeta e_3 g + f_3 g = e_2 g + \zeta \alpha e_3 + \alpha^{-1} f_3 \\ &= \lambda\,(e_2 + \zeta e_3 + f_3) + \mu\,(e_1 + e_3 + f_1)\,,\end{aligned}$$

for some $\lambda, \mu \in \mathbb{F}$. Then $e_2 g \in U$, so considering f_3 gives $\lambda = \alpha^{-1}$. Then considering e_3 yields $\mu = \zeta(\alpha - \alpha^{-1})$, and so $e_2 g = \alpha^{-1} e_2 + \zeta(\alpha - \alpha^{-1})(e_1 + f_1)$. Finally, $Q(e_2 g) = 0$ shows that $\alpha = \alpha^{-1} = \pm 1$ and so (6) is verified.

Let $\mathcal{A} \subseteq \mathcal{B}$ be as in Table 5, and let $X = \langle \mathcal{A} \rangle$. Then g stabilises $X^\perp$. If we can show that either of $e_1 g = \alpha e_1$ or $f_1 g = \alpha f_1$, then it follows from (6) that the same is true for the other. In particular, this will imply that $\langle e_1, f_1 \rangle^g = \langle e_1, f_1 \rangle$. It will then follow from $U^g = U$ that $\langle e_2, f_2 \rangle^g = \langle e_2, f_2 \rangle$. Hence, it will follow from Lemma 2(2) applied to (e_2, f_2) that $f_2 g = \alpha^{-1} f_2 = \alpha f_2$. Hence, to show that g is scalar it suffices to show that $vg = \alpha v$ for either $v = e_1$ or $v = f_1$, and for whichever of $v \in \{e_a, f_a, x, y\}$ is defined. We shall use (6) implicitly.

If d is odd, then Lemma 1(3) with $T = V_3$ and initially with $u = e_1 + e_3 + \zeta f_3$ and $s = x$, gives $ug = \alpha u$, and so $e_1 g = \alpha e_1$ and hence $f_1 g = \alpha f_1$. Now, setting $u = e_2 + f_1 + x$ and $s = e_1$ shows that $ug = \alpha u$. Hence $xg = \alpha x$, and so g is scalar.

If $\varepsilon = +$ then Lemma 1(3) applied to $T = V_4$, $u = e_3 + f_1 + \zeta f_3$ and $s = f_a \in X^\perp$ shows that $ug = \alpha u$. Hence $f_1 g = \alpha f_1$ and so $e_1 g = \alpha e_1$. Next, letting $s = f_1$ shows that $f_a g = \alpha f_a$. Finally, Lemma 2(2) applied to $f_a, e_a \in X^\perp$ proves that g is scalar.

Finally, if $\varepsilon = -$ then $X^\perp = \langle x, y \rangle$. Lemma 1(2), applied to $T = V_5$, initially with $s = f_3$, shows that $(e_1 - e_3 + x)g = \alpha(e_1 - e_3 + x)$. Applying the lemma again, this time with $s = e_3$ gives $(f_1 + f_3 + y)g = \alpha(f_1 + f_3 + y)$. Hence $g = \alpha I_d$. □

2.3 Symplectic groups on the cosets of orthogonal groups

We consider $\mathrm{Sp}_d(q)$, acting on the cosets of $\mathrm{GO}^\pm_d(q)$, with q even.

Proposition 1 *Let $G = \mathrm{Sp}_{2m}(q)$ with $2m \geq 6$ and q even, and let $M = \mathrm{GO}^\pm_{2m}(q)$. Then $b(G, M \setminus G) = 2m$.*

Proof We shall use the isomorphism $\mathrm{Sp}_{2m}(q) \cong \mathrm{GO}_{2m+1}(q)$ to consider the equivalent actions of $H = \mathrm{GO}_{2m+1}(q)$ on $\mathcal{N}^\pm(H, 2m)$, where the natural module for H is $V = \mathbb{F}_q^{2m+1}$ with quadratic form Q as in Definition 4. That is, we shall consider the

Table 6 Bases for $H = \mathrm{GO}_{2m+1}(q) \cong \mathrm{Sp}_{2m}(q)$ on $\mathcal{N}^{\pm}(H, 2m)$, with q even

Let $X^2 + X + \lambda^2$ be irreducible. Let $A_i = \langle e_i, f_i \rangle$ and $B_i = \langle e_i + x, f_i + \lambda x \rangle$	
$\mathcal{N}$	$\mathcal{B}$
$\mathcal{N}^+(H, 2m)$	$\{T = \bigoplus_{i=1}^{m} A_i, \quad U_i = A_1 \oplus \cdots \oplus A_{i-1} \oplus \langle e_i, f_i + x \rangle \oplus A_{i+1} \oplus \cdots \oplus A_m,$ $V_j = A_1 \oplus \cdots \oplus A_{j-1} \oplus \langle e_j + x, f_j \rangle \oplus A_{j+1} \oplus \cdots \oplus A_m \quad \mid 1 \le i \le m, 1 \le j \le m-1\}$
$\mathcal{N}^-(H, 2m)$	$\{T = B_1 \oplus (\bigoplus_{i=2}^{m} A_i), \quad U_i = B_1 \oplus A_2 \oplus \cdots \oplus A_{i-1} \oplus \langle e_i, f_i + x \rangle \oplus A_{i+1} \oplus \cdots \oplus A_m,$ $V_j = B_1 \oplus A_2 \oplus \cdots \oplus A_{i-1} \oplus \langle e_j + x, f_j \rangle \oplus A_{i+1} \oplus \cdots \oplus A_m, \quad W_1 = A_1 \oplus B_2 \oplus A_3 \oplus \cdots \oplus A_m,$ $W_2 = \langle e_1, f_1 + x \rangle \oplus B_2 \oplus A_3 \oplus \cdots \oplus A_m \quad \mid 2 \le i \le m, \ 2 \le j \le m-1\}$

actions of H on non-degenerate $2m$-dimensional subspaces of $+$ and $-$ type, since the point stabiliser of H in these actions is $\mathrm{GO}^{\pm}_{2m}(q)$.

We shall first show that the set $\mathcal{B}$ in Table 6 is a base for H, and then show that $\mathcal{B}$ is of minimal size. First notice that (e_i, f_i), $(e_i, e_i + f_i + x)$, and $(e_i + f_i + x, f_i)$ are hyperbolic pairs, therefore A_i, $\langle e_i, f_i + x\rangle$ and $\langle e_i + x, f_i\rangle$ are 2-spaces of $+$ type. The basis of B_i is an elliptic pair, so in each case $\mathcal{B} \subseteq \Omega$.

Let $g \in H_{(\mathcal{B})}$. Then we shall show that $g = 1$. From $Q(x) = 1$ and $\langle x\rangle = \mathrm{Rad}(V) = V \cap V^{\perp}$, we deduce that $xg = x$. We first consider $\mathcal{N}^{-}(H, 2m)$. For $2 \leq i \leq m$, the element g stabilises

$$T \cap U_i = B_1 \oplus A_2 \oplus \cdots \oplus A_{i-1} \oplus \langle e_i\rangle \oplus A_{i+1} \oplus \cdots \oplus A_m,$$

and so stabilises $\mathrm{Rad}(T \cap U_i) = \langle e_i\rangle$. Hence there exists $\alpha_i \in \mathbb{F}_q$ such that $e_i g = \alpha_i e_i$, for $2 \leq i \leq m$. Similarly, $\mathrm{Rad}(T \cap V_i)^g = \mathrm{Rad}(T \cap V_i)$ so $f_i g = \alpha_i^{-1} f_i$, for $2 \leq i \leq m-1$. Since $m \geq 3$, the space $S := \langle A_2, \ldots, A_{m-1}\rangle$ is non-degenerate and stabilised by g, so g also stabilises

$$S^{\perp} \cap W_1 = \langle A_1, A_m, x\rangle \cap W_1 = \langle A_1, A_m\rangle.$$

Hence g stabilises $\langle A_1, A_m\rangle \cap W_2 = \langle e_1, A_m\rangle$, and so fixes the radical of this space, which is $\langle e_1\rangle$. Moreover, g stabilises $\langle e_1, A_m\rangle \cap T = A_m = \langle e_m, f_m\rangle$. Hence, since $e_m g = \alpha_m e_m$, Lemma 2(2) shows that $f_m g = \alpha_m^{-1} f_m$. In addition, the element g stabilises $A_m^{\perp} \cap \langle A_1, A_m\rangle = A_1$, and Lemma 2(2) now yields $f_1 g = \alpha_1^{-1} f_1$. Next, for $2 \leq i \leq m$ we deduce from

$$(f_i + x)\, g = \alpha_i^{-1} f_i + x \in U_i$$

that $\alpha_i = 1$, and the same follows for α_1 from $(f_1 + x)g \in W_2$.

The arguments for $\mathcal{N}^{+}(H, 2m)$ are very similar but easier. Consideration of $T \cap U_i$ shows that for all i there exists an $\alpha_i \in \mathbb{F}_q$ such that $e_i g = \alpha_i e_i$. Then an identical argument applied to $T \cap V_j$ shows that $f_i g = \alpha_i^{-1} f_i$ for $i \leq m-1$. Therefore, g stabilises

$$\langle A_1, \ldots, A_{m-1}\rangle^{\perp} \cap T = \langle e_m, f_m\rangle,$$

and so $f_m g = \alpha_m^{-1} f_m$, also. Finally, notice that

$$(f_i + x)\, g = \alpha_i^{-1} f_i + x \in U_i$$

for all i, and hence $\alpha_i = 1$, as required.

It remains only to show that these bases are of minimal size. Let the set $\mathcal{A} = \{T, S_1, \ldots, S_{2m-1}\}$ consist of $2m-1$ non-degenerate $2m$-spaces of V of sign ε (either $+$ or $-$). We shall show that $H_{(\mathcal{A})} \neq 1$. The stabiliser in H of T is $H_T = \mathrm{GO}^{\varepsilon}_{2m}(q)$, which acts naturally on T as $\mathrm{GO}^{\varepsilon}_{2m}(q)$. It suffices to show that the stabiliser in H_T of all of the spaces $T \cap S_i$ for $1 \leq i \leq 2m-2$ is nontrivial.

Since $\dim(T \cap S_i) = 2m - 1$, the restriction of B to $T \cap S_i$ is degenerate, and so $T \cap S_i$ has a one-dimensional radical $\langle v_i \rangle$. Hence the 2-point stabiliser H_{T,S_i} stabilises the subspace $\langle v_i \rangle$ of T. Furthermore, since T is non-degenerate, it follows that $\dim(v_i^\perp \cap T) = 2m - 1$, and so $T \cap S_i = T \cap v_i^\perp$. Hence H_{T,S_i} is equal to $H_{T,\langle v_i \rangle}$ and so $H_{(\mathcal{B})} = \cap_{i=1}^{2m-2} H_{T,S_i}$ contains $(H_T)_{\langle v_1 \rangle, \ldots, \langle v_{2m-2} \rangle}$. This group is nontrivial by Lemma 8. □

3 Proof of Theorem 1 for almost simple groups

In this section, we shall prove the following theorem, which in particular implies Theorem 1 for almost simple groups.

Theorem 3 *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive almost simple group of degree n that is not large base. If $b(G)$ is greater than $\lceil \log n \rceil + 1$, then $G = \mathrm{M}_{24}$, $n = 24$ and $b(G) = 7$.*

Furthermore, if $b(G) \geq \log n + 1$ then $(G, n, b(G)) \in \{(\mathrm{M}_{12}, 12, 5), (\mathrm{M}_{23}, 23, 6), (\mathrm{M}_{24}, 24, 7)\}$ or $G = \mathrm{PSp}_{2m}(2)$ with $m \geq 3$, $n = 2^{2m} - 2^{m-1}$ and $b(G) = 2m = \lceil \log n \rceil + 1$.

We shall first consider the standard actions of $\mathrm{Alt}(\ell)$ and $\mathrm{Sym}(\ell)$ on partitions, then the actions of the classical groups on totally singular and non-degenerate k-spaces, and (for the orthogonal groups in even characteristic) non-singular 1-spaces. Then we shall look at the action of groups with socle $\mathrm{PSp}_d(2^f)$ on the cosets of the normaliser of $\mathrm{GO}_d^{\pm}(2^f)$, before considering the remaining subspace actions. Finally, we will deal with the non-standard actions, and hence prove Theorem 3.

3.1 Action on partitions

We first consider the non-large-base standard actions of $\mathrm{Alt}(\ell)$ and $\mathrm{Sym}(\ell)$.

Theorem 4 *Let $s \geq 2$ and $t \geq 2$, with $\ell := st \geq 5$, and let G be $\mathrm{Sym}(\ell)$. Let Ω be the set of partitions of $\{1, 2, \ldots, \ell\}$ into s subsets of size t, and let $n = |\Omega|$. Then $b := b(G, \Omega) < \log n + 1$.*

Proof The degree n is $\ell!/(t!)^s s!$. If $t = 2$, then $s \geq 3$ and $n \geq \frac{6!}{2^3 \cdot 3!} = 15$. However, $b = 3$ by [7, Remark 1.6(ii)], so $b < \log n$. If $s \geq t \geq 3$, then $n \geq \frac{9!}{(3!)^3 3!} = 280$, whilst $b \leq 6$ by [1, Theorem 4(i)], so again $b < \log n$.

For the remaining cases, by [1, Theorem 4(ii)]

$$b \leq \lceil \log_s t \rceil + 3 \leq \log_s t + 4 = \log_s(\ell/s) + 4 = \log_s \ell + 3. \tag{7}$$

Next consider $s = 2$, so that $t \geq 3$. We check in Magma [3] that if $t = 3, 4, 5$ then b is at most 4, 5, and 5, respectively, whilst $n = 10, 35, 126$, and so $b < \log n + 1$ in each case. Assume therefore that $\ell \geq 12$. Then

$$n = \frac{\ell!}{2((\ell/2)!)^2} = \frac{\ell(\ell-1)\ldots(\ell-\ell/2+1)}{2(\ell/2)!} = \frac{\ell(\ell-1)\ldots(\ell/2+2)(\ell/2+1)}{(\ell/2)(\ell/2-1)\ldots 2 \cdot 2} > 2^{\ell/2}.$$

In particular, since $\ell \geq 12$, we deduce from (7) that

$$b \leq \log \ell + 3 < \frac{\ell}{2} + 1 \leq \log n + 1.$$

Next, let $s = 3$. We may assume that $t > s$, so $\ell \geq 12$. Then, reasoning as for $s = 2$, we deduce that $n \geq 2^{\ell/3} \cdot 3^{\ell/3} > 2^{2\ell/3}$. Hence $\log n > 2\ell/3$, so (7) yields

$$b \leq \log \ell + 3 < \frac{2\ell}{3} + 1 < \log n + 1.$$

We are therefore left with $4 \leq s < t$, so that $\ell \geq 20$. For all ℓ, the groups $\mathrm{Alt}(\ell)$ and $\mathrm{Sym}(\ell)$ have no core-free subgroups of index less than ℓ, so $\ell < n$. From (7) we deduce that

$$b \leq \log_s \ell + 3 = \frac{\log \ell}{\log s} + 3 \leq \frac{\log \ell}{2} + 3 \leq \log \ell + 1 < \log n + 1.$$

□

3.2 Subspace actions

We now prove Theorem 3 for the subspace actions of almost simple groups. First we record two lemmas concerning base size and automorphism groups.

Lemma 11 *Let G be a finite almost simple primitive permutation group on Ω with socle G_0 a non-abelian simple classical group, and let $G_0 \trianglelefteq G_1 \trianglelefteq G \leq \mathrm{Sym}(\Omega)$. If G/G_1 has a subnormal series of length s with all quotients cyclic, then $b(G) \leq b(G_1) + s$.*

Proof If (G_0, Ω) is not isomorphic to $(\mathrm{Alt}(\ell), \{1, \ldots, \ell\})$ with $\ell \in \{5, 6, 8\}$, then by [17, Theorem 1.2] each element of G has a regular cycle. It follows that stabilising one point for each cyclic quotient suffices to extend a base for G_1 to one for G.

Let (G_0, Ω) be $(\mathrm{Alt}(\ell), \{1, \ldots, \ell\})$ for some $\ell \in \{5, 6, 8\}$. Then $G \leq \mathrm{Sym}(\ell)$, since the other automorphisms of $\mathrm{Alt}(6)$ do not act on 6 points, and so the result follows from $b(\mathrm{Sym}(\ell), \Omega) = b(\mathrm{Alt}(\ell), \Omega) + 1$. □

Recall the meaning of $\mathcal{S}(G, k)$ and $\mathcal{N}^\epsilon(G, k)$ from Notation 3. The following bounds are established in [18, Proof of Theorem 3.3].

Lemma 12 *Let G_0 be a simple classical group.*

(i) If $(G_0, k) \neq (\mathrm{P}\Omega^+_{2m}(q), m)$ then $b(G_0, \mathcal{S}(G, k)) \leq d/k + 10$.
(ii) $b(G_0, \mathcal{N}(G, k)) \leq d/k + 11$.
(iii) If $G_0 = \mathrm{PSL}_d(q)$ then $b(G_0, \mathcal{S}(G, k)) \leq d/k + 5$.

Lemma 13 *Let G be almost simple with socle G_0 one of $\mathrm{P}\Omega^-_4(q)$, $\mathrm{P}\Omega_5(q)$ or $\mathrm{P}\Omega^\pm_6(q)$. Assume that $G_0 \neq \mathrm{P}\Omega^-_4(q)$ for $q \leq 3$. Let $\Omega = \mathcal{N}^\epsilon(G, 1)$, with $\epsilon = +, -$ or blank, and let $n = |\Omega|$. Then $b := b(G) < \log n + 1$.*

Proof First let $d = 4$, so that $q \geq 4$. Then $\mathrm{Aut}(G_0)/\mathrm{PGO}_4^-(q)$ has a normal series of length at most two with all quotients cyclic, so Lemmas 7 and 11 imply that $b \leq 5$. From [6, Table 4.1.2] we see that

$$n = \frac{q\left(q^2+1\right)}{(q-1,2)} > 2^6,$$

so the result follows.

Next let $d = 5$, so that q is odd. Then $\mathrm{Aut}(G_0)/\mathrm{PGO}_5(q)$ is cyclic, so Lemmas 7 and 11 yield $b \leq 6$, whilst from [6, Table 4.1.2] we see that

$$n = \frac{q^2\left(q^4-1\right)}{2\left(q^2 \mp 1\right)} \geq 36 > 2^5,$$

so the result follows.

Finally, let $d = 6$. From Lemmas 7 and 11 we deduce that $b \leq 5$ if $q = 2$, and $b \leq 7$ otherwise. Moreover, by [6, Table 4.1.2],

$$n \geq \frac{q^2(q^3+1)}{(q-1,2)} > \begin{cases} 2^5 & \text{if } q = 2 \\ 2^6 & \text{if } q \geq 3 \end{cases}$$

as required. □

Proposition 2 *Let $d \geq 8$ be even, and let G be almost simple with socle $G_0 = \mathrm{P}\Omega_d^\varepsilon(q)$. Let Ω be $\mathcal{S}(G,k)$ or $\mathcal{N}^\epsilon(G,k)$, where $\epsilon = +, -$ or blank, and let $n = |\Omega|$. If G acts primitively on Ω then $b := b(G) < \log n + 1$.*

Proof We shall use throughout the proof the fact that if $G_0 \neq \mathrm{P}\Omega_8^+(q)$, or if $\Omega \neq \mathcal{S}(G,2)$ (see, for example, [4, Table 8.50]), then G/G_0 has a normal series with all quotients cyclic of length at most three, and less if $q = 2$ or q is prime, so that $b(G) \leq b(G_0) + 3$, by Lemma 11. Furthermore, under the same conditions, $b(G) \leq b(\mathrm{PGO}_d^\varepsilon(q)) + 2$, by the same lemma. If $G_0 = \mathrm{P}\Omega_8^+(p^f)$ and p is odd then $\mathrm{Out}(G_0) \cong \mathrm{Sym}(4) \times C_f$, whilst if $p = 2$ then $\mathrm{Out}(G_0) \cong \mathrm{Sym}(3) \times C_f$.

First consider $\Omega = \mathcal{S}(G,k)$. By [19, Tables 3.5E and F] we may assume that $1 \leq k \leq d/2$, and $k \leq d/2 - 1$ if $\varepsilon = -$. If $k \leq d/2 - 1$ then by [6, Table 4.1.2, Cases VI and VII]

$$n = \frac{\left(q^{\frac{d}{2}} \mp 1\right)\left(q^{\frac{d}{2}-k} \pm 1\right)\prod_{i=\frac{d}{2}-k+1}^{\frac{d}{2}-1}\left(q^{2i}-1\right)}{\prod_{i=1}^{k}\left(q^i-1\right)} \tag{8}$$

$$\geq \frac{\left(q^{\frac{d}{2}} \mp 1\right)\left(q^{\frac{d}{2}-1} \pm 1\right)}{q-1}\prod_{i=2}^{k}\left(q^i+1\right) > q^{d-k-1}\prod_{i=2}^{k} q^i \geq q^{d-2+\frac{k(k-1)}{2}}. \tag{9}$$

If $k = 1$ then Lemma 3 shows that $b \leq d + 1$, with tighter bounds when $q \leq 3$, whilst (9) gives $n > q^{d-2}$, so

$$\log n + 1 > (d - 2) \log q + 1 \geq b.$$

Similarly, if $k = 2$ then we deduce from Lemma 5 that $b \leq d/2 + 3$ if q is even or prime, and $b \leq d/2 + 5$ in general. From (9), we see that $\log n + 1 > (d - 1) \log q + 1$, so the result follows.

Next we consider the case $3 \leq k \leq d/2 - 1$, so that $b(G_0, \Omega) \leq d/k + 10$ by Lemma 12(i). First assume that $q \leq 3$ and $k = 3$. We calculate in Magma that if $(d, q) = (8, 2)$ then $b \leq 4$. For $(d, q) = (8, 3)$ we use the exact value of n and the fact that $b(G) \leq b(G_0) + 2$ to see that $\log n + 1 > 15 \geq b$. For $d \geq 10$ we see from (8) that

$$n \geq \frac{\left(q^{\frac{d}{2}} \mp 1\right)\left(q^{\frac{d}{2}-3} \pm 1\right)}{q - 1}\left(q^4 + 1\right)\left(q^2 + 1\right)\left(q^3 + 1\right) > q^{d-4}q^{4+3+2} \geq q^{d+5}.$$

Hence if $q = 2$ then

$$\log n + 1 \geq d + 6 \geq \frac{d}{3} + 11 \geq b,$$

and if $q = 3$ then

$$\log n + 1 \geq \frac{3}{2}(d + 5) + 1 \geq \frac{d}{3} + 13 \geq b.$$

In the remaining cases $k \geq 4$ or $q \geq 4$, so the result follows by a routine calculation from (9).

Finally consider $k = d/2$, so that $\varepsilon = +$. From [6, Table 4.1.2],

$$n = \prod_{i=1}^{\frac{d}{2}}\left(q^i + 1\right) \geq \prod_{i=1}^{\frac{d}{2}} q^i = q^{\frac{d(d+2)}{8}} \geq q^{10}.$$

It is shown in [18] that $b(G_0) \leq 9$, so $b \leq 10$ when $q = 2$, and $b \leq 12$ otherwise, and the result follows.

We now consider $\Omega = \mathcal{N}^{\epsilon}(G, k)$, with $\epsilon \in \{+, -\}$ or blank. The stabiliser of an element of Ω also stabilises a non-degenerate $d - k$ space, of the opposite sign if $\varepsilon = -$ and k is even, and of the same sign otherwise. Thus by considering the stabiliser of spaces of type $+$, $-$ and $\circ$, we may assume that $k \leq d/2$.

First assume that k is even, so that $2 \leq k \leq d/2$, and if $k = d/2$ then $\varepsilon = -$, by our assumption that G acts primitively. Then we deduce from [6, Table 4.1.2, Cases

X, XI, XIII] (by replacing d by $d-k$ if $\epsilon = +$ and $\varepsilon = -$) that

$$\begin{aligned} n &= \frac{q^{\frac{k(d-k)}{2}}\left(q^{\frac{d}{2}}-\varepsilon\right)\prod_{i=\frac{d-k}{2}}^{\frac{d}{2}-1}\left(q^{2i}-1\right)}{2\left(q^{\frac{k}{2}}-\epsilon\right)\left(q^{\frac{d-k}{2}}-\varepsilon\epsilon\right)\prod_{i=1}^{\frac{k}{2}-1}(q^{2i}-1)} \\ &= \frac{q^{\frac{k(d-k)}{2}}\left(q^{\frac{d}{2}}-\varepsilon\right)\left(q^{d-2}-1\right)}{2\left(q^{\frac{k}{2}}-\epsilon\right)\left(q^{\frac{d-k}{2}}-\varepsilon\epsilon\right)}\prod_{i=1}^{\frac{k}{2}-1}\frac{q^{d-k-2+2i}-1}{q^{2i}-1}. \end{aligned} \tag{10}$$

If $k = 2$ then it follows that $n > q^{2d-6} \geq q^{d+2}$, whilst from Lemmas 9 and 10 we see that $b \leq d/2 + 2 < \log n + 1$. For $k \geq 4$, notice that

$$\begin{aligned} n &> \frac{q^{\frac{k(d-k)}{2}}\left(q^{\frac{d}{2}}-\varepsilon\right)\left(q^{d-2}-1\right)}{4\left(q^{\frac{d}{2}}-1\right)}\prod_{i=1}^{\frac{k}{2}-1}q^{d-k-2} \\ &\geq \frac{1}{4}q^{\frac{k(d-k)}{2}+d-3+(d-k-2)(\frac{k}{2}-1)} = \frac{1}{4}q^{kd-k^2-1}. \end{aligned}$$

The quadratic $kd - k^2 - 1$ attains its minimum for $4 \leq k \leq d/2$ at $k = 4$, so

$$\log n + 1 > (4d-17)\log q - 1 \geq 4d - 18.$$

Then by Lemma 12(ii), $b \leq \frac{d}{4} + 14$. If $d \geq 10$, then

$$\log n + 1 \geq 4d - 18 \geq \frac{d}{4} + 14,$$

so it only remains to consider $(d, k, \varepsilon) = (8, 4, -)$. In this case, $(4d-17)\log q - 1 \geq 15\log q + 1$ and the result follows easily for $q \geq 3$. If $q = 2$ then $\mathrm{Out}(G_0)$ is cyclic, hence by Lemmas 11 and 12(ii), $b \leq 14$ and the result follows.

Now let k be odd, so without loss of generality $1 \leq k < d/2$. By [6, Table 4.1.2, Cases IX, XII, XIV]

$$n = \frac{q^{\frac{(kd-k^2-1)}{2}}\left(q^{\frac{d}{2}}-\varepsilon\right)\prod_{i=\frac{d-k+1}{2}}^{\frac{d}{2}-1}\left(q^{2i}-1\right)}{(2,q-1)\prod_{i=1}^{\frac{k-1}{2}}\left(q^{2i}-1\right)}.$$

If $k = 1$ then $n > \frac{q^{d-2}}{(2,q-1)}$, whilst Lemma 7 shows that $b \leq d+1$, with tighter bounds when $q \leq 3$, so the result follows easily. If $k \geq 3$ then q is odd, with $b \leq d/3 + 14$ by Lemma 12(ii). Now

$$n = \frac{1}{2}q^{\frac{(kd-k^2-1)}{2}}\left(q^{\frac{d}{2}}-\varepsilon\right)\prod_{i=1}^{\frac{k-1}{2}}\frac{q^{d-k-1+2i}-1}{q^{2i}-1},$$

$$n > \frac{1}{2}q^{\frac{(kd-k^2-1)}{2}+\frac{d}{2}-1}\prod_{i=1}^{\frac{k-1}{2}} q^{d-k-1} = \frac{1}{2}q^{\frac{kd-k^2-d-3}{2}+\frac{k-1}{2}(d-k-1)}$$
$$= \frac{1}{2}q^{kd-k^2-1} \geq \frac{1}{2}q^{3d-9-1},$$

where the last inequality follows as in the case k even, so the proof is complete. □

Proposition 3 *Let $d \geq 7$ and let G be almost simple with socle $G_0 = \mathrm{P}\Omega_d^\circ(q)$. Let Ω be $\mathcal{S}(G,k)$ or $\mathcal{N}^\pm(G,k)$, and let $n = |\Omega|$. If G acts primitively on Ω then $b := b(G) < \log n + 1$.*

Proof We shall use throughout the proof the fact that $\mathrm{Out}(G_0)$ has a normal series with at most two cyclic quotients, and $\mathrm{Aut}(G_0)/\mathrm{PGO}_d(q)$ is cyclic, so $b \leq b(G_0, \Omega) + 2$ and $b \leq b(\mathrm{PGO}_d(q), \Omega) + 1$, by Lemma 11.

First let $\Omega = \mathcal{S}(G,k)$. Then $1 \leq k \leq (d-1)/2$ and by [6, Table 4.1.2, Case VII]

$$n = \frac{\prod_{i=\frac{d-2k+1}{2}}^{\frac{d-1}{2}} \left(q^{2i}-1\right)}{\prod_{i=1}^{k}\left(q^i-1\right)}. \tag{11}$$

If $k \leq (d-3)/2$, then

$$n \geq \frac{\left(q^{d-1}-1\right)}{(q-1)} \cdot \frac{\left(q^{2k}-1\right)\ldots\left(q^4-1\right)}{\left(q^k-1\right)\ldots\left(q^2-1\right)} \geq q^{d-2}q^{\sum_{i=2}^{k} i} = q^{d-3+\frac{k(k+1)}{2}}.$$

If $k = 1$ then $n > q^{d-2} \geq 3^{d-2}$, and from Lemma 3 we deduce that $b \leq d+1$, as required. If $k = 2$ then $n \geq q^d$, whilst Lemma 5 gives $b \leq \lceil d/2 \rceil + 1$. If instead $3 \leq k \leq (d-3)/2$ then $d \geq 9$ and $n \geq q^{d+3}$. Hence

$$\log n + 1 \geq (d+3)\log q + 1 \geq 3d/2 + 11/2 \geq d/3 + 12 \geq b,$$

by Lemma 12(i).

Finally, assume that $k = (d-1)/2$, so that (11) simplifies to

$$n = \prod_{i=1}^{\frac{d-1}{2}} \left(q^i+1\right) \geq q^{\frac{d-1}{4}\left(\frac{d+1}{2}\right)} = q^{(d^2-1)/8}.$$

For $(d,q) \in \{(7,3),(7,5)\}$ the result follows from a MAGMA calculation. Otherwise, by Lemma 12(i),

$$b \leq \frac{d}{(d-1)/2} + 10 + 2 < 3 + 12 = 15,$$

so we are done.

Now let $\Omega = \mathcal{N}^{\pm}(G,k)$, so that without loss of generality k is even. Then by [6, Table 4.1.2, Cases XV and XVI]

$$n = \frac{q^{\frac{k(d-k)}{2}} \prod_{i=\frac{d-k+1}{2}}^{\frac{d-1}{2}} \left(q^{2i}-1\right)}{2\left(q^{\frac{k}{2}} \mp 1\right) \prod_{i=1}^{\frac{k}{2}-1} \left(q^{2i}-1\right)} = \frac{q^{\frac{k(d-k)}{2}} \left(q^{d-1}-1\right)}{2\left(q^{\frac{k}{2}} \mp 1\right)} \prod_{i=1}^{\frac{k}{2}-1} \frac{q^{d-k-1+2i}-1}{q^{2i}-1}$$
$$\geq \frac{1}{4} q^{\frac{k(d-k)}{2} + \left(d-1-\frac{k}{2}\right) + (d-k-1)\left(\frac{k}{2}-1\right)} = \frac{1}{4} q^{kd-k^2}$$

If $k = d-1$ then $n \geq \frac{1}{4}q^{d-1} \geq \frac{1}{4}3^{d-1}$, whilst $b = b(G, \mathcal{N}^{\pm}(G,1)) \leq d < \log n + 1$, by Lemma 7. Similarly, if $k = 2$ then $n \geq \frac{1}{4}q^{2d-4} > q^d$, whilst $b \leq \lceil d/2 \rceil + 1 < \log n + 1$ by Lemmas 9 and 10. For $4 \leq k \leq d-3$, the quadratic $-k^2 + kd$ attains its minimum at $k = d-3$, so $\log n + 1 \geq (3d-9)\log q - 1$. Now, Lemma 12(ii) yields $b \leq d/4 + 13$, which is less than

$$(3d+13)/2 \leq d \log q + (2d-9)\log q - 1 = \log n + 1,$$

so the proof is complete. □

Proposition 4 *Let $d \geq 4$, and let G be almost simple with socle $G_0 = \mathrm{PSp}_d(q)$, with $(d,q) \neq (4,2)$. Let Ω be $\mathcal{S}(G,k)$ or $\mathcal{N}(G,k)$, and let $n = |\Omega|$. If G acts primitively on Ω, then $b := b(G) < \log n + 1$.*

Proof We shall use throughout the proof the fact that $\mathrm{Out}(G_0)$ has a normal series with at most two cyclic quotients, so $b(G,\Omega) \leq b(G_0,\Omega) + 2$, with $b(G,\Omega) \leq b(G_0,\Omega) + 1$ if $q > 2$ is even or prime, by Lemma 11.

First let $\Omega = \mathcal{S}(G,k)$. Then $1 \leq k \leq d/2$, and by [6, Table 4.1.2]

$$n = \frac{\prod_{i=\frac{d}{2}-k+1}^{\frac{d}{2}} \left(q^{2i}-1\right)}{\prod_{i=1}^{k} \left(q^i-1\right)} = \prod_{i=1}^{k} \frac{q^{d-2k+2i}-1}{q^i-1}. \tag{12}$$

If $k = 1$ then $n = (q^d-1)/(q-1) > q^{d-1}$. By Lemma 3, $b \leq d+2$, with $b \leq d$ if $q = 2$ and $b \leq d+1$ if $q = 3$. The result now follows from a straightforward calculation, since $d \geq 4$.

If $k = 2$ and $d \geq 6$ then $b \leq d$, by Lemma 5, whilst $\log n + 1 > (2d-5) + 1 \geq b$. If $k = 2$ and $d = 4$ then Lemma 5 implies that $b(G_0,\Omega) \leq 4$ and a routine calculation shows that $b < \log n + 1$.

If $k \geq 3$ then Lemma 12(i) yields $b \leq \frac{d}{k} + 12$, with $b \leq \frac{d}{k} + 11$ when $q \leq 8$. First suppose that $d - 2k \geq 2$, so that $d \geq 8$. If $(d,q) = (8,2)$ then we verify the result in MAGMA. Otherwise, we notice that $n > |\mathcal{S}(\mathrm{PGO}_d^{\pm}(q),k)|$, and our upper bounds on b are less than the corresponding bounds for the orthogonal groups, so the result follows by the same calculations as in the proof of Proposition 2. We may therefore

assume that $k = \frac{d}{2}$, so that $b \leq 14$ in general, and $b \leq 13$ if $q \leq 8$. In this case

$$n = \prod_{i=1}^{\frac{d}{2}} (q^i + 1) \geq q^{\frac{d(d+2)}{8}},$$

so if $d \geq 10$ then the result is immediate. For $d = 6$ and $q \leq 4$, a MAGMA calculation establishes the result, whilst if $q \geq 5$ then $\log n + 1 > 14 \geq b$. For $d = 8$, if $q = 2$ then $\log n + 1 > 12 \geq b$, whilst for $q \geq 3$ we deduce that $\log n + 1 > 16 > b$.

Next let $\Omega = \mathcal{N}(G, k)$. Then k is even and without loss of generality $k \leq d/2 - 1$. By [6, Table 4.1.2]

$$n = \frac{q^{\frac{k(d-k)}{2}} \prod_{i=\frac{d-k+2}{2}}^{\frac{d}{2}} (q^{2i} - 1)}{\prod_{i=1}^{\frac{k}{2}} (q^{2i} - 1)}.$$

If $k = 2$ then $d \geq 6$ so

$$\log n + 1 \geq ((d-2) + (d-2)) \log q + 1 > d \geq b,$$

by Lemma 9. If $k \geq 4$ then from $d \geq 2k + 2$ we deduce that

$$q^{\frac{k(d-k)}{2}} \geq q^{\frac{k(k+2)}{2}} \geq q^{12} \text{ and } \left(q^{d-k+2} - 1\right) > q^2 \left(q^2 - 1\right) \left(q^k - 1\right),$$

so

$$\prod_{i=\frac{d-k+2}{2}}^{\frac{d}{2}} \left(q^{2i} - 1\right) \geq \left(q^d - 1\right) q^2 \prod_{i=1}^{\frac{k}{2}} \left(q^{2i} - 1\right).$$

Putting these together shows that $n \geq q^{12}(q^d - 1)q^2 > q^{d+13}$, so the result follows from Lemma 12(ii). □

Proposition 5 *Let $d \geq 3$, let G be almost simple with socle $G_0 = \mathrm{PSU}_d(q)$, let Ω be $\mathcal{S}(G, k)$ or $\mathcal{N}(G, k)$, and let $n = |\Omega|$. Then $b := b(G) < \log n + 1$.*

Proof We shall use throughout the proof the facts that $\mathrm{Aut}(G_0)/\mathrm{PGU}_d(q)$ is cyclic, whilst $\mathrm{Out}(G_0)$ has a normal series with two cyclic quotients, so it follows from Lemma 11 that $b(G, \Omega) \leq b(\mathrm{PGU}_d(q), \Omega) + 1$ and $b(G, \Omega) \leq b(G_0, \Omega) + 2$.

First let $\Omega = \mathcal{S}(G, k)$. Then by [6, Table 4.1.2]

$$n = \frac{\prod_{i=d-2k+1}^{d} \left(q^i - (-1)^i\right)}{\prod_{i=1}^{k} \left(q^{2i} - 1\right)} = \prod_{i=1}^{k} \frac{\left(q^{d-2k+2i-1} - (-1)^{d-1}\right) \left(q^{d-2k+2i} - (-1)^d\right)}{q^{2i} - 1},$$

so $n > q^d$ if $k = 1$, $n > q^{2d-4}$ if $k = 2$, and

$$n \geq \prod_{i=1}^{k} \left(q^{d-2k+2i-1} + 1\right) \geq q^{(d-1)+(d-3)+(d-5)} = q^{3d-9} \text{ if } k \geq 3. \tag{13}$$

If $k = 1$ then $b \leq d + 1 \leq \log n + 1$ by Lemma 3, so let $k = 2$. If $(d, q) = (4, 2)$ then a MAGMA calculation shows the result, and otherwise if $d = 4$ then $b \leq 6 \leq 4 \log q + 1 < \log n + 1$, by Lemma 5, as required. If $d \geq 5$ then we deduce from Lemma 5 that $b \leq d \leq \log n + 1$.

Finally, let $k \geq 3$, so that $d \geq 6$. For $(d, q) \in \{(6, 2), (6, 3), (7, 2), (7, 3)\}$ we verify the result computationally. Otherwise, $b \leq \frac{d}{k} + 12 \leq d/3 + 12$ by Lemma 12(i). If $d \geq 8$ then (13) gives

$$\log n + 1 \geq 3d - 8 \geq \frac{d}{3} + 12 \geq b,$$

as required. Similarly, if $q \geq 4$ then $\log n + 1 \geq 2(3d - 9) + 1 \geq d/3 + 12 \geq b$, which covers all the remaining cases.

Now let $\Omega = \mathcal{N}(G, k)$. Then by [6, Table 4.1.2]

$$n = \frac{q^{k(d-k)} \prod_{i=d-k+1}^{d} \left(q^i - (-1)^i\right)}{\prod_{i=1}^{k} \left(q^i - (-1)^i\right)}.$$

If $k \leq 2$ then $n > q^d$, and the result follows easily from Lemma 6 and Lemma 9. For $k \geq 3$, we get

$$\prod_{i=d-k+1}^{d} \left(q^i - (-1)^i\right) \geq \left(q^d - (-1)^d\right) \prod_{i=1}^{k} \left(q^i - (-1)^i\right),$$

because $d \geq 2k + 1 \geq 7$. Hence $n \geq q^{k^2+k}(q^d - (-1)^d) \geq q^{d+11}$, and the result follows from Lemma 12(ii). □

Proposition 6 *Let $d \geq 2$ and when $d = 2$, let $q \geq 7$. Let G be almost simple with socle $G_0 = \mathrm{PSL}_d(q)$, let $\Omega = \mathcal{S}(G, k)$, and let $n = |\Omega|$. Then $b := b(G) < \log n + 1$.*

Proof The group $\mathrm{Out}(G_0)$ has a normal series with all quotients cyclic of length at most three, and G/G_0 has such a series with length at most two if $k \neq d/2$, or if $d = 2$, or if q is prime; and is cyclic if more than one of these conditions hold. Hence by Lemma 11, $b \leq b(G_0, \Omega) + \ell$, where $\ell = 3$ in general, but with smaller values of ℓ for the special cases above.

First let $k = 1$, so that $n = (q^d - 1)/(q - 1) > q^{d-1}$, whilst $b \leq d + 2$ by Lemma 1, with smaller bounds if $q \leq 3$. The result follows from a lengthy but straightforward calculation, using $n = q + 1 \geq 8$ when $d = 2$.

If $k = 2$ then $n > q^{2d-4}$. If $d = 4$ and $q \leq 3$ then a MAGMA calculation shows that $b \leq 5 < \log n$, and if $d = 4$ and $q > 3$ then $b \leq 5 + 2 < \log n$, by Lemma 4. If $d > 4$ then $b \leq \lceil d/2 \rceil + 3 < \log n + 1$ by Lemma 4.

Assume finally that $d/2 \geq k \geq 3$, so that $d \geq 6$, and

$$n = \frac{q^d - 1}{q - 1} \cdot \frac{q^{d-1} - 1}{q^2 - 1} \cdot \frac{q^{d-2} - 1}{q^3 - 1} \prod_{i=1}^{k-3} \frac{\left(q^{d-k+i} - 1\right)}{\left(q^{i+3} - 1\right)} > q^{(d-1)+3+1} = q^{d+3}.$$

Then from Lemma 12(iii), we deduce that $b \leq d/3 + 8 \leq d + 4 \leq \log n + 1$. □

We now meet the unique infinite family of examples that attains the upper bound in Theorem 1.

Proposition 7 *Let $q = 2^f$, let $d = 2m \geq 4$, and let G be almost simple with socle $G_0 = \mathrm{Sp}_d(q)$. Assume that $(d, q) \neq (4, 2)$. Let $M = N_G(\mathrm{GO}_d^\epsilon(q))$, let $\Omega = M \setminus G$, let $n = |\Omega|$, and let $b = b(G)$.*

If $\epsilon = -$ and $q = 2$ then $\log n + 1 < b = \lceil \log n \rceil + 1$. Otherwise, $b < \log n + 1$.

Proof We calculate that $n = |\mathrm{Sp}_d(q) : \mathrm{GO}_d^\epsilon(q)| = q^m(q^m + \epsilon)/2$. If $q = 2$ then $b = 2m$ by Proposition 1. If $\epsilon = +$ then $n > 2^{2m-1}$, hence $\log n + 1 > b$. If $\epsilon = -$ then $\lceil \log n \rceil + 1 = 2m = b$.

It is proved in [18] that $b(G_0, \Omega) \leq 2m + 1$, so $b \leq 2m + 2$ by Lemma 11 since $\mathrm{Out}(G_0)$ is cyclic. Therefore if $q \geq 4$ then

$$\log n + 1 > \log(q^{2m-1}/2) + 1 = (2m - 1) \log q \geq 4m - 2 \geq b,$$

and the proof is complete. □

Our final result in this subsection deals with all of the remaining subspace actions.

Proposition 8 *Let G be an almost simple classical group, with a primitive subspace action on a set Ω of size n, with point stabiliser H. Assume that Ω is not a G-orbit of totally singular, non-degenerate, or non-singular subspaces, and that if the group $G_0 = \mathrm{soc}(G) = \mathrm{Sp}_{2m}(2^f)$ then $(G_0 \cap H) \neq \mathrm{GO}_{2m}^{\pm}(2^f)$. Then $b := b(G) < \log n + 1$.*

Proof Definition 1 implies that G is not simple, and H is a novelty maximal subgroup of G. Consulting [19] and [4], we see that one of the following holds:

(i) $G_0 = \mathrm{PSL}_d(q)$, $d \geq 3$ and $G \not\leq \mathrm{P\Gamma L}_d(q)$;
(ii) $G_0 = \mathrm{PSp}_4(q)$, q even and $G \not\leq \mathrm{PC\Gamma Sp}_4(q)$;
(iii) $G_0 = \mathrm{P\Omega}_8^+(q)$ and $G \not\leq \mathrm{PCO}_8^+(q)$ (in the notation of [4, Table 1.2]).

In particular, from [4], in each case there exists a group G_1 such that $G_0 \trianglelefteq G_1 \trianglelefteq G$, the quotient G/G_1 has a normal series of length at most two with all quotients cyclic, and $H \cap G_1$ is a subgroup of the stabilizer H_1 in G_1 of a totally singular k-space, of index greater than four. Let Ω_1 denote the right coset space of H_1 in G_1 and let $b_1 = b(G_1, \Omega_1)$. Then there exist $x_1, \ldots, x_{b_1} \in G_1$ such that $H_1^{x_1} \cap \cdots \cap H_1^{x_{b_1}}$ is trivial, so $H^{x_1} \cap \cdots \cap H^{x_{b_1}} \cap G_1$ is also trivial. By Lemma 11, $b \leq b_1 + 2$.

Finally, notice that $n \geq 4|\Omega_1|$ by the Orbit-Stabiliser Theorem, so if $b_1 < \log|\Omega_1| + 1 = \log 2|\Omega_1| \leq \log n - 1$, then $b < \log n + 1$. The result is now immediate from Propositions 6, 4 and 2. □

3.3 Proof of Theorem 3

Proof Let $G_0 = \mathrm{soc}(G)$. The only non-large-base almost simple primitive groups of degree $n \leq 8$ are the actions of $\mathrm{Alt}(5)$ and $\mathrm{Sym}(5)$ on 6 points, of $\mathrm{PSL}_3(2)$ on 7 points, and of $\mathrm{PSL}_2(7)$ and $\mathrm{PGL}_2(7)$ on 8 points, all of which have base size 3, which is less than $\log n + 1$. Hence the result holds for $n \leq 8$, and therefore for $b(G) \leq 4$.

Since the groups $\mathrm{PSL}_2(q)$ are isomorphic to many other simple groups, we shall consider them next. If $G_0 \cong \mathrm{PSL}_2(5)$ then all actions either have degree at most 6 or are large base, so let G_0 be $\mathrm{PSL}_2(q)$ for $q \geq 7$, and let $H = G_\omega$, for some $\omega \in \Omega$. We work through the choices for H, as described in [4, Table 8.1]. The result for $H \in \mathcal{C}_1$ follows from Proposition 6. Burness shows in [5, Table 3] that $b(G) \leq 3$ for the majority of the remaining choices of H. More precisely, he shows that $b(G) \leq 3$ if $H \in \mathcal{C}_2 \cup \mathcal{C}_3$, or if $H \in \mathcal{C}_5$ and $q = q_0^r$ with $r \neq 2$, or if $H \in \mathcal{C}_6$ and $q > 7$; or if $H \in \mathcal{C}_9$ and $q \neq 9$. We therefore need consider only the exceptions with $q \geq 7$. If $H \in \mathcal{C}_5$ and $q = q_0^2$, then $q_0 \geq 3$ and the action of G_0 on Ω is equivalent to that of $\mathrm{P}\Omega_4^-(q_0)$ on non-degenerate 1-spaces. If $q_0 = 3$ then $G_0 \cong \mathrm{Alt}(6)$, and the action is equivalent to the (large base) action on 2-sets. Hence we can assume that $q_0 \geq 4$, and the result follows from Lemma 13. If either $H \in \mathcal{C}_6$ and $q = 7$, or $H \in \mathcal{C}_9$ and $q = 9$, then $n \leq 7$, so the result follows. Thus for the remainder of the proof we shall assume that $G_0 \ncong \mathrm{PSL}_2(q)$.

Next, assume that the action of G is not standard. Burness, Guralnick and Saxl show in [7] that if $G_0 \cong \mathrm{Alt}(n)$ then $b(G) \leq 3$. For classical groups G, Burness shows in [5, Theorem 1.1] that either $n = 1408$ and $b(G) = 5$ or $b(G) \leq 4$. For the exceptional groups G, it is shown by Burness, Liebeck and Shalev in [9] that $b(G) \leq 6$; since the smallest degree of a faithful primitive representation of an exceptional group is 65 (see, for example, [14, Table B.2]), the result follows. Finally, Burness, O'Brien and Wilson show in [10] that if G is sporadic, then either $b(G) \leq 5$, or G is M_{23}, M_{24}, Co_3, Co_2, or $\mathrm{Fi}_{22}.2$, with a specified action. If $\log n + 1 \leq 5$, then $n \leq 16$, and the only sporadic group with a faithful primitive action on at most 16 points, other than M_{12} as given in the statement, is M_{11} on 11 or 12 points, with base size 4. The actions of M_{23} and M_{24} are given in the theorem statement, whilst the remaining actions have base size 6 and very large degree.

It remains to consider the standard actions that are not large base. If $G_0 = \mathrm{Alt}(\ell)$, then Ω is an orbit of partitions of $\{1, \ldots, \ell\}$, so $b(G) \leq \log n + 1$ by Theorem 4. Hence we may assume that G is a classical group in a subspace action.

If $G_0 = \mathrm{PSL}_d(q)$ then the result follows from Propositions 6 and 8. If instead $G_0 = \mathrm{PSU}_d(q)$ then we may assume that $d \geq 3$, and the result follows from Propositions 5 and 8.

If $G_0 = \mathrm{PSp}_d(q)$ then we may assume that $d \geq 4$, and $(d, q) \neq (4, 2)$, since $\mathrm{PSp}_4(2)' \cong \mathrm{PSL}_2(9)$. If the action is on k-spaces then the result follows from Proposition 4; if q is even and the point stabiliser is $\mathrm{GO}_d^{\pm}(q)$, then it follows from Proposition 7; and otherwise it follows from Proposition 8.

If $G_0 = \mathrm{P}\Omega_d^{\varepsilon}(q)$ then our assumption that $G_0 \ncong \mathrm{PSL}_2(q)$ implies that $d \geq 5$, so assume first that $d \in \{5, 6\}$, and let H_0 be whichever of $\mathrm{PSp}_4(q)$, $\mathrm{PSL}_4(q)$ or $\mathrm{PSU}_4(q)$ is isomorphic to G_0. If the action is on totally singular subspaces, then the action of

G_0 is equivalent to that of H_0 on totally singular subspaces. If the action is on non-degenerate 2-spaces, then the action of G_0 is equivalent to that of H_0 on the maximal subgroups in Class $\mathcal{C}_2$ or $\mathcal{C}_3$, and $b(G) \leq 3$ by [5, Table 3]. If the action is on an orbit of non-degenerate 1-spaces, then the result follows from Lemma 13, and otherwise it follows from Proposition 8. Hence we may assume that $d \geq 7$, and the result follows from Propositions 2, 3 and 8. □

4 Proof of Theorem 1

In this section, we prove Theorem 1.

Proposition 9 *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group of diagonal type and degree n. Then $b := b(G) \leq \max\{4, \log\log n\}$. In particular, $b < \log n$.*

Proof Let $\mathrm{soc}(G) = T^k$, where T is a non-abelian simple group and $k \geq 2$. Then $n = |T|^{k-1}$ and we may assume that $G = T^k.(\mathrm{Out}(T) \times \mathrm{Sym}(k))$. For the final claim, notice that $n \geq 60$, so $\log n > 4$, and so it suffices to prove the first claim.

If $k = 2$ then $b \leq 4$, as proved by Fawcett in [15]. It is also proved in [15] that if $k \geq 3$ then

$$b \leq \left\lceil \frac{\log k}{\log |T|} \right\rceil + 2. \tag{14}$$

If $3 \leq k \leq |T|$ then $b \leq 3$ and the result follows, so assume that $k > 60$. Then $n \geq 60^{60}$, so $\log\log n > 8$, and hence

$$b \leq \frac{\log k}{\log 60} + 3 \leq \frac{\log\log n}{5} + 3 \leq \log\log n.$$

□

We now consider product action type groups.

Proposition 10 *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group of product action type and degree n. If G is not large base then $b := b(G) < \log n + 1$.*

Proof Without loss of generality, we may assume that $G = H \wr \mathrm{Sym}(k)$, where $H \leq \mathrm{Sym}(\Gamma)$ is primitive, and either H is almost simple and not large base or H is of diagonal type. Let $|\Gamma| = m$, so $n = m^k$. Let $\{\gamma_1, \ldots, \gamma_c\} \subseteq \Gamma$ be a base of minimal size for the action of H on Γ, and let $\alpha_i' := (\gamma_i, \ldots, \gamma_i) \in \Gamma^k = \Omega$ for $1 \leq i \leq c$. It is shown in the proof of [11, Proposition 3.2] that there exists a set of $\lceil \log k \rceil$ 2-partitions of $\{1, \ldots, k\}$ such that the intersection in $\mathrm{Sym}(k)$ of the stabilizers of these partitions is trivial. Let $a = \lceil \log k \rceil$ and $r = \lfloor \log m \rfloor$. Then, as in the proof of [11, Lemma 3.8], there exists a subset $\{\alpha_1, \ldots, \alpha_{\lceil a/r \rceil}\}$ of Ω with the property that an element $g \in G$ which factorizes as $g = (1, \ldots, 1)\sigma$, where $1 \in H$ and $\sigma \in \mathrm{Sym}(k)$, fixes each α_i if and only if $\sigma = 1$. Hence, as noted in [11, Equation (13)], the set

$$\mathcal{B} := \left\{\alpha_1, \ldots, \alpha_{\lceil a/r \rceil}\right\} \cup \left\{\alpha_1', \ldots, \alpha_c'\right\}$$

is a base for G. In particular, we deduce that

$$b \leq \left\lceil \frac{\lceil \log k \rceil}{\lfloor \log m \rfloor} \right\rceil + b(H, \Gamma). \tag{15}$$

From Theorem 3 and Proposition 9, we see that either $b(H, \Gamma) \leq \lceil \log m \rceil + 1 \leq \log m + 2$, or $(H, m, b(H, \Gamma)) = (\mathrm{M}_{24}, 24, 7)$. In this latter case

$$b \leq \left\lceil \frac{\lceil \log k \rceil}{\lfloor \log m \rfloor} \right\rceil + b(H, \Gamma) \leq \left(\frac{1 + \log k}{4} + 1 \right) + 7 < k \log(24) + 1 \leq \log n + 1.$$

For the general case, assume first that $k \leq 4$, so that in particular $\lceil \log k \rceil \leq \lfloor \log m \rfloor$. Then by (15)

$$b \leq 1 + b(H, \Gamma) \leq \log m + 3 < 2 \log m + 1 \leq k \log m + 1 = \log n + 1.$$

If instead $k \geq 5$, then

$$\begin{aligned} b &\leq \left\lceil \frac{\lceil \log k \rceil}{\lfloor \log m \rfloor} \right\rceil + \log m + 2 \leq \frac{1 + \log k}{\lfloor \log m \rfloor} + \log m + 3 \leq \left(\frac{1 + \log k}{2} + 2 \right) + \log m + 1 \\ &< (k - 1) + \log m + 1 < k \log m + 1 = \log n + 1 \end{aligned}$$

as required. □

Finally, we state and prove a slightly more detailed version of Theorem 1.

Theorem 5 *Let G be a primitive subgroup of $\mathrm{Sym}(\Omega)$ with $|\Omega| = n$. Assume that G is not large base. Then $b := b(G) \geq \log n + 1$ if and only if G is one of the following.*

(i) A subgroup of $\mathrm{AGL}_d(2)$, with $b = d + 1 = \log n + 1$.
(ii) The group $\mathrm{Sp}_d(2)$, acting on the cosets of $\mathrm{GO}_d^-(2)$ with $d \geq 4$, in which case $\log n + 1 < b = \lceil \log n \rceil + 1$.
(iii) A Mathieu group M_n in its natural permutation representation with n in the set $\{12, 23, 24\}$. If $n = 12$ or 23 then $b = \lceil \log n \rceil + 1$, while if $n = 24$ then $b = 7 > \lceil \log n \rceil + 1$.

Proof We work through the cases of the O'Nan-Scott Theorem.

If G is of affine type, then without loss of generality $G = \mathrm{AGL}_d(p)$ with $n = p^d$, and the point stabiliser of G is $\mathrm{GL}_d(p)$, acting naturally on the set $\Omega = \mathbb{F}_p^d$. Let $\mathcal{B}$ be a base of minimal size for $\mathrm{GL}_d(p)$ on Ω. Then $\mathcal{B}$ is a basis for $\mathbb{F}_q^d$, so $b = |\mathcal{B}| + 1 = d + 1$ as required.

If G is of twisted wreath product type, then by [21, Section 3.6] the group G is a subgroup of a primitive product action group $H \wr P \leq \mathrm{Sym}(\Omega)$, with H of diagonal type. Hence the result follows from Proposition 10.

If G is almost simple, or of diagonal type, or of product action type, then the result follows from Theorem 3, Proposition 9 or Proposition 10, respectively. □

We conclude with a question.

Question 1 Which primitive groups $G \leq \mathrm{Sym}(n)$ satisfy $b(G) = \log n + 1$?

Notice that such a G must be a subgroup of $\mathrm{AGL}_d(2)$ for some d, and that if d is even then groups such as $2^d : \mathrm{Sp}(d, 2)$ have this property.

Acknowledgements The authors would like to thank the Isaac Newton Institute for Mathematical Sciences for support and hospitality during the programme "Groups, Representations and Applications: New perspectives", when work on this paper was undertaken. This work was supported by: EPSRC Grant Numbers EP/R014604/1 and EP/M022641/1. We are grateful to Professor Liebeck for several helpful suggestions.

References

1. Benbenishty, C., Cohen, J.A., Niemeyer, A.C.: The minimum length of a base for the symmetric group acting on partitions. Eur. J. Combin. **28**(6), 1575–1581 (2007)
2. Bochert, A.: Ueber die Zahl der verschiedenen Werthe, die eine Function gegebener Buchstaben durch Vertauschung derselben erlangen kann. Math. Ann. **33**(4), 584–590 (1889)
3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
4. Bray, J.N., Holt, D.F., Roney-Dougal, C.M.: The maximal subgroups of the low-dimensional finite classical groups. Lond. Math. Soc. Lecture Note Series, **407**. Cambridge University Press, Cambridge (2013)
5. Burness, T.C.: On base sizes for actions of finite classical groups. J. Lond. Math. Soc. (2) **75**(3), 545–562 (2007)
6. Burness, T.C., Giudici, M.: Classical groups, derangements and primes, Australian Mathematical Society Lecture Series, **25**. Cambridge University Press, Cambridge (2016)
7. Burness, T.C., Guralnick, R.M., Saxl, J.: On base sizes for symmetric groups. Bull. Lond. Math. Soc. **43**(2), 386–391 (2011)
8. Burness, T.C., Guralnick, R.M., Saxl, J.: On base sizes for algebraic groups. J. Eur. Math. Soc. **19**(8), 2269–2341 (2017)
9. Burness, T.C., Liebeck, M., Shalev, A.: Base sizes for simple groups and a conjecture of Cameron. Proc. Lond. Math. Soc. (3) **98**(1), 116–162 (2009)
10. Burness, T.C., O'Brien, E.A., Wilson, R.A.: Base sizes for sporadic simple groups. Israel J. Math. **177**, 307–333 (2010)
11. Burness, T.C., Seress, A.: On Pyber's base size conjecture. Trans. Am. Math. Soc. **367**(8), 5633–5651 (2015)
12. Cameron, P.J.: Finite permutation groups and finite simple groups. Bull. Lond. Math. Soc. **13**(1), 1–22 (1981)
13. Cameron, P.J., Kantor, W.M.: Random permutations: some group-theoretic aspects. Combin. Probab. Comput. **2**(3), 257–262 (1993)
14. Dixon, J.D., Mortimer, B.: Permutation Groups, Graduate Texts in Mathematics, 163. Springer-Verlag, New York (1996)
15. Fawcett, J.B.: The base size of a primitive diagonal group. J. Algebra **375**, 302–321 (2013)
16. Gill, N., Lodá, B., Spiga, P.: On the height and relational complexity of a finite permutation group. Nagoya Math. J., to appear. Arxiv preprint: arXiv:2005.03942

17. Guest, S., Spiga, P.: Finite primitive groups and regular orbits of group elements. Trans. Am. Math. Soc. **369**(2), 997–1024 (2017)
18. Halasi, Z., Liebeck, M.W., Maróti, A.: Base sizes of primitive groups: bounds with explicit constants. J. Algebra **521**, 16–43 (2019)
19. Kleidman, P.B., Liebeck, M.W.: The subgroup structure of the finite classical groups. London Mathematical Society Lecture Note Series, **129**. Cambridge University Press, Cambridge (1990)
20. Liebeck, M.W.: On minimal degrees and base sizes of primitive permutation groups. Arch. Math. (Basel) **43**(1), 11–15 (1984)
21. Praeger, C.E.: The inclusion problem for finite primitive permutation groups. Proc. Lond. Math. Soc. (3) **60**(1), 68–88 (1990)
22. Roney-Dougal, C.M., Siccha, S.: Normalisers of primitive permutation groups in quasipolynomial time. Bull. Lond. Math. Soc. **52**(2), 358–366 (2020)
23. Taylor, D.E.: The geometry of the classical groups. Sigma Series in Pure Mathematics, **9**. Heldermann Verlag, Berlin (1992)