On Relational Complexity and Base Size of Finite Primitive Groups

Veronica Kelsey and Colva M. Roney-Dougal
ON RELATIONAL COMPLEXITY AND BASE SIZE OF FINITE PRIMITIVE GROUPS

VERONICA KELSEY AND COLVA M. RONEY-DOUGAL

We show that if $G$ is a primitive subgroup of $S_n$ that is not large base, then any irredundant base for $G$ has size at most $5 \log n$. This is the first logarithmic bound on the size of an irredundant base for such groups, and it is the best possible up to a multiplicative constant. As a corollary, the relational complexity of $G$ is at most $5 \log n + 1$, and the maximal size of a minimal base and the height are both at most $5 \log n$. Furthermore, we deduce that a base for $G$ of size at most $5 \log n$ can be computed in polynomial time.

1. Introduction

Let $\Omega$ be a finite set. A base for a subgroup $G$ of $\text{Sym}(\Omega)$ is a sequence $\Lambda = (\omega_1, \ldots, \omega_l)$ of points of $\Omega$ such that $G(\Lambda) = G_{\omega_1, \ldots, \omega_l} = 1$. The minimum base size, denoted $b(G, \Omega)$ or just $b(G)$ if the meaning is clear, is the minimum length of a base for $G$. Base size has important applications in computational group theory; see, for example, [Sims 1970] for the importance of a base and strong generating set.

Liebeck [1984] proved the landmark result that with the exception of one family of groups, if $G$ is a primitive subgroup of $S_n = \text{Sym}([1, \ldots, n])$, then $b(G) < 9 \log n$. The members of the exceptional family are called large-base groups: they are product action or almost simple groups whose socle is one or more copies of the alternating group $A_r$ acting on $k$-sets. Moscatiello and Roney-Dougal [2022] improve this bound, and show that if $G$ is not large base, then either $G = M_{24}$ in its 5-transitive action of degree 24 or $b(G) \leq \lceil \log n \rceil + 1$. Here and throughout, all logarithms are to the base 2.

We say that a base $\Lambda = (\omega_1, \ldots, \omega_k)$ for a permutation group $G$ is irredundant if

$$G > G_{\omega_1} > G_{\omega_1, \omega_2} > \cdots > G_{\omega_1, \ldots, \omega_l} = 1.$$ 

If no irredundant base is longer than $\Lambda$, then $\Lambda$ is a maximal irredundant base, and we denote the length of $\Lambda$ by $I(G, \Omega)$ or $I(G)$.

From Liebeck’s $9 \log n$ bound on base size, a straightforward argument (see Lemma 1.2) shows that if $G$ is a primitive non-large-base subgroup of $S_n$, then

Keywords: permutation group, base size, relational complexity, computational complexity.
$I(G) \leq 9 \log^2 n$. However, Gill, Lodà and Spiga [Gill et al. 2022b] conjectured that for such groups $G$ there exists a constant $c$ such that $I(G) \leq c \log n$. They show that for some families of groups the conjecture holds with $c = 7$. Our main result establishes this conjecture, whilst also improving the constant.

**Theorem 1.1.** Let $G$ be a primitive subgroup of $S_n$. If $G$ is not large base, then

$$I(G) < 5 \log n.$$  

It turns out that there are infinitely many primitive groups for which the maximal irredundant base size is greater than $\lceil \log n \rceil + 1$. For example, if $d \geq 5$, $G = \text{PGL}_d(3)$ and $\Omega$ is the set of 1-spaces of $\mathbb{F}_3^d$, then by Theorem 3.1 $I(G, \Omega) = 2d - 1 > \lceil \log n \rceil + 1$. Hence, up to a multiplicative constant the bounds in Theorem 1.1 are the best possible.

Relational complexity has been extensively studied in model theory, see, for example, [Lachlan 1984]. A rephrasing of the definition, to make it easier to work with for permutation groups, was introduced more recently in [Cherlin et al. 1996]. For an excellent discussion and more context, see [Gill et al. 2022a]. Let $k, l \in \mathbb{N}$ with $k \leq l$, and let $\Lambda = (\lambda_1, \ldots, \lambda_l), \Sigma = (\sigma_1, \ldots, \sigma_l) \in \Omega^l$. We say that $\Lambda$ and $\Sigma$ are $k$-subtuple complete with respect to a subgroup $G$ of $\text{Sym}(\Omega)$, and write $\Lambda \sim_k \Sigma$, if for every subset of $k$ indices $i_1, \ldots, i_k$ there exists $g \in G$ such that $(\lambda_{g_i}^{\Lambda}, \ldots, \lambda_{g_i}^{\Lambda}) = (\sigma_{i_1}, \ldots, \sigma_{i_k})$. The relational complexity of $G$, denoted $\text{RC}(G)$, is the smallest $k$ such that for all $l \geq k$ and all $\Lambda, \Sigma \in \Omega^l$, if $\Lambda \sim_k \Sigma$, then $\Lambda \in \Sigma^G$. Cherlin [2000] gave examples of groups with relational complexity 2, called binary groups, and conjectured that this list is complete. In a dramatic breakthrough, Gill, Liebeck and Spiga [Gill et al. 2022a] have just announced a proof of this conjecture.

Let $\Lambda$ be a base for a permutation group $G$. Then $\Lambda$ is minimal if no proper subsequence of $\Lambda$ is a base. We denote the maximum size of a minimal base by $B(G)$. The height, $H(G)$, of $G$ is the size of the largest subset $\Delta$ of $\Omega$ with the property that $G_{(\Gamma)} \neq G_{(\Delta)}$ for each $\Gamma \subsetneq \Delta$. The following key lemma relates all of the group statistics studied in this paper.

**Lemma 1.2** [Gill et al. 2022b, Equation 1.1 and Lemma 2.1]. Let $G$ be a subgroup of $S_n$. Then

$$b(G) \leq B(G) \leq H(G) \leq I(G) \leq b(G) \log n,$$

and

$$\text{RC}(G) \leq H(G) + 1.$$  

Gill, Lodà and Spiga [Gill et al. 2022b] proved that if $G \leq S_n$ is primitive and not large base, then $H(G) < 9 \log n$; and so, $\text{RC}(G) < 9 \log n + 1$ and $B(G) < 9 \log n$.

It will follow immediately from Theorem 1.1 and Lemma 1.2 that we can tighten all of these bounds.
Corollary 1.3. Let $G$ be a primitive subgroup of $S_n$. If $G$ is not large base, then

$$\text{RC}(G) < 5 \log n + 1, \quad \text{B}(G) < 5 \log n, \quad \text{and} \quad \text{H}(G) < 5 \log n.$$  

Blaha [1992] proved that the problem of computing a minimal base for a permutation group $G$ is NP-hard. Furthermore, he showed that the obvious greedy algorithm to construct an irredundant base for $G$ produces one of size $O(b(G) \log \log n)$. Thus, if $G$ is primitive and not large base, it follows from Liebeck’s result that in polynomial time one can construct a base of size $O(\log n \log \log n)$. Since an irredundant base can be computed in polynomial time (see, for example, [Sims 1970]), we get the following corollary, which improves this bound to the best possible result, up to a multiplicative constant.

Corollary 1.4. Let $G$ be a primitive subgroup of $S_n$ which is not large base. Then a base for $G$ of size at most $5 \log n$ can be constructed in polynomial time.

(We note that using the bound on $B(G)$ from [Gill et al. 2022b], a very slightly more complicated argument would yield a similar result, but with $9 \log n$ in place of $5 \log n$.)

The paper is structured as follows. In Section 2, we prove some preliminary lemmas about $I(G)$. In Section 3, we let $\mathbb{F}$ be an arbitrary field and find upper and lower bounds on the size of an irredundant base for $\text{PGL}_d(\mathbb{F})$ acting on subspaces of $\mathbb{F}^d$, which differ by only a small amount. In Section 4, we prove a result which is a slight strengthening of Theorem 1.1 for almost simple groups. Finally, in Section 5, we complete the proof of Theorem 1.1.

2. Preliminary bounds on group statistics

Here we collect various lemmas about bases, and about the connection between $I(G)$ and other group statistics.

For a subgroup $G$ of $\text{Sym}(\Omega)$ and a fixed sequence $(\omega_1, \ldots, \omega_l)$ of points from $\Omega$, we let $G^{(i)} = G_{\omega_1,\ldots,\omega_i}$ for $0 \leq i \leq l$, so $G^{(0)} = G$. Furthermore, the maximum length of a chain of subgroups in $G$ is denoted by $\ell(G)$.

Lemma 2.1. Let $G$ be a subgroup of $S_n$.

(i) If $G$ is insoluble, then $I(G) < \log |G| - 1$.

(ii) If $G$ is transitive and $n \geq 5$, then $I(G) < \log |G| - 1$.

(iii) If $G$ is transitive and $b = b(G)$, then $I(G) \leq (b - 1) \log n + 1$.

Proof. Let $a$ be the number of prime divisors of $|G|$, counting multiplicity. Since $G$ is insoluble there exists a prime greater than $2^2$ dividing $|G|$, and so $|G| > 2^a + 1$. It is clear that $I(G) \leq \ell(G) \leq a$, and so Part (i) follows, and we assume from now on that $G$ is transitive.
Let \( l = I(G) \) with a corresponding base \( \Lambda = (\omega_1, \ldots, \omega_l) \). Since \( G \) is transitive, \( [G^{(0)} : G^{(1)}] = n \) by the Orbit–Stabiliser Theorem. From \( [G^{(i)} : G^{(j)}] \geq 2 \) for \( 2 \leq i \leq l \), it follows that \( |G| \geq 2^{l-1}n \). Hence, if \( n \geq 5 \), then \( |G| \geq 2^{l-1} \cdot 5 > 2^{l+1} \). Therefore, by taking logs Part (ii) follows.

Similarly, \( |G| \leq n^b \), and so \( 2^{l-1}n \leq |G| \leq n^b \). Hence,

\[
l - 1 + \log n = \log(2^{l-1}n) \leq \log |G| \leq b \log n,
\]

and so

\[
l \leq b \log n - \log n + 1 = (b - 1) \log n + 1
\]

and Part (iii) follows.

**Lemma 2.2.** Let \( G \) be a subgroup of \( \text{Sym}(\Omega) \), let \( l \geq 1 \) and let \( \Lambda = (\lambda_1, \ldots, \lambda_l) \in \Omega^l \). Then there exists a subsequence \( \Sigma \) of \( \Lambda \) such that \( \Sigma \) can be extended to an irredundant base and \( G_{(\Sigma)} = G_{(\Lambda)} \).

**Proof.** The sequence \( \Lambda \) cannot be extended to an irredundant base if and only if there exists a subsequence \( \lambda_i, \ldots, \lambda_{i+j} \) of \( \Lambda \) with \( j \geq 1 \) such that

\( G^{(i)} = G^{(i+1)} = \cdots = G^{(i+j)} \).

Let \( \Sigma \) be the subsequence of \( \Lambda \) given by deleting all such \( \lambda_{i+1}, \ldots, \lambda_{i+j} \). Since \( G^{(i)} = G^{(i+j)} \) it follows that \( G_{(\Lambda)} = G_{(\Sigma)} \). \( \square \)

The following describes the relationship between the irredundant base size of a group and that of a subgroup.

**Lemma 2.3.** Let \( H \) and \( G \) be subgroups of \( S_n \), with \( H \leq G \). Then the following hold.

(i) \( I(H) \leq I(G) \).

(ii) If \( H \triangleleft G \), then \( I(G) \leq I(H) + \ell(G/H) \).

(iii) If \( H \leq G \) and \( [G : H] \) is prime, then \( I(H) \leq I(G) \leq I(H) + 1 \).

**Proof.** An irredundant base for \( H \leq G \) can be extended to an irredundant base for \( G \), so Part (i) is clear. Part (ii) is [Gill et al. 2022b, Lemma 2.8] and Part (iii) follows immediately from Parts (i) and (ii). \( \square \)

### 3. Groups with socle \( \text{PSL}_d(q) \) acting on subspaces

Throughout this section, let \( \mathbb{F} \) be a field, let \( V \) be a \( d \)-dimensional vector space over \( \mathbb{F} \) and let \( \Omega = \mathcal{P}G_m(V) \) be the set of all \( m \)-dimensional subspaces of \( V \). In this section we begin by proving Theorem 3.1, which bounds \( I(\text{PGL}_d(\mathbb{F}), \Omega) \) in terms of \( d \) and \( m \).

In Section 3B, let \( q = p^f \) for some prime \( p \) and \( f \geq 1 \) and let \( \mathbb{F} = \mathbb{F}_q \). By finding lower bounds on \( n = |\Omega| \), we then prove Proposition 3.6, which bounds \( I(\text{PGL}_d(q), \Omega) \) in terms of \( n \).
3A. **Bounds as a function of d and m.** In this subsection, we prove the following theorem, which in the case \( m = 1 \) and \( \mathbb{F} \) a finite field recovers the lower bounds found by Lodà [2020].

**Theorem 3.1.** Let \( \text{PGL}_d(\mathbb{F}) \) act on \( \Omega \). Then

\[
I(\text{PGL}_d(\mathbb{F})) \leq (m + 1)d - 2m + 1
\]

and

\[
I(\text{PGL}_d(\mathbb{F})) \geq \begin{cases} md - m^2 + 1, & \text{if } \mathbb{F} = \mathbb{F}_2, \\ (m + 1)d - m^2, & \text{otherwise.} \end{cases}
\]

We begin by proving the upper bound in Theorem 3.1. Let \( M = M(V) \) be the algebra of all linear maps from \( V \) to itself. Furthermore, let \( \omega_0 = \langle 0 \rangle \), let \( l > 1 \) be an integer, let \( \Lambda = (\omega_1, \omega_2, \ldots, \omega_l) \in \Omega^l \) and for \( 0 \leq k \leq l \), let

\[
M_k = \{ g \in M \mid \omega_i g \leq \omega_i \text{ for } 0 \leq i \leq k \}, \text{ so that } M_0 = M.
\]

For \( 0 \leq k \leq l - 1 \), it is easily verified that \( M_{k+1} \) is a subspace of \( M_k \). Now assume in addition that

\[
M_0 > M_1 > \cdots > M_l = \mathbb{F}I,
\]

with \( l \) as large as possible. Fix a basis \( \langle e_1, \ldots, e_d \rangle \) of \( V \) which first goes through \( \omega_1 \cap \omega_2 \), then extends to a basis of \( \omega_1 \), and then for each \( k \geq 2 \) extends successively to a basis of \( \langle \omega_1, \ldots, \omega_k \rangle \). Therefore, there exist integers

\[
m = a_1 \leq \cdots \leq a_l = d \quad \text{such that } \langle e_1, \ldots, e_{a_l} \rangle = \langle \omega_1, \ldots, \omega_l \rangle.
\]

Since \( \omega_0 = \langle 0 \rangle \), we may let \( a_0 = 0 \). From now, on we identify \( M \) with the algebra of \( d \times d \) matrices over \( \mathbb{F} \) with respect to this basis.

We will show that \( l \leq (m + 1)d - 2m + 1 \), from which the upper bound in Theorem 3.1 will follow. For \( 0 \leq k \leq l - 1 \), let

\[
f_k = \dim(M_k) - \dim(M_{k+1}),
\]

and let \( b_k = a_{k+1} - a_k \) so that \( 0 \leq b_k \leq m \). In the following lemmas we consider the possible values of \( f_k \) based on \( b_k \).

**Lemma 3.2.** Let \( f_k \) and \( b_k \) be as above.

1. The dimension of \( M_1 \) is \( d^2 - m(d - m) \), and so \( f_0 = m(d - m) \).
2. \( f_1 = b_1(d - b_1) \).

**Proof.** First consider Part (i). Since \( \omega_1 = \langle e_1, \ldots, e_m \rangle \) it follows that \( g = (g_{ij}) \in M_1 \) if and only if \( e_i g \in \omega_1 \) for \( 1 \leq i \leq m \). Equivalently, \( g_{ij} = 0 \) for \( 1 \leq i \leq m \) and \( m + 1 \leq j \leq d \). Hence, \( \dim(M_1) = d^2 - m(d - m) \), and the final claim follows from \( \dim(M_0) = d^2 \).
Now consider (ii). The subspace $M_2$ contains all matrices of shape
\[
\begin{pmatrix}
x_1 & 0 & 0 \\
x_2 & x_3 & 0 \\
x_4 & 0 & x_5 \\
y_1 & y_2 & y_3 & y_4
\end{pmatrix},
\]
where $x_1$, $x_3$ and $x_5$ are square with $m - b_1$, $b_1$ and $b_1$ rows, respectively. Hence,
\[
\dim(M_2) = (m - b_1)^2 + 2b_1(m - b_1) + 2b_1^2 + (d - m - b_1)d
\]
\[
= d^2 - m(d - m) - b_1(d - b_1),
\]
and the result follows from Part (i).

**Lemma 3.3.** Let $k \geq 2$. Then $f_k \geq \max\{1, b_k(d - m)\}$.

**Proof.** For $0 \leq k \leq l$ we define two subspaces of $M_k$, namely
\[
X_k = \{g \in M_k | e_i g = 0 \text{ for } a_k + 1 \leq i \leq d\} \quad \text{and} \quad Y_k = \{g \in M_k | e_i g = 0 \text{ for } 1 \leq i \leq a_k\}.
\]
We begin by showing that
\begin{equation}
(2) \quad M_k = X_k \oplus Y_k \quad \text{and} \quad \dim(Y_k) = d(d - a_k).
\end{equation}
By construction, $X_k \cap Y_k = \{0_M\}$. Let $g = (g_{ij}) \in M_k$. Then there exist $x = (x_{ij})$, $y = (y_{ij}) \in M$, with $x_{ij} = g_{ij}$ and $y_{ij} = 0$ for $i \leq a_k$, and $x_{ij} = 0$ and $y_{ij} = g_{ij}$ for $i \geq a_k + 1$. Then $g = x + y$ with $x \in X_k$ and $y \in Y_k$, hence $M_k = X_k \oplus Y_k$. Since $g \in Y_k$ if and only if $g_{ij} = 0$ for $i \leq a_k$, it follows that $\dim(Y_k) = d(d - a_k)$. Hence, (2) holds.

Our assumption that $M_k > M_{k+1}$ implies that $f_k \geq 1$, so we may assume that $b_k \geq 1$. By (2),
\[
f_k = \dim(M_k) - \dim(M_{k+1})
\]
\[
= (\dim(X_k) + \dim(Y_k)) - (\dim(X_{k+1}) + \dim(Y_{k+1}))
\]
\[
= \dim(X_k) - \dim(X_{k+1}) + d(d - a_k) - d(d - a_k + 1)
\]
\[
= \dim(X_k) - \dim(X_{k+1}) + b_k d.
\]
We now bound $\dim(X_k) - \dim(X_{k+1})$. By choice of basis
\[
\omega_{k+1} = \langle u_1, \ldots, u_{m-b_k}, e_{a_k+1}, \ldots, e_{a_k+b_k}\rangle
\]
for some $u_1, \ldots, u_{m-b_k} \in \langle \omega_1, \ldots, \omega_k\rangle$. Hence if $v \in \{e_{a_k+1}, \ldots, e_{a_k+b_k}\}$, then $\langle v \rangle M_{k+1} \leq \omega_{k+1}$. Therefore, $\langle v M_{k+1}\rangle$ has dimension at most $m$, and so $\dim(X_{k+1}) \leq \dim(X_k) + b_k m$. Hence,
\[
f_k = \dim(X_k) - \dim(X_{k+1}) + b_k d \geq -b_k m + b_k d = b_k (d - m). \quad \square
Proof of upper bound of Theorem 3.1. We shall show that $l \leq (m+1)d - 2m + 1$, from which the result will follow, since $I(\text{PGL}_d(F), \Omega) = I(\text{GL}_d(F), \Omega)$ and $\text{GL}_d(F)$ is a subgroup of $M$.

For $0 \leq b \leq m$, let
\[ C_b = \{ k \in \{0, \ldots, l-1\} \mid b_k = b \}, \]
and let $c_b = |C_b|$. Then
\[ l = \sum_{b=0}^{m} c_b. \] (3)

Since $a_l = d$ and $a_0 = 0$, it follows that
\[ d = a_l - a_0 = \sum_{k=0}^{l-1} (a_{k+1} - a_k) = \sum_{k=0}^{l-1} b_k = \sum_{b=0}^{m} b c_b = \sum_{b=1}^{m} b c_b. \] (4)

Since $a_1 = m$ and $a_0 = 0$, it follows that $b_0 = m$, so $0 \in C_m$ and $c_m \geq 1$. Since $\omega_1 \neq \omega_2$ it follows that $b_1 \neq 0$, and $1 \in C_{b_1}$, so
\[ c_{b_1} \geq 1 \quad \text{and} \quad c_m \geq 1 + \delta_{m,b_1}, \]
where $\delta_{m,b_1}$ is the Kronecker delta. Lemmas 3.2 and 3.3 yield
\[ f_0 = m(d-m), \quad f_1 = b_1(d-b_1) = b_1(m-b_1) + b_1(d-m), \]
\[ f_k \geq \max\{1, b_k(d-m)\} \quad \text{for} \ k \geq 2. \] (5)

Since $M_0 = M$ and $M_l = FI$, it follows from the definition of $f_k$ that
\[ d^2 - 1 = \dim(M_0) - \dim(M_l) \]
\[ = \sum_{k=0}^{l-1} (\dim(M_k) - \dim(M_{k+1})) \]
\[ = \sum_{k=0}^{l-1} f_k = \sum_{k \in C_0} f_k + \sum_{k \in C_{b_1} \setminus \{1\}} f_k + \sum_{k \notin C_0 \cup C_{b_1}} f_k \]
\[ \geq \sum_{k \in C_0} 1 + b_1(m-b_1) + b_1(d-m) + \sum_{k \notin C_0 \cup C_{b_1}} b_k(d-m) \]
\[ = c_0 + b_1(m-b_1) + \sum_{k \notin C_0 \cup C_{b_1}} b_k(d-m) \] (by (6))
\[ = c_0 + b_1(m-b_1) + \sum_{k \notin C_0} b_k(d-m) \]
\[ = c_0 + b_1(m-b_1) + (d-m) \sum_{b=1}^{m} b c_b \]
\[ = c_0 + b_1(m-b_1) + (d-m) d \] (by (4)).

By rearranging, we find that
\[ c_0 \leq md - b_1(m-b_1) - 1. \] (7)
We bound \( I(G) \) by maximising \( l = \sum_{b=0}^{m} c_b \) subject only to (4), (5) and (7). By (4), an upper bound on \( \sum_{b=0}^{m} c_b \) is given by maximising \( c_0 \), maximising \( c_b \) for \( b \) small and minimising \( c_b \) for \( b \) large. Hence, we substitute \( c_b = md - b_1(m - b_1) - 1 \) by (7), substitute \( c_b = 0 \) for \( b \notin \{0, 1, b_1, m\} \), and maximise \( c_1 \) and minimise \( c_m \) subject to (5).

First let \( m = 1 \). Since \( b_1 \neq 0 \) it follows that \( b_1 = 1 \), and hence \( c_1 = d \) by (4). Now let \( m \geq 2 \). Then there are three possibilities for \( b_1 \). If \( b_1 = m \), then to minimise \( c_m \) subject to (5) let \( c_m = 2 \), and so (4) yields \( c_1 = d - 2m \). If \( b_1 = 1 \), then \( c_m = 1 \), and (4) yields \( c_1 = d - m \). Otherwise \( c_m = c_{b_1} = 1 \), and (4) yields \( c_1 = d - m - b_1 \).

Hence, in all cases

\[
|C_1 \cup C_{b_1} \cup C_m| = 2 + d - m - b_1.
\]

Therefore,

\[
\sum_{b=0}^{m} c_b \leq (md - b_1(m - b_1) - 1) + 2 + d - m - b_1 = (m+1)d - m + 1 - b_1(m - b_1 + 1).
\]

Hence if \( \sum_{b=0}^{m} c_b \) is maximal, then \( b_1(m - b_1 + 1) \) is minimal subject to \( 1 \leq b_1 \leq m \). Therefore, \( b_1 \) is 1 or \( m \), and so

\[
\sum_{b=0}^{m} c_b \leq (m + 1)d - 2m + 1.
\]

The result now follows from (3). \( \square \)

We now consider the lower bounds in Theorem 3.1.

**Proof of lower bound of Theorem 3.1.** Let \( G = \text{GL}_d(\mathbb{F}) \). Here we give a sequence of \( m \)-spaces of \( V \) such that each successive point stabiliser in \( G \) is a proper subgroup of its predecessor. Its length is therefore a lower bound on \( I(\text{PGL}_d(\mathbb{F}), \Omega) \).

For \( 1 \leq k \leq md - m^2 + d \), we define the following three variables:

\[
r_k = \left\lfloor \frac{k-2}{m} \right\rfloor + m + 1, \quad s_k = m - ((k - 2) \mod m) \quad \text{and} \quad t_k = k - md + m^2.
\]

A few remarks are in order. Firstly, it is immediate from the definition of \( s_k \) that

\[
1 \leq s_k \leq m.
\]

Secondly, if \( m + 2 \leq k \leq md - m^2 + 1 \), then

\[
m + 2 \leq r_k \leq d.
\]

Finally, notice that \( t_k \leq d \) for all \( k \), and

\[
2 \leq t_k \leq m + 1 \quad \text{if and only if} \quad md - m^2 + 2 \leq k \leq md - m^2 + m + 1.
\]
Therefore, the following sets $W_k$ of $m$ linearly independent vectors of $V$ are well defined.

\[
W_k = \begin{cases}
\{ e_i \mid i \in \{1, \ldots, m+1\} \setminus \{m+2-k\} \}, & 1 \leq k \leq m+1, \\
\{ e_i \mid i \in \{1, \ldots, m, r_k\} \setminus \{s_k\} \}, & m+2 \leq k \leq md-m^2+1, \\
\{ e_1 + e_{r_k}, e_i \mid i \in \{2, \ldots, m+1\} \setminus \{t_k\} \}, & md-m^2+2 \leq k \leq md-m^2+m+1, \\
\{ e_1 + e_{t_k}, e_i \mid i \in \{2, \ldots, m\} \}, & md-m^2+m+2 \leq k \leq md-m^2+d.
\end{cases}
\]

Let $\omega_k = (W_k) \in \Omega$, and let $G^{(k)} = G_{\omega_1, \ldots, \omega_k}$. For $1 \leq x, y \leq d$, let $T(x, y)$ be the matrix $I + E_{x,y}$ (acting on $V$ on the right), and let $\text{Supp}_x(W_k)$ be the set of vectors in $W_k$ which are nonzero in position $x$. Recall that

\[
e_i T(x, y) = \begin{cases}
e_i + e_y, & \text{if } i = x, \\
e_i, & \text{otherwise}.
\end{cases}
\]

Hence, if a vector $v$ is zero in position $x$, then $vT(x, y) = v$. Thus, $\omega_k T(x, y) = \omega_k$ if and only if $\text{Supp}_x(W_k) T(x, y) \subseteq \omega_k$. In particular, if $\text{Supp}_x(W_k) = \emptyset$, then $\omega_k T(x, y) = \omega_k$. Furthermore, $T(x, y) \in G$ unless $x = F_2$ and $x = y$.

It is clear that $G > G^{(1)}$, so let $k \in \{2, \ldots, md-m^2+1\}$ and let $j \leq k$. We shall show that there exist $x$ and $y$ such that $\omega_k T(x, y) \neq \omega_k$ and $\omega_j T(x, y) = \omega_j$ for all $j < k$. Hence, $T(x, y) \in G^{(k-1)} \setminus G^{(k)}$ and so $G^{(k-1)} > G^{(k)}$.

First consider $k \in \{2, \ldots, m+1\}$, and let $T = T(m+1, m+2-k)$. Then $\text{Supp}_{m+1}(W_1) = \emptyset$, and for $1 < j \leq k$

\[
\text{Supp}_{m+1}(W_j) T = \{ e_{m+1} \} T = \{ e_{m+1} + e_{m+2-k} \}.
\]

Hence, $\text{Supp}_{m+1}(W_j) T \subseteq \omega_j$ if and only if $j \neq k$. Therefore, $\omega_j T = \omega_j$ for $j < k$, and $\omega_k T \neq \omega_k$.

Next consider $k \in \{m+2, \ldots, md-m^2+1\}$. Hence (8) holds, and so we may let $T$ be the matrix $T(r_k, s_k)$. If $j \leq m+1$ or if $r_j \neq r_k$, then $\text{Supp}_{r_k}(W_j) = \emptyset$ and so $\omega_j T = \omega_j$. Therefore, assume that $j \geq m+2$ and $r_j = r_k$. Then

\[
\text{Supp}_{r_k}(W_j) T = \{ e_{r_k} \} T = \{ e_{r_k} + e_{s_k} \}.
\]

Since $(r_j, s_j) = (r_k, s_k)$ if and only if $j = k$, it follows that $\text{Supp}_{r_k}(W_j) T \subseteq \omega_j$ if and only if $j \neq k$. Therefore, $\omega_j T = \omega_j$ for $j < k$, and $\omega_k T \neq \omega_k$. Hence, $G^{(k-1)} > G^{(k)}$ for $1 \leq k \leq md-m^2+1$, and so if $F = F_2$ then the result follows.

It remains to consider $|F| > 2$ and $k \geq md-m^2+2$. Let $T = T(t_k, t_k)$, and let $u \in \{ e_i, e_1 + e_i \mid 1 \leq i \leq d \}$. Then

\[
u T = \begin{cases}
e_1 + 2e_{t_k}, & \text{if } u = e_1 + e_{t_k}, \\
2u, & \text{if } u = e_{t_k}, \\
u, & \text{otherwise}.
\end{cases}
\]
If \(1 \leq j \leq md - m^2 + 1\), then \(W_j \subseteq \{e_1, \ldots, e_d\}\), and if \(md + m^2 + 1 < j < k\), then \(W_j \subseteq \{e_1 + e_{t_j}, e_1, \ldots, e_d\}\) with \(t_j \neq t_k\). Hence, if \(j < k\), then \(\text{Supp}_{t_k}(W_j)T \subseteq \omega_j\), and so \(\omega_j T = \omega_j\). Since \(e_1 + e_{t_k} \in \omega_k\) but \(e_1 + 2e_{t_k} \notin \omega_k\) it follows that \(\omega_k T(t_k, t_k) \neq \omega_k\). Hence, \(G^{(k-1)} > G^{(k)}\) for \(1 \leq k \leq md - m^2 + d\), and so the result follows. □

**Remark 3.4.** The interested reader may wish to check, using the notation of the previous proof, that the following holds. Let \(\Lambda = (\omega_i)_{2 \leq i \leq md - m^2 + 1}\) if \(\mathbb{F} = \mathbb{F}_2\), and \(\Lambda = (\omega_i)_{m+1 \leq i \leq md - m^2 + d}\) otherwise. Then \(\Lambda\) is a minimal base for the action of 
\(\text{PGL}_d(\mathbb{F})\) on \(\mathcal{P}\mathcal{G}_m(\mathbb{F})\). Hence,

\[
B(\text{PGL}_d(\mathbb{F}), \mathcal{P}\mathcal{G}(V)) \geq \begin{cases} 
md - m^2, & \text{if } \mathbb{F} = \mathbb{F}_2, \\
(m+1)d - m^2 - m, & \text{otherwise.}
\end{cases}
\]

**3B. Upper bounds as a function of \(|\Omega|\).** We now let \(q = p^f\) for some prime \(p\) and integer \(f \geq 1\), and let \(\mathbb{F} = \mathbb{F}_q\). Our main result in this subsection is Proposition 3.6, which bounds \(I(\text{PGL}_d(q), \Omega)\) as a function of \(n = |\Omega|,\) rather than of \(m\) and \(d\). We begin by bounding the size of \(\Omega = \mathcal{P}\mathcal{G}_m(\mathbb{F}_q^d)\).

**Lemma 3.5.** Let \(n(d, m, q) = |\mathcal{P}\mathcal{G}_m(\mathbb{F}_q^d)|\). Then

\[
\log |\Omega| = \log(n(d, m, q)) > \begin{cases} 
d^2/4 + 1/2, & \text{if } q = 2 \text{ and } m = d/2 \geq 2, \\
md(m - d) \log q, & \text{for all } m \text{ and } q.
\end{cases}
\]

**Proof.** The second bound is immediate since \((q^{d-m+i} - 1)/q^i - 1 > q^{d-m}\) for \(1 \leq i \leq m\). Hence, we consider \(n(2m, m, 2)\), which we must show is greater than \(2^{m+1/2}\).

We induct on \(m\). Since \(n(4, 2, 2) = 35 > 2^{2+1/2}\), the result holds for \(m = 2\). Now,

\[
n(2m, m, 2) = \frac{(2^{2m} - 1)(2^{2m-1} - 1)(2^{2m-2} - 1) \cdots (2^m + 1)}{(2^m - 1)(2^{m-1} - 1)(2^{m-2} - 1) \cdots (2 - 1)}
= \frac{(2^{2m} - 1)(2^{2m-1} - 1)}{(2^m - 1)^2} \cdot \frac{(2^{2m-2} - 1) \cdots (2^m + 1)(2^m - 1)}{(2^{m-1} - 1)(2^{m-2} - 1) \cdots (2 - 1)}
= \frac{(2^{2m} - 1)(2^{2m-1} - 1)}{(2^m - 1)^2} \cdot n(2m - 2, m - 1, 2)
\geq \frac{(2^{2m} - 1)(2^{2m-1} - 1)}{(2^m - 1)^2} \cdot 2^{(m-1)^2+1/2} \quad \text{(by induction)}.
\]

It is easily verified that

\[(2^m + 1)(2^{2m-1} - 1) = 2^{3m-1} + 2^{2m-1} - 2^m - 1 > 2^{3m-1} - 2^{2m-1} = 2^{2m-1}(2^m - 1).
\]
Hence,
\[
\frac{(2^m - 1)(2^{m-1} - 1)}{(2^m - 1)^2} \leq \frac{(2^m + 1)(2^{m-1} - 1)}{(2^m - 1)} 2^{(m-1)^2}
\]
> \frac{2^{2m-1}(2^m - 1)}{(2^m - 1)} 2^{(m-1)^2} = 2^m.
and the result follows. \(\Box\)

Recall that \(q = p^f\) with \(p\) prime, and \(\Omega = \mathcal{P}G_m(\mathbb{F}_{q^d})\), with \(n = |\Omega|\).

**Proposition 3.6.** Let \(G = \text{PGL}_d(q)\) and assume that \(m \leq \frac{d}{2}\). Then

\[
\log q = |G|, \quad (9) \quad I(G) = I(\text{PGL}_n(q)) + \ell(C_f) \leq (m + 1)d - 2m + 1 + \log f.
\]

First let \(m = 1\), so that \(I(G) \leq 2(d - 1) + 1 + \log f\). Then, by Lemma 3.5, \((d - 1) \log q < \log n\). Hence, the result is immediate for \(q = 2\), and follows from \(\log q > \frac{3}{2}\) for \(q \geq 3\).

Now let \(m = \frac{d}{2} \geq 2\), so that \(I(G) \leq \frac{d^2}{2} + 1 + \log f\). If \(q = 2\) then \(\frac{d^2}{4} + \frac{1}{2} < \log n\) by Lemma 3.5, and so the result follows. If \(q \geq 3\), then it follows from \(d \geq 4\) that \(1 \leq \frac{d^2}{4}\), and so

\[
\frac{d^2}{2} + 1 \leq \frac{3d^2}{4} < \frac{d^2}{2} \log q = 2m(d - m) \log q.
\]
Therefore,

\[
I(G) \leq 2m(d - m) \log q + \log f < 2 \log n + \log f,
\]
by Lemma 3.5. Finally consider \(1 < m < \frac{d}{2}\). Then \(1 \leq d - 2m\), and so

\[
d - 2m + 1 \leq 2(d - 2m) \leq m(d - 2m).
\]
Hence by (9),

\[
I(G) - \log f \leq md + d - 2m + 1 \leq m(d - 2m) = 2m(d - m) \leq 2m(d - m) \log q.
\]
Therefore, \(I(G) \leq 2m(d - m) \log q + \log f \leq 2 \log n + \log f\), by Lemma 3.5. \(\Box\)
4. Almost simple groups

In this section, we prove Theorem 1.1 for almost simple groups. More precisely, we prove the following result.

**Theorem 4.1.** Let $G$ be an almost simple primitive subgroup of $S_n$. If $G$ is not large base, then

$$I(G, \Omega) < 5 \log n - 1.$$ 

We begin with two definitions which we shall use to divide this section into cases.

**Definition 4.2.** Let $G$ be almost simple with socle $G_0$, a classical group with natural module $V$. 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.

(i) $M = G_U$ for some proper nonzero subspace $U$ of $V$, where if $G_0 \neq \text{PSL}_d(F)$, then $U$ is either totally singular or nondegenerate, or if $G$ is orthogonal and $p = 2$ a nonsingular 1-space.

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

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

**Definition 4.3.** Let $G$ be almost simple with socle $G_0$. A transitive action of $G$ on $\Omega$ is **standard** if up to equivalence of actions one of the following holds, and is **nonstandard** otherwise.

(i) $G_0 = A_r$ and $\Omega$ is an orbit of subsets or partitions of $\{1, \ldots, r\}$.

(ii) $G$ is a classical group in a subspace action.

This section is split into three subsections. The first considers $G_0 = \text{PSL}_d(q)$ acting on subspaces and pairs of subspaces. In the second, we deal with the case of $G$ another classical group in a subspace action. Finally, in the third, we prove Theorem 4.1.

**4A. $G_0 = \text{PSL}_d(q)$.** Let $G$ be almost simple with socle $\text{PSL}_d(q)$, in a subspace action on a set $\Omega$. We first consider $\Omega = \mathcal{P}G_m(V)$.

**Proposition 4.4.** Let $G$ be almost simple with socle $\text{PSL}_d(q)$ acting on $\Omega = \mathcal{P}G_m(V)$, and let $n = |\Omega|$. Then

$$I(G) < 3 \log n.$$ 

**Proof.** If $m = 1$, then $G \leq \text{PGL}_d(q)$, so $I(G) \leq I(\text{PGL}_d(q))$ by Lemma 2.3(i). Otherwise $G \cap \text{PGL}_d(q)$ has index at most 2 in $G$, so by Lemma 2.3(i) and (iii)

$$I(G) \leq I(G \cap \text{PGL}_d(q)) + 1 \leq I(\text{PGL}_d(q)) + 1.$$
Therefore, we can bound $I(G)$ by our bound for $I(\PGL_d(q))$ when $m = 1$, and by one more than that when $m > 1$. Thus, Proposition 3.6 yields $I(G) \leq 2 \log n + \log f + 1$. It is easily seen that $\log f + 1 \leq \log q \leq m(d - m) \log q$, and so by Lemma 3.5 $\log f + 1 < \log n$ and the result follows.

We now consider the action of $G$ on the following subsets of $\P G_m(V) \times \P G_{d - m}(V)$, with $m < \frac{d}{2}$:

\[ \Omega^\oplus = \{ (U, W) | U, W \leq V, \dim U = m, \dim W = d - m, \text{ with } U \oplus W = V \}, \]

\[ \Omega^\leq = \{ (U, W) | U, W \leq V, \dim U = m, \dim W = d - m, \text{ with } U \leq W \}. \]

Note that in both cases we require $d \geq 3$.

**Lemma 4.5.** Let $G$ be almost simple with socle $\PSL_d(q)$, let $H = G \cap \PGL_d(q)$ and let $\Omega$ be either $\Omega^\oplus$ or $\Omega^\leq$. Then

\[ I(G, \Omega) \leq 2I(H, \P G_m(V)) + 1. \]

**Proof.** We first show that

\[ I(H, \Omega) \leq I(H, \P G_m(V)) + I(H, \P G_{d - m}(V)). \]

Let $l = I(H, \Omega)$ and let $\Lambda = \{ [U_1, W_1], \ldots, [U_l, W_l] \}$ be a corresponding base, where $\dim(U_i) = m$ for all $i$. Let $\Pi = (U_1, \ldots, U_l)$, and let $\Sigma = (W_1, \ldots, W_l)$. Then by Lemma 2.2, $\Pi$ and $\Sigma$ contain subsequences which can be extended to irredundant bases for the action of $H$ on $\P G_m(V)$ and $\P G_{d - m}(V)$, respectively.

Let $\Pi'$ be the subsequence of $\Pi$ which contains $U_i$ if and only if $H_{U_1, \ldots, U_{i-1}, U_i} > H_{U_1, \ldots, U_{i-1}, U_i}$. Then $\Pi'$ can be extended to an irredundant base for the action of $H$ on $\P G_m(V)$. Let $k = |\Pi'|$, so $k \leq I(H, \P G_m(V))$.

Let $\Sigma' = (W_{j_1}, \ldots, W_{j_k})$ be the subsequence of $\Sigma$ which contains $W_i$ if and only if $H_{U_1, \ldots, U_{i-1}} = H_{U_1, \ldots, U_{i-1}, U_i}$. Assume, for a contradiction, that $\Sigma'$ cannot be extended to an irredundant base for the action of $H$ on $\P G_{d - m}(V)$. Since $H$ is irreducible, $H > H_{W_{j_k}}$. Therefore, there exists $s \geq 2$ such that

\[ H_{W_{j_1}, W_{j_2}, \ldots, W_{j_{k-1}}} = H_{W_{j_1}, W_{j_2}, \ldots, W_{j_{k-1}}} \cdot W_s. \]

Let $i = j_s$. Then intersecting both sides of the above expression with $H_{W_1, \ldots, W_{i-1}}$ gives

\[ H_{W_1, \ldots, W_{i-1}} = H_{W_1, \ldots, W_{i-1}} \cdot W_i. \]

Since $W_i \in \Sigma'$, it follows that

\[ H_{U_1, \ldots, U_{i-1}} = H_{U_1, \ldots, U_{i-1}} \cdot U_i. \]

Elements of $H = G \cap \PGL_d(q)$ cannot map $U_i$ to $W_i$. Thus, (11) and (12) imply that

\[ H_{[U_1, W_1], \ldots, [U_{i-1}, W_{i-1}]} = H_{[U_1, W_1], \ldots, [U_{i-1}, W_{i-1}], [U_i, W_i]}, \]

a contradiction since $\Lambda$ is irredundant. Hence $l - k \leq I(H, \P G_{n-m}(V))$, and so (10) holds.
The subgroups of $\text{Sym}(\mathcal{P}G_m(V))$ and $\text{Sym}(\mathcal{P}G_{n-m}(V))$ representing the actions of $H$ are permutation isomorphic. Therefore, (10) implies that $I(H, \Omega) \leq 2I(H, \mathcal{P}G_m(V))$. Since $H$ has index at most 2 in $G$, the result follows from Lemma 2.3(iii).

**Lemma 4.6.** Let $\Omega$ be either $\Omega_5^\oplus$ or $\Omega_8^\subseteq$, and let $n = |\Omega|$. Let $G$ be an almost simple subgroup of $\text{Sym}(\Omega)$ with socle $\text{PSL}_d(q)$. Then

$$I(G) < 5(\log n - 1).$$

**Proof.** Let $H = G \cap \text{PG}_d(q)$, then by Proposition 3.6 and Lemma 4.5

$$I(G) \leq 2I(H, \mathcal{P}G_m) + 1 \leq \begin{cases} 4(d-1)+3, & \text{if } m = 1 \text{ and } q = 2, \\ \frac{8}{3}(d-1) \log q + 2 \log f + 3, & \text{if } m = 1 \text{ and } q \geq 3, \\ 4m(d-m) \log q + 2 \log f + 1, & \text{otherwise}. \end{cases}$$

Since $1 \leq m < \frac{d}{2}$, each $m$-dimensional subspace of $V$ has more than one complement and is contained in more than one $(d-m)$-dimensional subspace. Hence $n \geq 2|\mathcal{P}G_m(V)|$, and so Lemma 3.5 gives

$$m(d-m) \log q < \log \frac{n}{2} = \log n - 1.$$ 

Recall that $d \geq 3$. First let $m = 1$. If $(d, q) = (3, 2)$, then $n \in \{21, 28\}$. Therefore, by (13), it follows that $I(G) \leq 11 < 5(\log n - 1)$.

Hence if $q = 2$, then we may assume that $d \geq 4$, and so by (13) and (14),

$$I(G) \leq 4(d-1) + 3 \leq 5(d-1) < 5(\log n - 1).$$

Still with $m = 1$, let $q \geq 3$. Then

$$I(G) \leq \frac{8}{3}(d-1) \log q + 2 \log f + 3 \quad \text{(by (13))},$$

$$< \frac{8}{3}(d-1) \log q + 2(d-1) \log q + 1 \quad \text{(since } \log f + 1 \leq \log q < (d-1) \log q),$$

$$< 5(d-1) \log q \quad \text{(since } 1 < \frac{1}{3}(d-1) \log q),$$

$$< 5(\log n - 1) \quad \text{(by (14))}.$$

Finally, let $m \geq 2$ so that $m(d-m) \geq 6$. Then it is easily checked that $2 \log f + 1 \leq m(d-m) \log q$, so by (13) and (14),

$$I(G) \leq 4m(d-m) \log q + 2 \log f + 1 \leq 5m(d-m) \log q < 5(\log n - 1).$$

\[ \square \]

**4B. $G_0$ another classical group.**

**Lemma 4.7.** Let $G$ be almost simple with socle $G_0 = \mathcal{P}O_8^+(q)$, acting faithfully and primitively on a set $\Omega$ of size $n$. Then

$$I(G) < 5 \log n - 1.$$
Proof. Let $q \geq 3$. Then the reader may check that $6f < q^2$, and so by [Gill et al. 2022b, (6.19)],

$$|G| < 6f q^{28} \leq q^{30}.$$  

If $q = 2$, then $|G| \leq 6|G_0| < q^{30}$ also. Hence by Lemma 2.1(ii), since $n > 4$,

$$I(G) \leq \log q^{30} - 1 = 5 \log q^6 - 1 < 5 \log n - 1,$$

by [Landazuri and Seitz 1974]. □

Proposition 4.8. Let $G$ be almost simple with socle $G_0$, a classical group with natural module $V$. Assume that $G_0 \neq \text{PSL}(V)$ and $G_0 \neq \text{PΩ}^+_8(q)$. Let $0 < m < d$, let $\Omega$ be a $G$-orbit of totally isotropic, totally singular, or nondegenerate subspaces of $V$ of dimension $m$, and let $n = |\Omega|$. Then

$$I(G, \Omega) < 5 \log n - 1.$$

Proof. First, let $G_0 = \text{PSO}^+_d(q)$ and $m = \frac{d}{2}$. Then $d \geq 10$, and so $2d^2 - 12d + 16 > 0$. Hence $10d^2 - 20d > 8d^2 - 8d + 16$ and it follows that $n = \frac{d^2}{8} - \frac{d}{4} > \frac{d^2}{10} - \frac{d}{10} + \frac{1}{5}$. By [Burness and Giudici 2016, Table 4.12],

$$n = \prod_{i=1}^{d/2-1} (q^i + 1) > \prod_{i=1}^{d/2-1} q^i = q^{d^2/8-d/4} > q^{d^2/10-d/10+1/5}.$$  

Hence,

$$I(G) \leq \log |G| - 1 \quad \text{(by Lemma 2.1(ii))},$$

$$\leq \log \left( q^{d^2/2-d/2+1} \right) - 1 \quad \text{(by [Gill et al. 2022b, p. 25])},$$

$$= 5 \log \left( q^{d^2/10-d/10+1/5} \right) - 1$$

$$< 5 \log n - 1 \quad \text{(by (15))}.$$  

Therefore, we may assume for the rest of the proof that $G_0 \neq \text{PΩ}^+_d(q)$, so by [Gill et al. 2022b, Lemma 7.14],

$$\frac{1}{2} m(d - m) \log q < \log n.$$  

Since $\Omega$ is a $G$-orbit of subspaces, if $G_0 = \text{PSp}_4(q)$, then $G$ does not induce the graph isomorphism by [Bray et al. 2013, Table 8.14]. Hence since $G_0 \neq \text{PΩ}^+_8(q)$ and $\Omega \subseteq \text{PG}m(V)$, we may assume that $G \leq \text{PΓL}_d(q)$. Then Lemma 2.3(i) implies that

$$I(G) \leq I(\text{PΓL}_d(q), \text{PG}m(V)),$$

and so, in particular, the bounds from Proposition 3.6 apply.

We begin with $m = 1$. If $q = 2$, then we split into two cases. If $d \leq 4$, then by Proposition 3.6,

$$I(G) \leq 2(d - 1) + 1 = 7 < 5 \log n - 1.$$
Therefore, it follows from Proposition 3.6 and (16),

$$I(G) \leq 2(d - 1) + 1 \leq 2(d - 1) + \frac{1}{2}(d - 1) - 1 < 5\log n - 1.$$ 

To complete the case of $m = 1$, let $q \geq 3$. Since $G_0 \neq \text{PSL}_d(q)$, we may assume that $d \geq 3$ and so it can be verified that $\frac{6}{7}f + 1 < 3 \leq d$. Hence,

$$2 + \log f < \frac{7}{6}f(d - 1) \leq \frac{7}{6}f(d - 1) \log p = \frac{7}{6}(d - 1) \log q.$$ 

Therefore, it follows from Proposition 3.6 and (16) that

$$I(G) \leq \frac{4}{3}(d - 1) \log q + \log f + 1 < \frac{5}{2}(d - 1) \log q - 1 < 5\log n - 1.$$ 

Now let $m = \frac{d}{2}$ and $q = 2$. Then by Proposition 3.6 and (16),

$$I(G) \leq \frac{d^2}{2} + 1 = 4\left(\frac{1}{2}m(d - m)\right) + 1 < 4\log n + 1 < 5\log n - 1,$$

since $n > 4$.

Hence, we may assume that $m \geq 2$, that $m(d - m) \geq 4$, and that if $m = \frac{d}{2}$, then $q \geq 3$. Therefore,

$$I(G) \leq 2m(d - m) \log q + \log f \quad \text{(by Proposition 3.6)},$$

$$\leq 2m(d - m) \log q + \frac{1}{2}m(d - m) \log q - \frac{4}{3} \quad \text{(since 4log} q \geq 3(\log f + 1) + 1),$$

$$< \frac{14}{3} \log n - \frac{4}{3} \quad \text{(by (16))},$$

$$< 5\log n - 1. \quad \Box$$

**4C. Proof of Theorem 4.1.** We begin by proving Theorem 4.1 for nonstandard actions.

**Proposition 4.9.** Let $G$ be an almost simple, primitive nonstandard subgroup of $\text{Sym}(\Omega)$ and let $n = |\Omega|$. Then

$$I(G, \Omega) \leq 4\log n + 1.$$ 

**Proof.** By a landmark result of Burness and others [Burness 2018; Burness 2007; Burness et al. 2009; Burness et al. 2010], either $(G, \Omega) = (M_{24}, \{1, \ldots, 24\})$ or $b(G, \Omega) \leq 6$. By [Gill et al. 2022b, p. 10], $I(M_{24}, \{1, \ldots, 24\}) = 7 < 2\log 24$. If $b(G) \leq 5$, then the result follows by Lemma 2.1(iii). Hence we may assume that $b(G, \Omega) = 6$.

Let $G$ have point stabiliser $H$. By a further result of Burness [2018, Theorem 1], either

(17) $(G, H) \in \{(M_{23}, M_{22}), (Co_3, McL.2), (Co_2, U_6(2).2), (Fi_{22}.2, 2.U_6(2).2)\}$

or

(18) $(\text{Soc}(G), H) \in \{(E_7(q), P_7), (E_6(q), P_1), (E_6(q), P_0)\}.$

We first deal with \((G, H) = (M_{23}, M_{22})\). Since \(M_{23}\) is the point stabiliser of \(M_{24}\), it follows that
\[
I(M_{23}, \{1, \ldots, 23\}) = I(M_{24}, \{1, \ldots, 23, 24\}) - 1 = 6 < 2 \log 23.
\]

For the other cases of (17) and (18) we verify that \(|H| < [G : H]^4\), and so since \(H\) is insoluble, it will follow by Lemma 2.1(i) that
\[
I(G) = I(H) + 1 < \log |H| < \log [G : H]^4 = 4 \log n.
\]

For the remaining \((G, H)\) in (17), it is easy to use [Conway et al. 1985] to verify that \(|H| < [G : H]^4\). Therefore, we may assume that \((\text{Soc}(G), H)\) is as in (18). Let \(m(G)\) be the smallest degree of a faithful transitive permutation representation of \(G\). If \(|G| < m(G)^5\), then
\[
|H| = \frac{|G|}{[G : H]} < \frac{m(G)^5}{[G : H]} \leq [G : H]^4,
\]
and so the result will follow.

First, let \(G_0 = E_6(q)\). Then by [Steinberg 1968],
\[
|E_6(q)| = \frac{q^{36}(q^{12} - 1)(q^9 - 1)(q^8 - 1)(q^6 - 1)(q^5 - 1)(q^2 - 1)}{(3, q - 1)}
\]
and \(|\text{Out}(E_6(q))| \leq 2f(3, q - 1) \leq q(3, q - 1)\). Hence,
\[
|G| \leq q^{37}(q^{12} - 1)(q^9 - 1)(q^8 - 1)(q^6 - 1)(q^5 - 1)(q^2 - 1) < q^{37+12+9+8+6+5+2} = q^{79}.
\]

By [Vasilev 1997, p. 2],
\[
m(G) \geq m(G_0) \geq \frac{(q^9 - 1)(q^8 + q^4 + 1)}{q - 1} = (q^8 + q^7 + \cdots + q + 1)(q^8 + q^4 + 1) > q^{16}.
\]

Hence, \(|G| < q^{79} < q^{80} < m(G)^5\), as required.

Now let \(G_0 = E_7(q)\). Then by [Steinberg 1968],
\[
|E_7(q)| = \frac{q^{63}(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^{10} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)}{(2, q - 1)}
\]
and \(|\text{Out}(E_7(q))| = (2, q - 1) f < (2, q - 1)q\). Hence,
\[
|G| \leq q^{64}(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^{10} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)
\]
\[
< q^{64+18+14+12+10+8+6+2} = q^{134}.
\]

By [Vasilev 1997, p. 5],
\[
m(G) = \frac{(q^{14} - 1)(q^9 + 1)(q^5 + 1)}{q - 1}
\]
\[
= (q^{13} + q^{12} + \cdots + q + 1)(q^9 + 1)(q^5 + 1) > q^{13+9+5} = q^{27}.
\]

Hence, \(|G| < q^{134} < q^{135} < m(G)^5\). \(\square\)
We note that this bound could be improved if the groups with minimal base size 5 were classified.

**Proof of Theorem 4.1.** If the action of $G$ on $\Omega$ is nonstandard, then the result follows by Proposition 4.9. Hence, we may assume that $G$ is standard.

If $G$ is alternating and not large base, then $\Omega$ is a set of partitions. Hence, $I(G, \Omega) < 2 \log |\Omega|$ by [Gill et al. 2022b, Lemma 6.6].

Therefore $G$ is classical, and the action of $G$ on $\Omega$ is a subspace action. If $G$ is as in Case (ii) of Definition 4.2, then $I(G, \Omega) < \frac{11}{3} \log |\Omega|$ by [Gill et al. 2022b, Lemma 6.7]. If $G_0 = \text{PSL}_d(q)$ and $\Omega$ is a set of subspaces, then the result follows by Proposition 4.4 or Lemma 4.6, respectively. If $G_0 \neq \text{PSL}_d(q)$ and $\Omega$ is a set of subspaces, then the result follows by Proposition 4.8. Hence, by [Burness et al. 2013, 5.4], we may assume that either $G_0 = \text{P}^+(\Omega_{8}(q))$ and $G$ contains a triality automorphism; or $G_0 = \text{Sp}_4(2^f)'$ and $G$ contains a graph automorphism. In the former case the result holds by Lemma 4.7. In the latter $I(G, \Omega) < \frac{11}{3} \log |\Omega|$ by [Gill et al. 2022b, Lemma 6.12].

□

5. Proof of Theorem 1.1

Here we use the form and notation of the O’Nan–Scott Theorem from [Praeger 1990]. We begin by considering groups of type PA, and then we prove Theorem 1.1.

**Lemma 5.1.** Let $G$ be a subgroup of $S_n$ of type PA that is not large-base. Then

$$I(G) < 5 \log n.$$  

**Proof.** Since $G$ is of type PA there exists an integer $r \geq 2$, a finite set $\Delta$ and an almost simple subgroup $H$ of $\text{Sym}(\Delta)$ such that $G \leq H \ltimes S_r$. Since $G$ is not large base, neither is $H$. Let $s = |\Delta|$, so that $n = s^r$ with $s \geq 5$. Then

$$I(G, \Omega) \leq I(H^r, \Delta^r) + \ell(S_r) \quad (\text{by Lemma 2.3(i) and (ii)}),$$

$$\leq I(H^r, \Delta^r) + \frac{3}{2} r \quad (\text{by [Cameron et al. 1989]}),$$

$$\leq r(I(H, \Delta) - 1) + 1 + \frac{3}{2} r \quad (\text{by [Gill et al. 2022b, Lemma 2.6]}),$$

$$< r(5 \log s - 2) + 1 + \frac{3}{2} r \quad (\text{by Theorem 4.1}),$$

$$< 5 \log s^r - \frac{1}{2} r + 1$$

$$\leq 5 \log n \quad (\text{since } r \geq 2).$$

□

We can now prove Theorem 1.1.

**Proof of Theorem 1.1.** Let $G$ be a primitive group which is not large base. If $G$ is almost simple, then the result holds by Theorem 4.1. If $G$ is of type PA, then the result holds by Lemma 5.1. For all other $G$, the result holds by [Gill et al. 2022b, Propositions 3.1, 4.1 and 5.1]. □
Acknowledgements

The authors would like to thank Nick Gill for encouraging us to look at this problem, Peter Cameron for his helpful remarks, and the reviewer for their insightful comments, which have significantly improved the paper.

References


Received July 29, 2021. Revised November 15, 2021.

VERONICA KELSEY
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MANCHESTER
MANCHESTER
UNITED KINGDOM
veronica.kelsey@manchester.ac.uk

COLVA M. RONEY-DOUGAL
MATHEMATICAL INSTITUTE
UNIVERSITY OF ST. ANDREWS
FIFE
UNITED KINGDOM
colva.roney-dougal@st-andrews.ac.uk
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local data of rational elliptic curves with nontrivial torsion</td>
<td>1</td>
</tr>
<tr>
<td>Alexander J. Barrios and Manami Roy</td>
<td></td>
</tr>
<tr>
<td>A note on the two-dimensional Lagrangian mean curvature equation</td>
<td>43</td>
</tr>
<tr>
<td>Arunima Bhattacharya</td>
<td></td>
</tr>
<tr>
<td>A new gap for complete hypersurfaces with constant mean curvature in space forms</td>
<td>51</td>
</tr>
<tr>
<td>Juan-Ru Gu, Li Lei and Hong-Wei Xu</td>
<td></td>
</tr>
<tr>
<td>Prime thick subcategories on elliptic curves</td>
<td>69</td>
</tr>
<tr>
<td>Yuki Hirano and Genki Ouchi</td>
<td></td>
</tr>
<tr>
<td>On relational complexity and base size of finite primitive groups</td>
<td>89</td>
</tr>
<tr>
<td>Veronica Kelsey and Colva M. Roney-Dougal</td>
<td></td>
</tr>
<tr>
<td>An algorithm taking Kirby diagrams to trisection diagrams</td>
<td>109</td>
</tr>
<tr>
<td>Willi Kepplinger</td>
<td></td>
</tr>
<tr>
<td>Short closed geodesics on cusped hyperbolic surfaces</td>
<td>127</td>
</tr>
<tr>
<td>Hanh Vo</td>
<td></td>
</tr>
<tr>
<td>Generalizations of degeneracy second main theorem and Schmidt’s subspace theorem</td>
<td>153</td>
</tr>
<tr>
<td>Si Duc Quang</td>
<td></td>
</tr>
<tr>
<td>Generalized ideal classes in application to toroidal solenoids</td>
<td>189</td>
</tr>
<tr>
<td>Maria Sabitova</td>
<td></td>
</tr>
<tr>
<td>Erratum to the article Split bounded extension algebras and Han’s conjecture</td>
<td>229</td>
</tr>
<tr>
<td>Claude Cibils, Marcelo Lanzilotta, Eduardo N. Marcos and Andrea Solotar</td>
<td></td>
</tr>
</tbody>
</table>