Received: 31 August 2023 | Revised: 16 January 2024 | Accepted: 2 February 2024

DOI: 10.1112/blms.13027

RESEARCH ARTICLE

Bulletin of the London Mathematical Society

Irredundant bases for the symmetric group

Colva M. Roney-Dougal | **Peiran Wu**

School of Mathematics and Statistics, University of St Andrews, St Andrews, UK

Correspondence
Peiran Wu, School of Mathematics and Statistics, University of St Andrews, St Andrews KY16 9SS, UK.
Email: pw72@st-andrews.ac.uk

Funding information
Isaac Newton Institute for Mathematical Sciences; EPSRC, Grant/Award Number: EP/R014604/1; Simons Foundation

Abstract

An irredundant base of a group G acting faithfully on a finite set Γ is a sequence of points in Γ that produces a strictly descending chain of pointwise stabiliser subgroups in G, terminating at the trivial subgroup. Suppose that G is S_n or A_n acting primitively on Γ, and that the point stabiliser is primitive in its natural action on n points. We prove that the maximum size of an irredundant base of G is $O\left(\sqrt{n}\right)$, and in most cases $O\left((\log n)^2\right)$. We also show that these bounds are best possible.

MSC 2020
20B15 (primary), 20D06, 20E15 (secondary)

1 | INTRODUCTION

Let G be a finite group that acts faithfully and transitively on a set Γ with point stabiliser H. A sequence $(\gamma_1, \dots, \gamma_l)$ of points of Γ is an *irredundant base* for the action of G on Γ if

$$G > G_{\gamma_1} > G_{\gamma_1,\gamma_2} > \cdots > G_{\gamma_1,\dots,\gamma_l} = 1. \tag{1}$$

Let $\mathrm{b}(G,H)$ and $\mathrm{I}(G,H)$ denote the minimum and the maximum sizes of an irredundant base in Γ for G respectively.

Recently, Gill and Liebeck showed in [7] that if G is an almost simple group of Lie type of rank r over the field $\mathbb{F}_{p^f}$ of characteristic p and G is acting primitively, then

$$\mathrm{I}(G,H) \leqslant 177r^8 + \Omega(f),$$

where $\Omega(f)$ is the number of prime factors of f, counted with multiplicity.

Suppose now that G is the symmetric group S_n or the alternating group A_n. An upper bound for $\mathrm{I}(G,H)$ is the maximum length of a strictly descending chain of subgroups in G, known as the *length*, $\ell(G)$, of G. Define $\varepsilon(G) := \ell(G/\operatorname{soc} G)$. Cameron, Solomon, and Turull proved in [4] that

$$\ell(G) = \left\lfloor \frac{3n-3}{2} \right\rfloor - b_n + \varepsilon(G),$$

where b_n denotes the number of 1s in the binary representation of n. For $n \geqslant 2$, this gives

$$\ell(G) \leqslant \frac{3}{2}n - 3 + \varepsilon(G). \tag{2}$$

This type of upper bound is best possible for such G in general, in that for the natural action of S_n or A_n on n points, the maximum irredundant base size is $n-2+\varepsilon(G)$. A recent paper [8] by Gill and Lodà determined the exact values of $\mathrm{I}(G,H)$ when H is maximal and intransitive in its natural action on n points, and in each case $\mathrm{I}(G,H) \geqslant n-3+\varepsilon(G)$.

In this article, we present improved upper bounds for $\mathrm{I}(G,H)$ in the case where H is primitive. Note that whenever we refer to the 'primitivity' of a subgroup of G, we do so with respect to the natural action of G on n points. We say that a primitive subgroup H of G is *large* if there are integers m and k such that H is $(\mathrm{S}_m \wr \mathrm{S}_k) \cap G$ in product action on $n = m^k$ points or there are integers m and r such that H is $\mathrm{S}_m \cap G$ acting on the r-subsets of a set of size m, i.e. on $n = \binom{m}{r}$ points. Logarithms are taken to the base 2.

Theorem 1. *Suppose G is S_n or A_n $(n \geqslant 7)$ and $H \neq \mathrm{A}_n$ is a primitive maximal subgroup of G.*

(i) *Either $\mathrm{I}(G,H) < (\log n)^2 + \log n + 1$, or H is large and $\mathrm{I}(G,H) < 3\sqrt{n} - 1$.*
(ii) *There are infinitely many such G and H for which $\mathrm{I}(G,H) \geqslant \sqrt{n}$.*
(iii) *There are infinitely many such G and H for which*

$$\mathrm{I}(G,H) > (\log n)^2/(2(\log 3)^2) + \log n/(2\log 3)$$

and H is not large.

We also state our upper bounds for $\mathrm{I}(G,H)$ in terms of $t := |G : H|$. It is easy to show that $\mathrm{I}(G,H) \leqslant \mathrm{b}(G,H)\log t$. Burness, Guralnick, and Saxl showed in [3] that with finitely many (known) exceptions, in fact $\mathrm{b}(G,H) = 2$, in which case it follows that

$$\mathrm{I}(G,H) \leqslant 2\log t.$$

Similar $O(\log t)$ upper bounds on the maximum irredundant base size were recently shown to hold for all non-large-base primitive groups of degree t [9, 10], raising the question of whether such bounds are best possible in our case. Using Theorem 1, we shall obtain better bounds in terms of t.

Corollary 2.

(i) *There exist constants $c_1, c_2 \in \mathbb{R}_{>0}$ such that, if G is S_n or A_n $(n \geqslant 7)$ and $H \neq \mathrm{A}_n$ is a primitive maximal subgroup of G of index t, then either $\mathrm{I}(G,H) < c_1(\log\log t)^2$, or H is large and $\mathrm{I}(G,H) < c_2(\log t/\log\log t)^{1/2}$.*
(ii) *There is a constant $c_3 \in \mathbb{R}_{>0}$ and infinitely many such G and H for which $\mathrm{I}(G,H) > c_3(\log t/\log\log t)^{1/2}$.*

(iii) *There is a constant* $c_4 \in \mathbb{R}_{>0}$ *and infinitely many such* G *and* H *for which* $\mathrm{I}(G,H) > c_4(\log\log t)^2$ *and* H *is not large.*

Remark 3. We may take $c_1 = 3.5, c_2 = 6.1, c_3 = 1, c_4 = 0.097$. If we assume $n > 100$, then $c_1 = 1.2$ and $c_2 = 4.4$ suffice.

A sequence $\mathcal{B}$ of points in Γ is *independent* if no proper subsequence $\mathcal{B}'$ satisfies $G_{(\mathcal{B}')} = G_{(\mathcal{B})}$. The maximum size of an independent sequence for the action of G on Γ is denoted $\mathrm{H}(G,H)$. It can be shown that $\mathrm{b}(G,H) \leqslant \mathrm{H}(G,H) \leqslant \mathrm{I}(G,H)$. Another closely related property of the action is the *relational complexity*, denoted $\mathrm{RC}(G,H)$, a concept which originally arose in model theory. Cherlin, Martin, and Saracino defined $\mathrm{RC}(G,H)$ in [5] under the name 'arity' and showed that $\mathrm{RC}(G,H) \leqslant \mathrm{H}(G,H) + 1$.

Corollary 4. *Suppose* G *is* S_n *or* A_n $(n \geqslant 7)$ *and* $H \neq \mathrm{A}_n$ *is a primitive maximal subgroup of* G. *Then either* $\mathrm{RC}(G,H) < (\log n)^2 + \log n + 2$, *or* H *is large and* $\mathrm{RC}(G,H) < 3\sqrt{n}$.

The maximal subgroups of the symmetric and alternating groups were classified in [1, 11]. In order to prove statements (i) and (ii) of Theorem 1, we examine two families of maximal subgroups in more detail and determine lower bounds on the maximum irredundant base size, given in the next two results.

Theorem 5. *Let* p *be an odd prime number and* d *a positive integer such that* $p^d \geqslant 7$ *and let* $n = p^d$. *Suppose* G *is* S_n *or* A_n *and* H *is* $\mathrm{AGL}_d(p) \cap G$. *If* $d = 1$, *then*

$$\mathrm{I}(G,H) = 1 + \Omega(p-1) + \varepsilon(G).$$

If $d \geqslant 2$ *and* $p = 3, 5$, *then*

$$\frac{d(d+1)}{2} + d - 1 + \varepsilon(G) \leqslant \mathrm{I}(G,H) < \frac{d(d+1)}{2}(1 + \log p) + \varepsilon(G).$$

If $d \geqslant 2$ *and* $p \geqslant 7$, *then*

$$\frac{d(d+1)}{2} + d\,\Omega(p-1) - 1 + \varepsilon(G) \leqslant \mathrm{I}(G,H) < \frac{d(d+1)}{2}(1 + \log p) + \varepsilon(G).$$

Theorem 6. *Let* $m \geqslant 5$ *and* $k \geqslant 2$ *be integers and let* $n = m^k$. *Suppose* G *is* S_n *or* A_n *and* H *is* $(\mathrm{S}_m \wr \mathrm{S}_k) \cap G$ *in product action. Then*

$$1 + (m-1)(k-1) + \varepsilon(G) \leqslant \mathrm{I}(G,H) \leqslant \frac{3}{2}mk - \frac{1}{2}k - 1.$$

After laying out some preliminary results in Section 2, we shall prove Theorems 5 and 6 in Sections 3 and 4, respectively, before proving Theorem 1 and Corollary 2 in Section 5.

2 | THE MAXIMUM IRREDUNDANT BASE SIZE

In this section, we collect two general lemmas. Let G be a finite group acting faithfully and transitively on a set Γ with point stabiliser H. If $(\gamma_1, \dots, \gamma_l)$ is an irredundant base of G, then it satisfies

(1). The tail of the chain in (1) is a strictly descending chain of subgroups in G_{γ_1}, which is conjugate to H. Therefore,

$$\mathrm{I}(G, H) \leqslant \ell(H) + 1 \leqslant \Omega(|H|) + 1.$$

To obtain a lower bound for $\mathrm{I}(G, H)$, one approach is to look for a large explicit irredundant base. The following lemma says it suffices to find a long chain of subgroups in G such that every subgroup in the chain is a pointwise stabiliser of some subset in Γ.

Lemma 2.1. *Let l be the largest natural number such that there are subsets $\Delta_0, \Delta_1, \dots, \Delta_l \subseteq \Gamma$ satisfying*

$$G_{(\Delta_0)} > G_{(\Delta_1)} > \cdots > G_{(\Delta_l)}.$$

Then $\mathrm{I}(G, H) = l$.

Proof. Since l is maximal, we may assume that $\Delta_0 = \emptyset$ and $\Delta_l = \Gamma$ and that $\Delta_{i-1} \subseteq \Delta_i$, replacing Δ_i with $\Delta_1 \cup \cdots \cup \Delta_i$ if necessary. For each $i \in \{1, \dots, l\}$, write $\Delta_i \setminus \Delta_{i-1} = \{\gamma_{i,1}, \dots, \gamma_{i,m_i}\}$. Then $(\gamma_{1,1}, \dots, \gamma_{1,m_1}, \gamma_{2,1}, \dots, \gamma_{2,m_2}, \dots, \gamma_{l,1}, \dots, \gamma_{l,m_l})$ is a base for G and every subgroup $G_{(\Delta_i)}$ appears in the corresponding chain of point stabilisers. Therefore, by removing all redundant points, we obtain an irredundant base of size at least l, so $\mathrm{I}(G, H) \geqslant l$.

On the other hand, given any irredundant base $(\gamma_1, \dots, \gamma_m)$ of G, we can take $\Delta_i := \{\gamma_1, \dots, \gamma_i\}$. Therefore, $\mathrm{I}(G, H) = l$. □

Once we have an upper or lower bound for $\mathrm{I}(G, H)$, we can easily obtain a corresponding bound for the maximum irredundant base size of various subgroups of G.

Lemma 2.2. *Suppose M is a subgroup of S_n with $M \nleqslant \mathrm{A}_n$. Then*

$$\mathrm{I}(\mathrm{S}_n, M) - 1 \leqslant \mathrm{I}(\mathrm{A}_n, M \cap \mathrm{A}_n) \leqslant \mathrm{I}(\mathrm{S}_n, M).$$

Proof. This follows immediately from [9, Lemma 2.8; 10, Lemma 2.3]. □

3 | THE AFFINE CASE

In this section, we prove Theorem 5. The upper bounds will follow easily from examinations of group orders. Therefore, we focus most of our efforts on the construction of an irredundant base, leading to the lower bounds.

Let p be a prime number and d be an integer such that $p^d \geqslant 7$ and let V be a d-dimensional vector space over the field $\mathbb{F}_p$. Let G be $\mathrm{Sym}(V)$ or $\mathrm{Alt}(V)$. Consider the affine group $\mathrm{AGL}(V)$, the group of all invertible affine transformations of V, and let $H := \mathrm{AGL}(V) \cap G$.

Theorem 3.1 [11]. *The subgroup H is maximal in G (with $p^d \geqslant 7$) if and only if one of the following holds:*

(i) $d \geqslant 2$ *and* $p \geqslant 3$*;*
(ii) $G = \mathrm{Sym}(V)$*,* $d = 1$*, and* $p \geqslant 7$*;*

(iii) $G = \mathrm{Alt}(V)$, $d \geqslant 3$, *and* $p = 2$;
(iv) $G = \mathrm{Alt}(V)$, $d = 1$, *and* $p = 13, 19$ *or* $p \geqslant 29$.

In this section, we only consider the case where p is odd. Owing to Lemma 2.2, we shall assume $G = \mathrm{Sym}(V)$ and $H = \mathrm{AGL}(V)$ for now. In the light of Lemma 2.1, we introduce a subgroup T of diagonal matrices and look for groups containing T that are intersections of G-conjugates of H (Subsection 3.1) and subgroups of T that are such intersections (Subsection 3.2), before finally proving Theorem 5 (Subsection 3.3).

3.1 | Subspace stabilisers and the diagonal subgroup

Let T be the subgroup of all diagonal matrices in $\mathrm{GL}(V)$ with respect to a basis $\mathbf{b}_1, \dots, \mathbf{b}_d$. Let μ be a primitive element of $\mathbb{F}_p$. We now find a strictly descending chain of groups from $\mathrm{Sym}(V)$ to T consisting of intersections of G-conjugates of H. We treat the cases $d = 1$ and $d \geqslant 2$ separately.

Lemma 3.2. *Suppose $d = 1$ and $G = \mathrm{Sym}(V)$. Then there exists $x \in G$ such that $H \cap H^x = T$.*

Proof. Since V is one-dimensional, $\mathrm{GL}(V) = T$ is generated by the scalar multiplication m_μ by μ. Let $\mathbf{u} \in V \setminus \{\mathbf{0}\}$ and let $t_\mathbf{u}$ be the translation by $\mathbf{u}$. Then $H = \langle t_\mathbf{u} \rangle \rtimes \langle m_\mu \rangle$ is the normaliser of $\langle t_\mathbf{u} \rangle$ in G and $\langle t_\mathbf{u} \rangle$ is a characteristic subgroup of H. Hence H is self-normalising in G. Define (in cycle notation)

$$x := (\mathbf{u}\ \ \mu^{-1}\mathbf{u})(\mu\mathbf{u}\ \ \mu^{-2}\mathbf{u}) \cdots (\mu^{\frac{p-3}{2}}\mathbf{u}\ \ \mu^{-\frac{p-1}{2}}\mathbf{u}) \in G.$$

Then $x \notin H$ and so x does not normalise H. But x normalises $\langle m_\mu \rangle$, as ${m_\mu}^x = {m_\mu}^{-1}$. Therefore,

$$T = \langle m_\mu \rangle \leqslant H \cap H^x < H.$$

Since the index $|H : T| = p$ is prime, $H \cap H^x = T$. □

The following two lemmas concern the case $d \geqslant 2$. An affine subspace of V is a subset of the form $\mathbf{v} + W$, where $\mathbf{v} \in V$ and W is a vector subspace of V. The (affine) dimension of $\mathbf{v} + W$ is the linear dimension of W. For an affine transformation $h = g t_\mathbf{u}$ with $g \in \mathrm{GL}(V)$ and $t_\mathbf{u}$ denoting the translation by some $\mathbf{u} \in V$, if $\mathrm{fix}(h)$ is non-empty, then $\mathrm{fix}(h)$ is an affine subspace of V, since $\mathrm{fix}(h) = \mathbf{v} + \ker(g - \mathrm{id}_V)$ for any $\mathbf{v} \in \mathrm{fix}(h)$.

Lemma 3.3. *Suppose $d \geqslant 2$, $p \geqslant 3$, and $G = \mathrm{Sym}(V)$. Let W be a proper, non-trivial subspace of V and let $K < \mathrm{GL}(V)$ be the setwise stabiliser of W. Then there exists $x \in G$ such that $H \cap H^x = K$.*

Proof. Let $\lambda \in \mathbb{F}_p^\times \setminus \{1\}$ and define $x \in \mathrm{Sym}(V)$ by setting

$$\mathbf{v}^x := \begin{cases} \lambda\mathbf{v}, & \text{if } \mathbf{v} \in W, \\ \mathbf{v}, & \text{otherwise.} \end{cases}$$

We first show that $K = \mathrm{C}_H(x)$ and then that $H \cap H^x = \mathrm{C}_H(x)$.

Firstly, let $g \in K$. For all $\mathbf{v} \in W$, we calculate that $\mathbf{v}^{g^x} = (\lambda^{-1}\mathbf{v})^{gx} = (\lambda^{-1}\mathbf{v}^g)^x = \mathbf{v}^g$. For all $\mathbf{v} \in V \setminus W$, we see that $\mathbf{v}^{g^x} = \mathbf{v}^{gx} = \mathbf{v}^g$. Hence $g^x = g$, and so $K \leqslant \mathrm{C}_H(x)$. Now, let h be an element of $\mathrm{C}_H(x)$ and write $h = gt_{\mathbf{u}}$ with $g \in \mathrm{GL}(V)$ and $\mathbf{u} \in V$, so that $h^{-1} = t_{-\mathbf{u}}g^{-1}$. Suppose for a contradiction that there exists $\mathbf{v} \in W \setminus \{\mathbf{0}\}$ with $\lambda\mathbf{v}^g + \mathbf{u} \notin W$. Then

$$\mathbf{v} = \mathbf{v}^{xhx^{-1}h^{-1}} = (\lambda\mathbf{v})^{hx^{-1}h^{-1}} = (\lambda\mathbf{v}^g + \mathbf{u})^{x^{-1}h^{-1}} = (\lambda\mathbf{v}^g + \mathbf{u})^{h^{-1}} = \lambda\mathbf{v}.$$

Since $\lambda \neq 1$, this is a contradiction and so for all $\mathbf{v} \in W$,

$$\mathbf{v} = (\lambda\mathbf{v}^g + \mathbf{u})^{x^{-1}h^{-1}} = (\mathbf{v}^g + \lambda^{-1}\mathbf{u})^{h^{-1}} = \mathbf{v} + (\lambda^{-1} - 1)\mathbf{u}^{g^{-1}}.$$

Hence $\mathbf{u} = \mathbf{0}$ and $\mathbf{v}^g \in W$. Therefore, $h = gt_{\mathbf{0}}$ stabilises W, whence $h \in K$. Thus, $\mathrm{C}_H(x) = K$.

Since $\mathrm{C}_H(x) \leqslant H \cap H^x$, it remains to show that $H \cap H^x \leqslant \mathrm{C}_H(x)$. Suppose otherwise. Then there is some $h \in H \cap H^x$ such that $h' := xhx^{-1}h^{-1} \neq 1$. The set $\mathrm{fix}(h')$ is either empty or an affine subspace of dimension at most $d-1$. Moreover, for any $\mathbf{v} \in V$, if $\mathbf{v} \notin (W \setminus \{\mathbf{0}\}) \cup W^{h^{-1}}$, then x fixes both $\mathbf{v}$ and $\mathbf{v}^h$, and $\mathbf{v}^{h'} = \mathbf{v}^{hx^{-1}h^{-1}} = \mathbf{v}^{hh^{-1}} = \mathbf{v}$, when $\mathbf{v} \in \mathrm{fix}(h')$. Therefore,

$$V = (W \setminus \{\mathbf{0}\}) \cup W^{h^{-1}} \cup \mathrm{fix}(h').$$

Then

$$p^d = |V| \leqslant \left|W \setminus \{\mathbf{0}\}\right| + \left|W^{h^{-1}}\right| + \left|\mathrm{fix}(h')\right| \leqslant (p^{d-1} - 1) + p^{d-1} + p^{d-1} = 3p^{d-1} - 1.$$

This is a contradiction as $p \geqslant 3$, and so $H \cap H^x = \mathrm{C}_H(x) = K$. $\square$

We now construct a long chain of subgroups of G by intersecting subspace stabilisers.

Lemma 3.4. *Suppose $d \geqslant 2$ and $G = \mathrm{Sym}(V)$. Let $l_1 := d(d+1)/2 - 1$. Then there exist stabilisers $K_1, \dots, K_{l_1}$ in $\mathrm{GL}(V)$ of linear subspaces such that*

$$G > H > K_1 > K_1 \cap K_2 > \cdots > \bigcap_{i=1}^{l_1} K_i = T. \tag{3}$$

Proof. Let $\mathcal{I} := \{(i,j) \mid i,j \in \{1,\dots,d\}, i \leqslant j\} \setminus \{(1,d)\}$ be ordered lexicographically. Note that $|\mathcal{I}| = l_1$. For each $(i,j) \in \mathcal{I}$, let $K_{i,j}$ be the stabiliser in $\mathrm{GL}(V)$ of $\langle \mathbf{b}_i, \mathbf{b}_{i+1}, \dots, \mathbf{b}_j \rangle$ and define $\mathcal{I}_{i,j} := \{(k,l) \in \mathcal{I} \mid (k,l) \leqslant (i,j)\}$. Since $T \leqslant K_{i,j}$ for all i, j, we see that

$$T \leqslant \bigcap_{(i,j)\in\mathcal{I}} K_{i,j} \leqslant \bigcap_{i=1}^{d} K_{i,i} = T.$$

Hence equality holds, proving the final equality in (3).

We now show that, for all $(i,j) \in \mathcal{I}$,

$$\bigcap_{(k,l)\in\mathcal{I}_{(i,j)}\setminus\{(i,j)\}} K_{k,l} > \bigcap_{(k,l)\in\mathcal{I}_{(i,j)}} K_{k,l}.$$

For $1 \leqslant j < d$, let $g_{1,j}$ be the linear map that sends $\mathbf{b}_j$ to $\mathbf{b}_j + \mathbf{b}_{j+1}$ and fixes $\mathbf{b}_k$ for $k \neq j$. Then $g_{1,j}$ stabilises $\langle \mathbf{b}_1 \rangle, \ldots, \langle \mathbf{b}_{j-1} \rangle$ and any sum of these subspaces, but not $\langle \mathbf{b}_1, \ldots, \mathbf{b}_j \rangle$. Hence $g_{1,j} \in K_{1,l}$ for all $l < j$ but $g_{1,j} \notin K_{1,j}$. For $2 \leqslant i \leqslant j \leqslant d$, let $g_{i,j}$ be the linear map that sends $\mathbf{b}_j$ to $\mathbf{b}_{i-1} + \mathbf{b}_j$ and fixes $\mathbf{b}_k$ for $k \neq j$. Then $g_{i,j}$ stabilises $\langle \mathbf{b}_1 \rangle, \ldots, \langle \mathbf{b}_{j-1} \rangle, \langle \mathbf{b}_j, \mathbf{b}_{i-1} \rangle, \langle \mathbf{b}_{j+1} \rangle, \ldots, \langle \mathbf{b}_d \rangle$ and any sum of these subspaces, but not $\langle \mathbf{b}_i, \ldots, \mathbf{b}_j \rangle$. Hence $g_{i,j} \in K_{k,l}$ for all $(k,l) < (i,j)$ but $g_{i,j} \notin K_{i,j}$.

Therefore, the $K_{i,j}$s, ordered lexicographically by the subscripts, are as required. □

We have now found the initial segment of an irredundant base of $\mathrm{Sym}(V)$. The next subsection extends this to a base.

3.2 | Subgroups of the diagonal subgroup

We now show that, with certain constraints on p, every subgroup of T is an intersection of G-conjugates of T, and hence, by Lemma 3.4, an intersection of G-conjugates of H. We first prove a useful result about subgroups of the symmetric group generated by a k-cycle.

Lemma 3.5. *Let $s \in \mathrm{S}_m$ be a cycle of length $k < m$ and let a be a divisor of k. Suppose that $(k,a) \neq (4,2)$. Then there exists $x \in \mathrm{S}_m$ such that*

$$\langle s \rangle \cap \langle s \rangle^x = \langle s^a \rangle.$$

Proof. Without loss of generality, assume $s = (1\,2\, \cdots\, k)$ and $a > 1$. If $a = k$, then take $x := (1\, m)$, so that $\langle s \rangle \cap \langle s \rangle^x = 1$, as $m \notin \mathrm{supp}(s^i)$ and $m \in \mathrm{supp}((s^i)^x)$ for all $1 \leqslant i < k$. Hence we may assume $a < k$ and $k \neq 4$. We find that

$$s^a = (1\;\; a+1\;\; \cdots\;\; k-a+1)(2\;\; a+2\;\; \cdots\;\; k-a+2)\cdots(a\;\; 2a\;\; \cdots\;\; k).$$

Let

$$x := (1\;\; 2\;\; \cdots\;\; a)(a+1\;\; a+2\;\; \cdots\;\; 2a)\cdots(k-a+1\;\; k-a+2\;\; \cdots\;\; k).$$

Then $(s^a)^x = s^a$. Hence $\langle s^a \rangle = \langle s^a \rangle^x \leqslant \langle s \rangle \cap \langle s \rangle^x$.

To prove that equality holds, suppose $\langle s^a \rangle < \langle s \rangle \cap \langle s \rangle^x$. Then there exists $b \in \{1, \ldots, a-1\}$ such that $(s^b)^x = s^c$ for some c not divisible by a. Computing

$$1^{s^c} = 1^{x^{-1}s^b x} = a^{s^b x} = (a+b)^x = a+b+1 = 1^{s^{a+b}}.$$

Therefore,

$$2^{s^c} = 2^{s^{a+b}} = \begin{cases} a+b+2, & \text{if } b \neq a-1 \text{ or } k > 2a, \\ 1, & \text{if } b = a-1 \text{ and } k = 2a. \end{cases} \tag{4}$$

On the other hand,

$$2^{x^{-1}s^b x} = 1^{s^b x} = (b+1)^x = \begin{cases} b+2, & \text{if } b \neq a-1, \\ 1, & \text{if } b = a-1. \end{cases} \tag{5}$$

Comparing (4) and (5), we see that $b = a - 1$ and $k = 2a$. In particular, $a \neq 2$ by the assumption that $k \neq 4$. It follows that $a^{s^c} = a^{s^{a+b}} = a - 1$, whereas

$$a^{x^{-1}s^b x} = (a-1)^{s^b x} = (2a-2)^x = 2a - 1,$$

a contradiction. The result follows. $\square$

Recall from Subsection 3.1 the subgroup T of $\mathrm{GL}(V)$ and the primitive element μ of $\mathbb{F}_p$. For each $i \in \{1, \dots, d\}$, let $g_i \in \mathrm{GL}(V)$ send $\mathbf{b}_i$ to $\mu\mathbf{b}_i$ and fix $\mathbf{b}_j$ for $j \neq i$. Then $T = \langle g_1, \dots, g_d \rangle$.

Lemma 3.6. *Suppose $d \geqslant 1$, $p \geqslant 3$, and $G = \mathrm{Sym}(V)$. Let $i \in \{1, \dots, d\}$ and let a be a divisor of $(p-1)$ with $(p, a) \neq (5, 2)$. Then there exists $x \in G$ such that*

$$T \cap T^x = \left\langle g_1, \dots, g_{i-1}, {g_i}^a, g_{i+1}, \dots, g_d \right\rangle.$$

Proof. Up to a change of basis, $i = 1$. The map $g_1 \in \mathrm{GL}(V) < G$ has a cycle $s = (\mathbf{b}_1\ \mu\mathbf{b}_1\ \mu^2\mathbf{b}_1\ \cdots\ \mu^{p-2}\mathbf{b}_1)$. Treating s as a permutation on the subspace $\langle \mathbf{b}_1 \rangle$, we see that, for all $\mathbf{u} \in \langle \mathbf{b}_1 \rangle$ and $\mathbf{w} \in \langle \mathbf{b}_2, \dots, \mathbf{b}_d \rangle$ (if $d = 1$, then consider $\mathbf{w} = \mathbf{0}$),

$$(\mathbf{u} + \mathbf{w})^{g_1} = \mathbf{u}^{g_1} + \mathbf{w} = \mathbf{u}^s + \mathbf{w}.$$

By Lemma 3.5, since s is a $(p-1)$-cycle and $(p-1, a) \neq (4, 2)$, there exists $x \in \mathrm{Sym}(\langle \mathbf{b}_1 \rangle)$ such that $\langle s \rangle \cap \langle s \rangle^x = \langle s^a \rangle$. Define $\tilde{x} \in G$ by setting

$$(\mathbf{u} + \mathbf{w})^{\tilde{x}} := \mathbf{u}^x + \mathbf{w}$$

for all $\mathbf{u} \in \langle \mathbf{b}_1 \rangle$ and $\mathbf{w} \in \langle \mathbf{b}_2, \dots, \mathbf{b}_d \rangle$. Let g be any element of T and write $g = g_1^c g'$ with $c \in \{1, \dots, p-1\}$ and $g' \in \langle g_2, \dots, g_d \rangle$. Then, with $\mathbf{u}$ and $\mathbf{w}$ as above,

$$(\mathbf{u} + \mathbf{w})^g = \mathbf{u}^{g_1^c} + \mathbf{w}^{g'} = \mathbf{u}^{s^c} + \mathbf{w}^{g'}$$

and similarly

$$(\mathbf{u} + \mathbf{w})^{g^{\tilde{x}}} = \mathbf{u}^{(s^c)^x} + \mathbf{w}^{g'}.$$

Hence $g^{\tilde{x}} \in T$ if and only if $(s^c)^x \in \langle s \rangle$, which holds if and only if $a \mid c$. Therefore, $T \cap T^{\tilde{x}} = \left\langle g_1^a, g_2, \dots, g_d \right\rangle$, as required. $\square$

Lemma 3.7. *Suppose $d \geqslant 1$, $p \geqslant 3$, and $G = \mathrm{Sym}(V)$. Let $l_2 := d$ if $p = 3, 5$, and $l_2 := d\,\Omega(p-1)$ otherwise. Then there are subsets $Y_1, \dots, Y_{l_2} \subseteq G$ such that*

$$T > \bigcap_{x \in Y_1} T^x > \bigcap_{x \in Y_2} T^x > \cdots > \bigcap_{x \in Y_{l_2}} T^x = 1.$$

Proof. First, suppose $p = 3$ or $p = 5$. For all $i \in \{1, \dots, d\}$, by Lemma 3.6, there exists $y_i \in G$ such that

$$T \cap T^{y_i} = \left\langle g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_d \right\rangle;$$

setting $Y_i := \{y_1, \dots, y_i\}$ gives

$$\bigcap_{x \in Y_i} T^x = \langle g_{i+1}, \dots, g_d \rangle.$$

Therefore, $Y_1, \dots, Y_d$ are as required.

Now, suppose $p \geqslant 7$. Let $a_1, \dots, a_{\Omega(p-1)}$ be a sequence of factors of $(p-1)$ such that $a_i \mid a_{i+1}$ for all i. Let $\mathcal{I} := \{1, \dots, d\} \times \{1, \dots, \Omega(p-1)\}$ be ordered lexicographically. For each pair $(i,j) \in \mathcal{I}$, by Lemma 3.6, there exists $y_{i,j} \in G$ such that

$$T \cap T^{y_{i,j}} = \langle g_1, \dots, g_{i-1}, g_i{}^{a_j}, g_{i+1}, \dots, g_d \rangle;$$

setting $Y_{i,j} := \{y_{i',j'} \mid (i',j') \in \mathcal{I}, (i',j') < (i,j)\}$ gives

$$\bigcap_{x \in Y_{i,j}} T^x = \langle g_i{}^{a_j}, g_{i+1}, \dots, g_d \rangle.$$

Therefore, the $Y_{i,j}$s, ordered lexicographically by the subscripts, are as required. □

This completes our preparations for the proof of Theorem 5.

3.3 | Proof of Theorem 5

Recall the assumption that G is S_{p^d} or A_{p^d} (p is an odd prime and $p^d \geqslant 7$), which we identify here with $\mathrm{Sym}(V)$ or $\mathrm{Alt}(V)$, and $H = \mathrm{AGL}_d(p) \cap G$, which we identify with $\mathrm{AGL}(V) \cap G$.

Proof of Theorem 5. First, suppose $d \geqslant 2$, $p \geqslant 3$, and $G = \mathrm{Sym}(V)$. Let $K_1, \dots, K_{l_1}$ be as in Lemma 3.4. For each $i \in \{1, \dots, l_1\}$, by Lemma 3.3, there exists $x_i \in G$ such that $H \cap H^{x_i} = K_i$. Define $X_i := \{1\} \cup \{x_j \mid 1 \leqslant j < i\} \subseteq G$ for all such i. Then by Lemma 3.4,

$$G > H = \bigcap_{x \in X_1} H^x > \bigcap_{x \in X_2} H^x > \cdots > \bigcap_{x \in X_{l_1+1}} H^x = T. \tag{6}$$

Let $Y_1, \dots, Y_{l_2} \subseteq G$ be as in Lemma 3.7. For each $i \in \{1, \dots, l_2\}$, let $Z_i := \{xy \mid x \in X_{l_1+1}, y \in Y_i\}$, so that

$$\bigcap_{z \in Z_i} H^z = \bigcap_{y \in Y_i} \left(\bigcap_{x \in X_{l_1+1}} H^x \right)^y = \bigcap_{y \in Y_i} T^y.$$

Then Lemma 3.7 gives

$$T > \bigcap_{z \in Z_1} H^x > \bigcap_{z \in Z_2} H^x > \cdots > \bigcap_{z \in Z_{l_2}} H^x = 1. \tag{7}$$

Concatenating the chains (6) and (7), we obtain a chain of length $l_1 + l_2 + 1$.

Now, suppose $d \geqslant 2$, $p \geqslant 3$, and G is $\mathrm{Sym}(V)$ or $\mathrm{Alt}(V)$. By Lemmas 2.1 and 2.2, since $\mathrm{AGL}(V) \nleq \mathrm{Alt}(V)$, the lower bounds in the theorem hold. For the upper bound on $\mathrm{I}(G, H)$, simply compute

$$\begin{aligned}\mathrm{I}(G,H) &\leqslant 1 + \Omega(|H|) \leqslant \Omega(p^d(p^d-1)(p^d-p)\cdots(p^d-p^{d-1})) + \varepsilon(G)\\ &< \frac{d(d+1)}{2} + \log((p^d-1)(p^{d-1}-1)\cdots(p-1)) + \varepsilon(G)\\ &< \frac{d(d+1)}{2}(1+\log p) + \varepsilon(G).\end{aligned}$$

Finally, suppose $d = 1$ and $p \geqslant 7$. Using Lemma 3.7, we obtain the chain (7) again. Concatenating the chain $G > H > T$ with (7) and applying Lemmas 2.1 and 2.2, we see that $\mathrm{I}(G, H) \geqslant 1 + \Omega(p-1) + \varepsilon(G)$. In fact, equality holds, as $\mathrm{I}(G, H) \leqslant 1 + \Omega(|H|) = 1 + \Omega(p-1) + \varepsilon(G)$. □

4 | THE PRODUCT ACTION CASE

In this section, we prove Theorem 6. Once again, most work goes into the explicit construction of an irredundant base in order to prove the lower bounds, while the upper bounds will be obtained easily from the length of S_n.

Throughout this section, let $m \geqslant 5$ and $k \geqslant 2$ be integers, and let G be S_{m^k} or A_{m^k}. Let $M := \mathrm{S}_m \wr \mathrm{S}_k$ act in product action on $\Delta := \{(a_1, \ldots, a_k) \mid a_1, \ldots, a_k \in \{1, \ldots, m\}\}$ and identify M with a subgroup of S_{m^k}.

Theorem 4.1 [11]. *The group $M \cap G$ is a maximal subgroup of G if and only if one of the following holds:*

(i) $m \equiv 1 \pmod 2$;
(ii) $G = \mathrm{S}_{m^k}$, $m \equiv 2 \pmod 4$, *and* $k = 2$;
(iii) $G = \mathrm{A}_{m^k}$, $m \equiv 0 \pmod 4$, *and* $k = 2$;
(iv) $G = \mathrm{A}_{m^k}$, $m \equiv 0 \pmod 2$, *and* $k \geqslant 3$.

The strategy to proving the lower bound in Theorem 6 is once again to find suitable two-point stabilisers from which a long chain of subgroups can be built.

For each pair of points $\alpha, \beta \in \Delta$, let $d(\alpha, \beta)$ denote the Hamming distance between α and β, namely the number of coordinates that differ.

Lemma 4.2. *Let $x \in M$. Then for all $\alpha, \beta \in \Delta$,*

$$d(\alpha^x, \beta^x) = d(\alpha, \beta).$$

Proof. Write x as $(v_1, \ldots, v_k)w$ with $v_1, \ldots, v_k \in \mathrm{S}_m$ and $w \in \mathrm{S}_k$. Let $\alpha = (a_1, \ldots, a_k)$ and $\beta = (b_1, \ldots, b_k)$. Write $\alpha^x = (a'_1, \ldots, a'_k)$ and $\beta^x = (b'_1, \ldots, b'_k)$. Then for each $i \in \{1, \ldots, k\}$,

$$a_i = b_i \iff {a_i}^{v_i} = {b_i}^{v_i} \iff a'_{i^w} = b'_{i^w}.$$

Since w is a permutation of $\{1, \ldots, k\}$, the result holds. □

Define $u \in \mathrm{S}_m$ to be $(1\ 2\ \cdots\ m)$ if m is odd, and $(1\ 2\ \cdots\ m-1)$ if m is even, so that u is an even permutation. Let $U := \langle u \rangle \leqslant \mathrm{S}_m$ and note that $\mathrm{C}_{\mathrm{S}_m}(u) = U$. The group U will play a central role in the next lemma.

Lemma 4.3. *Let $i \in \{2, \dots, k\}$ and $r \in \{1, \dots, m\}$. Let T_r be the stabiliser of r in S_m and let W_i be the pointwise stabiliser of 1 and i in S_k. Then there exists $x_{i,r} \in \mathrm{A}_{m^k}$ such that*

$$M \cap M^{x_{i,r}} = \left(U \times (\mathrm{S}_m)^{i-2} \times T_r \times (\mathrm{S}_m)^{k-i}\right) \rtimes W_i.$$

Proof. Without loss of generality, assume $i = 2$. Define $x = x_{2,r} \in \mathrm{Sym}(\Delta)$ by

$$(a_1, a_2, \dots, a_k)^x = \begin{cases} ({a_1}^u, a_2, \dots, a_k) & \text{if } a_2 = r, \\ (a_1, a_2, \dots, a_k) & \text{otherwise.} \end{cases}$$

The permutation x is a product of m^{k-2} disjoint $|u|$-cycles and is therefore even.

Let $K := \left(U \times T_r \times (\mathrm{S}_m)^{k-2}\right) \rtimes W_2$. We show first that $K \leqslant M \cap M^x$. Let $h = (v_1, \dots, v_m)w^{-1}$ be an element of K. Then $v_1 \in U$, v_2 fixes r, and w fixes 1 and 2. Therefore, for all $\alpha = (a_1, a_2, \dots, a_k) \in \Delta$, if $a_2 = r$, then

$$\begin{aligned} \alpha^{hx} &= ({a_1}^{v_1}, a_2, {a_{3^w}}^{v_{3^w}}, \dots, {a_{k^w}}^{v_{k^w}})^x = ({a_1}^{v_1 u}, a_2, {a_{3^w}}^{v_{3^w}}, \dots, {a_{k^w}}^{v_{k^w}}) \\ &= ({a_1}^{u v_1}, a_2, {a_{3^w}}^{v_{3^w}}, \dots, {a_{k^w}}^{v_{k^w}}) = ({a_1}^{u}, a_2, a_3, \dots, a_k)^h = \alpha^{xh}; \end{aligned}$$

and if $a_2 \neq r$, then

$$\begin{aligned} \alpha^{hx} &= ({a_1}^{v_1}, {a_2}^{v_2}, {a_{3^w}}^{v_{3^w}}, \dots, {a_{k^w}}^{v_{k^w}})^x = ({a_1}^{v_1}, {a_2}^{v_2}, {a_{3^w}}^{v_{3^w}}, \dots, {a_{k^w}}^{v_{k^w}}) \\ &= (a_1, a_2, a_3, \dots, a_k)^h = \alpha^{xh}. \end{aligned}$$

Therefore, x and h commute. Since h is arbitrary, $K = K \cap K^x \leqslant M \cap M^x$.

Let B be the base group $(\mathrm{S}_m)^k$ of M. Since $K \leqslant M \cap M^x$, we find that $B \cap K \leqslant B \cap M^x$. We now show that $B \cap M^x \leqslant B \cap K$, so let $h_1 = (v_1, \dots, v_k) \in B \cap M^x$. Then ${h_1}^{x^{-1}} \in M$. We show that $v_1 \in U$ and v_2 fixes r, so that $h_1 \in K$. By letting $g_1 := (1, 1, v_3, \dots, v_k) \in K$ and replacing h_1 with $g_1^{-1}h_1$, we may assume $v_3 = \cdots = v_k = 1$. Let $h_2 := xh_1x^{-1}h_1^{-1} = {h_1}^{x^{-1}}h_1^{-1} \in M$, and let $\alpha := (a, b, c, \dots, c)$ and $\beta := (a, r, c, \dots, c)$ be elements of Δ with $a \neq m$ and $b \notin \{r, r^{v_2^{-1}}\}$. Then α and α^{h_1} are both fixed by x, and so $\alpha^{h_2} = \alpha$. On the other hand,

$$\beta^{h_2} = \begin{cases} (a^{uv_1u^{-1}v_1^{-1}}, r, c, \dots, c), & \text{if } r^{v_2} = r, \\ (a^u, r, c, \dots, c), & \text{otherwise.} \end{cases}$$

Since $d(\alpha^{h_2}, \beta^{h_2}) = d(\alpha, \beta) = 1$ by Lemma 4.2 and $a^u \neq a$, it must be the case that $r^{v_2} = r$ and $a^{uv_1u^{-1}v_1^{-1}} = a$. Therefore, $v_2 \in T_r$ and, as a is arbitrary in $\{1, \dots, m-1\}$, we deduce that $v_1 \in \mathrm{C}_{\mathrm{S}_m}(u) = U$ and hence $h_1 \in K$. Thus, $B \cap M^x \leqslant B \cap K$ and so $B \cap M^x = B \cap K$.

To show that $M \cap M^x \leqslant K$, let $h_3 \in M \cap M^x$. Now, $B \trianglelefteq M$ and so $B \cap K = B \cap M^x \trianglelefteq M \cap M^x$. Therefore,

$$h_3 \in \mathrm{N}_M(B \cap K) = \left(\mathrm{N}_{\mathrm{S}_m}(U) \times T_r \times (\mathrm{S}_m)^{k-2}\right) \rtimes W_2.$$

The equality uses the fact that $\mathrm{N}_{\mathrm{S}_m}(U) \neq T_r$ (as $m \geqslant 5$). Through left multiplication by an element of K, we may assume $h_3 \in \mathrm{N}_{\mathrm{S}_m}(U) \times (1_{\mathrm{S}_m})^{k-1}$. Then $h_3 \in B \cap M^x \leqslant K$. Since h_3 is arbitrary, the intersection $M \cap M^x \leqslant K$. Therefore, $K = M \cap M^x$, as required. □

We are now ready to prove the main result for the product action case. Recall the assumption that G is S_{m^k} or A_{m^k} and $H = M \cap G$.

Proof of Theorem 6. Firstly, suppose that $H = M$. Let $\mathcal{I} := \{2, \dots, k\} \times \{1, \dots, m-1\}$, ordered lexicographically. For each $(i, r) \in \mathcal{I}$, let $x_{i,r} \in \mathrm{A}_{m^k} \leqslant G$ be as in Lemma 4.3, and define

$$X_{i,r} := \{1\} \cup \{x_{i',r'} \mid (i', r') \in \mathcal{I}, (i', r') \leqslant (i, r)\} \subseteq G.$$

Then for all $(i, r) \in \mathcal{I}$,

$$B \cap \bigcap_{x \in X_{i,r}} M^x = U \times (1_{\mathrm{S}_m})^{i-2} \times (\mathrm{S}_m)_{1,\dots,r} \times (\mathrm{S}_m)^{k-i}.$$

Hence, for all $(i, r), (j, s) \in \mathcal{I}$ with $(i, r) < (j, s)$, $\bigcap_{x \in X_{i,r}} M^x > \bigcap_{x \in X_{j,s}} M^x$. This results in the following chain of stabiliser subgroups, of length $(m-1)(k-1)+2$:

$$G > M > \bigcap_{x \in X_{2,1}} M^x > \cdots > \bigcap_{x \in X_{2,m-1}} M^x > \bigcap_{x \in X_{3,1}} M^x > \cdots > \bigcap_{x \in X_{k,m-1}} M^x > 1.$$

Therefore, by Lemma 2.1, $\mathrm{I}(G, H) = \mathrm{I}(G, M) \geqslant (m-1)(k-1)+2$.

Now, if $H \neq M$, then $G = \mathrm{A}_{m^k}$, and $\mathrm{I}(G, H) \geqslant \mathrm{I}(\mathrm{S}_{m^k}, M) - 1 \geqslant (m-1)(k-1)+1$ by Lemma 2.2.

Finally, for the upper bound on $\mathrm{I}(G, H)$, we use (2) and [4, Lemma 2.1] to compute

$$\begin{aligned} \mathrm{I}(G, H) &\leqslant 1 + \ell(H) \leqslant 1 + \ell(M) \leqslant 1 + k\,\ell(\mathrm{S}_m) + \ell(\mathrm{S}_k) \\ &\leqslant 1 + k\left(\frac{3}{2}m - 2\right) + \left(\frac{3}{2}k - 2\right) \leqslant \frac{3}{2}mk - \frac{1}{2}k - 1. \end{aligned}$$

□

5 | PROOF OF THEOREM 1

In this final section, we zoom out for the general case and prove Theorem 1 by considering the order of H and assembling results from previous sections.

Recall that G is S_n or A_n $(n \geqslant 7)$ and $H \neq \mathrm{A}_n$ is a primitive maximal subgroup of G. Maróti proved in [12] several useful upper bounds on the order of a primitive subgroup of the symmetric group.

Lemma 5.1.

(i) $|H| < 50n^{\sqrt{n}}$.

(ii) *At least one of the following holds:*

(a) $H = S_m \cap G$ *acting on* r*-subsets of* $\{1, \dots, m\}$ *with* $n = \binom{m}{r}$ *for some integers* m, r *with* $m > 2r \geqslant 4$*;*

(b) $H = (\mathrm{S}_m \wr \mathrm{S}_k) \cap G$ *with* $n = m^k$ *for some* $m \geqslant 5$ *and* $k \geqslant 2$*;*

(c) $|H| < n^{1+\lfloor \log n \rfloor}$*; and*

(d) H *is one of the Mathieu groups* $M_{11}, M_{12}, M_{23}, M_{24}$ *acting 4-transitively.*

Proof. Part (i) follows immediately from [12, Corollary 1.1]. Part (ii) follows from [12, Theorem 1.1] and the description of the maximal subgroups of S_n and A_n in [11]. □

Equipped with these results as well as Theorems 5 and 6, we are ready to prove Theorem 1.

Proof of Theorem 1. If H is as in case (a) of Lemma 5.1(ii), then $n = \binom{m}{r} \geqslant \binom{m}{2} = \frac{m(m-1)}{2}$. Hence $m < 2\sqrt{n}$ and, by (2),

$$\mathrm{I}(G, H) \leqslant 1 + \ell(H) \leqslant 1 + \ell(S_m) < 3\sqrt{n} - 1.$$

If H is as in case (b) of Lemma 5.1(ii), then $n = m^k$. By Theorem 6, $\mathrm{I}(G, H) \leqslant \frac{3}{2}mk - \frac{1}{2}k - 1$. If $k = 2$, then

$$\mathrm{I}(G, H) \leqslant 3m - 2 < 3\sqrt{n} - 1.$$

If $k \geqslant 3$, then

$$\mathrm{I}(G, H) < \frac{3}{2}m\frac{\log n}{\log m} \leqslant \frac{3}{2}\sqrt[3]{n}\frac{\log n}{\log 5} < 3\sqrt{n} - 1.$$

If H is as in case (c) of Lemma 5.1(ii), then

$$\mathrm{I}(G, H) \leqslant 1 + \ell(H) \leqslant 1 + \log|H| < 1 + \log\left(n^{1+\log n}\right) = (\log n)^2 + \log n + 1.$$

Using the lists of maximal subgroups in [6], one can check that $\ell(M_{11}) = 7$, $\ell(M_{12}) = 8$, $\ell(M_{23}) = 11$, and $\ell(M_{24}) = 14$. It is thus easy to verify that $\mathrm{I}(G, H) \leqslant 1 + \ell(H) < (\log n)^2$ in case (d) of Lemma 5.1(ii). Therefore, part (i) of the theorem holds.

We now prove parts (ii) and (iii). By Theorem 3.1, if $n = 3^d$ for some integer $d \geqslant 2$, then $H = \mathrm{AGL}_d(3) \cap G$ is a maximal subgroup of G. Theorem 5 now gives

$$\mathrm{I}(G, H) > \frac{d^2}{2} + \frac{d}{2} = \frac{(\log n)^2}{2(\log 3)^2} + \frac{\log n}{2\log 3},$$

as required.

By Theorem 4.1, if $n = m^2$ for some odd integer $m \geqslant 5$, then $H = (\mathrm{S}_m \wr \mathrm{S}_2) \cap G$ is a maximal subgroup of G. Theorem 6 now gives $\mathrm{I}(G, H) \geqslant m = \sqrt{n}$, as required. □

Finally, we prove an additional lemma.

Lemma 5.2. *Let t be the index of H in G. There exist constants $c_5, c_6, c_7, c_8 \in \mathbb{R}_{>0}$ such that*

(i) $c_5 \log t / \log\log t < n < c_6 \log t / \log\log t$; *and*
(ii) $c_7 \log\log t < \log n < c_8 \log\log t$.

Proof. It suffices to prove that such constants exist for n sufficiently large, so we may assume $n > 100$. We first note that $\log t < \log |G| \leqslant n \log n$, from which we obtain

$$\log\log t < \log n + \log\log n < \log n + (\log n)\frac{\log\log 100}{\log 100} < 1.412 \log n.$$

Hence we may take $c_7 = 1/1.412 > 0.708$ for $n > 100$. By Lemma 5.1(i),

$$\begin{aligned}\log t = \log |G : H| &= \log |G| - \log |H| > \log \frac{n!}{2} - \log\left(50 n^{\sqrt{n}}\right)\\ &> (n \log n - n \log e - 1) - \left(\sqrt{n}\log n + \log 50\right) = n\log n - n \log e - \sqrt{n}\log n - \log 100\\ &> n \log n - n(\log e)\frac{\log n}{\log 100} - \sqrt{n}(\log n)\frac{\sqrt{n}}{\sqrt{100}} - (\log 100)\frac{n \log n}{100 \log 100}\\ &> 0.672\, n \log n,\end{aligned}$$

where the second inequality follows from Stirling's approximation and the last inequality follows from the fact that $\log e / \log 100 < 0.218$. We deduce further that $\log\log t > \log n$ and hence take $c_8 = 1$ for $n > 100$.

Finally, $\log t / \log\log t < n \log n / \log n = n$ and $\log t / \log\log t > 0.672\, n \log n / 1.412 \log n = 0.672\, n / 1.412$. Therefore, for $n > 100$, we may take $c_5 = 1$, $c_6 = 1.412/0.672 < 2.11$. □

Corollary 2 now follows by combining Theorem 1 and Lemma 5.2.

Remark 5.3. Verifying all cases with $7 \leqslant n \leqslant 100$ by enumerating primitive maximal subgroups of S_n and A_n in Magma [2], we may take $c_5 = 1$, $c_6 = 4.03$, $c_7 = 0.70$, and $c_8 = 1.53$ in the statement of Lemma 5.2. With these values of the constants and those in the proof of Lemma 5.2, it is straightforward to obtain the values of the constants c_2, c_3, c_4 given in Remark 3. For the values of c_1, we use in addition the fact that, for any n_0, if $n \geqslant n_0$, then $(\log n)^2 + (\log n) + 1 = (\log n)^2\left(1 + 1/\log n + 1/(\log n)^2\right) < c_8^2\left(1 + 1/\log n_0 + 1/(\log n_0)^2\right)(\log\log t)^2$.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous referees for their careful reading and helpful comments. The authors would like to thank the Isaac Newton Institute for Mathematical Sciences for its support and hospitality during the programme *Groups, representations and applications: new perspectives*, when work on this article was undertaken. This work was supported by EPSRC grant no. EP/R014604/1, and also partially supported by a grant from the Simons Foundation. For the purpose of open access, the authors have applied a Creative Commons attribution (CC BY) licence to any Author Accepted Manuscript version arising.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

ORCID

Colva M. Roney-Dougal https://orcid.org/0000-0002-0532-3349
Peiran Wu https://orcid.org/0009-0005-9506-3235

REFERENCES

1. M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Algebra **92** (1985), no. 1, 44–80.
2. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.
3. T. C. Burness, R. M. Guralnick, and J. Saxl, *On base sizes for symmetric groups*, Bull. Lond. Math. Soc. **43** (2011), no. 2, 386–391.
4. P. J. Cameron, R. Solomon, and A. Turull, *Chains of subgroups in symmetric groups*, J. Algebra **127** (1989), no. 2, 340–352.
5. G. L. Cherlin, G. A. Martin, and D. H. Saracino, *Arities of permutation groups: wreath products and k-sets*, J. Comb. Theory Ser. A **74** (1996), no. 2, 249–286.
6. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An atlas of finite groups*, Oxford University Press, Oxford, 1985.
7. N. Gill and M. W. Liebeck, *Irredundant bases for finite groups of Lie type*, Pac. J. Math. **322** (2023), no. 2, 281–300.
8. N. Gill and B. Lodà, *Statistics for S_n acting on k-sets*, J. Algebra **607** (2022), 286–299.
9. N. Gill, B. Lodà, and P. Spiga, *On the height and relational complexity of a finite permutation group*, Nagoya Math. J. **246** (2022), 372–411.
10. V. Kelsey and C. M. Roney-Dougal, *On relational complexity and base size of finite primitive groups*, Pac. J. Math. **318** (2022), no. 1, 89–108.
11. M. W. Liebeck, C. E. Praeger, and J. Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra **111** (1987), no. 2, 365–383.
12. A. Maróti, *On the orders of primitive groups*, J. Algebra **258** (2002), no. 2, 631–640.