Permutation Representations of Group Quotients and of Quasisimple Groups

Robert Chamberlain

A thesis submitted for the degree of
Doctor of Philosophy in Mathematics

University of Warwick, Department of Mathematics

April 2020

Contents

Declarations

This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy. It has been composed by myself and has not been submitted in any previous application for any degree.

The work presented was carried out by the author.

Parts of this thesis have been published by the author:

Robert Chamberlain. Subgroups with no abelian composition factors are not distinguished. *Bull. Aust. Math. Soc.*, 101(3):446–452, 2020

Robert Chamberlain. Minimal exceptional p-groups. *Bulletin of the Australian Mathematical Society*, 98(3):434–438, 2018

Summary

The *minimal degree*, $\mu(G)$, of a finite group G is the least n such that G embeds in S_n. Such embeddings, called *permutation representations*, are often used to represent groups on computers. Algorithms working with such representations have time and space complexity depending on n so it is often worth putting some time into getting n as close to $\mu(G)$ as possible.

In the second chapter of this thesis we study group quotients. Despite a quotient G/N of G being smaller and in some sense simpler than G it possible to have $\mu(G/N) > \mu(G)$, in which case G is called *exceptional* and N is called *distinguished* in G. We characterise exceptional p-groups of least order and show that normal subgroups with no abelian chief factors are not distinguished. These develop from work by Kovács, Easdown and Praeger.

In the third chapter we study quasisimple groups. The most significant result in the third chapter is the calculation of $\mu(2 \cdot A_n)$ for all n. This is in some sense the worst case for the minimal degree of a quasisimple group as $\mu(2 \cdot A_n)$ grows with $\left(\frac{n}{2}\right)!$. A representation of degree $\mu(2 \cdot A_n)$ is first given, then the proof that it is minimal comes in two parts. We describe a dynamic programming algorithm for computing $\mu(2 \cdot A_n)$ for small n. This is done for $n \leq 850$. For $n > 850$ we use an inductive proof to compute $\mu(2 \cdot A_n)$.

We also compute $\mu(\mathrm{SL}(n, q))$ following work by Cooperstein and conclude with comments on the minimal degrees of other classical groups and of Schur covers of some sporadic simple groups.

Chapter 1

Introduction

In this thesis we study the following question:

Given a finite group G, what is the smallest n such that G embeds into S_n?

This question is of particular importance in computational group theory. Permutations are easily represented on a computer and there many group theoretic algorithms which work with permutation groups (subgroups of S_n). It is therefore useful when working with a finite group G to embed G into some S_n.

The vast majority (perhaps all) of algorithms that work with subgroups of S_n have time and space complexities which depend on n. It is therefore worthwhile spending some time to reduce this n.

1.1 Definitions and Conventions

Definition 1.1.1 (Permutation Representation)
Given a finite group G, a (permutation) representation *of G is a group homomorphism*

$$\rho : G \to S_n \cong \mathrm{Sym}(\Omega)$$

for some set Ω of size n. This is equivalent to an action of G on Ω.

Definition 1.1.2 (Minimal Permutation Representation)
We call ρ minimal *if $\ker(\rho) = 1$ and n is as small as possible. We denote such n by $\mu(G)$ and call $\mu(G)$ the* minimal degree *of G.*

Note that the main question we are investigating is precisely:

Given a finite group G, what is $\mu(G)$?

We list here some notation and conventions for the readers reference. These conventions will be consistent throughout the thesis.

- All groups are assumed to be finite.
- $[n] = \{1, \ldots, n\}$.
- ν_p denotes p-adic valuation. That is $k = \nu_p(n)$ if $p^k \mid n$ and $p^{k+1} \nmid n$.
- $G/H = \{Hg | g \in G\}$.
- For $g \in G$ and $H \leq G$, $H^g = g^{-1}Hg$.
- If $H \leq G$ then $\mathrm{core}_G(H)$ denotes the largest normal subgroup of G contained in H.
- Permutations act on the right.
- Where unambiguous, $G^\Omega = \rho(G)$.
- Where unambiguous, properties of ρ and properties of G^Ω are considered interchangeable. For example we say ρ is transitive if G^Ω is transitive.
- When ρ is implicit, for brevity we denote $x^g = x^{\rho(g)}$ for $g \in G$, $x \in \Omega$.
- For $\alpha \in \Omega$, $G_\alpha = \{g \in G | \alpha^g = \alpha\}$.
- For $\alpha \in \Omega$, $\alpha^G = \{\alpha^g | g \in G\}$.
- For $\Delta \subseteq \Omega$ and $g \in G$, $\Delta^g = \{x^g | x \in \Delta\}$.
- For $\Delta \subseteq \Omega$, $G_\Delta = \{g \in G | \Delta^g = \Delta\}$.
- For $\Delta \subseteq \Omega$, $G_{(\Delta)} = \cap_{x \in \Delta} G_x$.
- If $\Delta^G = \Delta$ then G^Δ denotes the restricted action of G on Δ.
- We call $\Delta \subseteq \Omega$ a block for G^Ω if for all $g \in G$ we have either $\Delta^g = \Delta$ or $\Delta \cap \Delta^g = \emptyset$.
- If $\Delta \subseteq \Omega$ forms a block for G^Ω then $\mathcal{B}_\Delta = \{\Delta^g | g \in G\}$ denotes the block system containing Δ.
- If $\Delta \subseteq \Omega$ forms a block for G^Ω then $G^{\mathcal{B}_\Delta}$ denotes the natural action of G on $\mathcal{B}_\Delta$.

Proposition 1.1.1
$\mathrm{core}_G(H) = \cap_{g \in G} H^g$

Proof: Notice that $\mathrm{core}_G(H) = \mathrm{core}_G(H)^g \leq H^g$ for all $g \in G$. This gives $\mathrm{core}_G(H) \leq \cap_{g \in G} H^g$.

Conversely, let $L = \cap_{g \in G} H^g \leq H$. For $x \in G$ the map $g \mapsto gx$ permutes the elements of G. So $L^x = \cap_{g \in G} H^{gx} = \cap_{g \in G} H^g = L$.

Hence $\mathrm{core}_G(H) \geq \cap_{g \in G} H^g$. $\square$

Definition 1.1.3
Two representations $\rho : G \to \mathrm{Sym}(\Omega)$, $\sigma : G \to \mathrm{Sym}(\Delta)$ are equivalent *if there exists a bijection $\pi : \Omega \to \Delta$ such that for all $g \in G$ and $x \in \Omega$ we have $\pi(x)^{\sigma(g)} = \pi(x^{\rho(g)})$.*

Intuitively ρ and σ are equivalent if we can obtain σ from ρ by relabelling Ω. For the next definition, we need a small result.

Proposition 1.1.2
Let $\Omega_1, \ldots, \Omega_k$ be the orbits of G^Ω. Fix a point $\alpha_i \in \Omega_i$ in each orbit and denote $H_i = G_{\alpha_i}$. Then G^Ω is equivalent to the action of G on $\sqcup_{i=1}^k G/H_i$ by right multiplication.

Proof: We define $\pi : \Omega \to \sqcup_{i=1}^k G/H_i$ by $\pi(\alpha_i^g) = H_i g$ for $i \in [k]$, $g \in G$.

To see π is well defined, suppose $\alpha_i^{g_1} = \alpha_i^{g_2}$. Then $g_1 g_2^{-1} \in H_i$, so $H_i g_1 = H_i g_2$ as required.

To see π is injective, suppose $\pi(\alpha_i^{g_1}) = \pi(\alpha_i^{g_2})$. Then $H_i g_1 = H_i g_2$, so $g_1 g_2^{-1} \in H_i$ and therefore $\alpha_i^{g_1} = \alpha_i^{g_2}$. Clearly π is surjective.

To see π is an equivalence, $\pi(\alpha_i^{g_1}) g_2 = H_i g_1 g_2 = \pi((\alpha_i^{g_1})^{g_2})$. This completes the proof. $\square$

Definition 1.1.4 (Subgroup Correspondence)
Using the notation in Proposition 1.1.2 we say ρ (equivalently G^Ω) corresponds to $\{H_1, \ldots, H_k\}$ and call $\{H_1, \ldots, H_k\}$ the subgroup correspondence *of ρ.*

Note that the subgroup correspondence is in fact a multiset and that the choices for H_i are unique up to conjugacy, justifying the term 'the subgroup correspondence'.

1.2 Basic Results

We list in this section useful or interesting results which are very easy to prove and may be used later without reference.

Proposition 1.2.1 (Immediate Results)
We begin with some immediate results

1. $|G| \leq \mu(G)!$.
2. $\mu(G) \leq |G|$.
3. *If* $H \leq G$ *then* $\mu(H) \leq \mu(G)$.
4. $\mu(G \times H) \leq \mu(G) + \mu(H)$.

Proof:

1. This follows immediately from the fact G embeds into $S_{\mu(G)}$.
2. This is Cayley's Theorem - G acts faithfully on itself.
3. We know there exists an embedding $\rho : G \to S_{\mu(G)}$. Restricting this to H gives embedding $\rho|_H : H \to S_{\mu(G)}$.
4. Let $n = \mu(G)$ and $m = \mu(H)$ so there are embeddings $G \hookrightarrow S_n$ and $H \hookrightarrow S_m$. There is a natural embedding $S_n \times S_m \hookrightarrow S_{n+m}$, so we may embed $G \times H \hookrightarrow S_n \times S_m \hookrightarrow S_{n+m}$.

□

Proposition 1.2.2 (Properties of Representations)
The following table defines properties of a permutation representation $\rho : G \to \mathrm{Sym}(\Omega)$ *and the corresponding properties of the subgroup correspondence for* ρ. *We prove in each case that the two properties are equivalent.*

	ρ	$\{H_1, \ldots, H_k\}$
degree	n	$\sum_{i=1}^{k}[G : H_i]$
faithful	$\ker(\rho) = 1$	$\cap_{i=1}^{k}\mathrm{core}_G(H_i) = \mathrm{core}_G(\cap_{i=1}^{k} H_i) = 1$
no. orbits		k
primitive	*transitive* *no non-trivial block*	$k = 1$ H_1 *maximal*
regular	*transitive* *trivial point stabiliser*	$k = 1$ $H_1 = 1$

Proof:
Degree, **no. orbits** and **regular** follow from the subgroup correspondence (Proposition 1.1.2). Since the above properties are preserved under equivalence we may assume $\Omega = \sqcup_{i=1}^{k} G/H_i$.

Faithful:

First notice that

$$\cap_{i=1}^{k}\mathrm{core}_G(H_i) = \cap_{i=1}^{k} \cap_{g\in G} H_i^g = \cap_{g\in G}(\cap_{i=1}^{k} H_i)^g = \mathrm{core}_G(\cap_{i=1}^{k} H_i)$$

We actually prove the stronger result that $\ker(\rho) = \cap_{i=1}^{k}\mathrm{core}_G(H_i)$.

Now, suppose $x \in \ker(\rho)$. Then $H_i gx = H_i g$ for each $i \in [k]$ and $g \in G$. For fixed i, g, this implies $x \in H_i^g$, so $x \in \cap_i \cap_{g\in G} H_i^g = \cap_{i=1}^{k}\mathrm{core}_G(H_i)$. Hence $\ker(\rho) \leq \cap_{i=1}^{k}\mathrm{core}_G(H_i)$.

Conversely, suppose $x \in \cap_{i=1}^{k}\mathrm{core}_G(H_i)$. In particular, for each $i \in [k]$ and $g \in G$ we have $x \in H_i^g$ so $H_i gx = H_i g$. Hence $x \in \ker(\rho)$.

Primitive:

It is a straightforward check that if ρ is imprimitive then the subgroup K fixing a non-trivial block of G^Ω satisfies $H_1 < K < G$. Conversely if $H_1 < L < G$ then it is a straightforward check that $H_1 L = \{H_1 g | g \in L\}$ forms a non-trivial block in Ω. □

Proposition 1.2.3
Suppose $\mathrm{Soc}(G) = N_1 \times \cdots \times N_k$ *where* N_i *is a minimal normal subgroup of* G *for each* i*. Then a minimal representation of* G *has at most* k *orbits.*

Proof: Suppose $\{H_1, \ldots, H_r\}$ corresponds to a minimal representation of G with $r > k$. Let $K_i = \mathrm{core}_G(H_i)$, so $\cap_{i=1}^{r} K_i = 1$. Let $C_i = \cap_{j\neq i} K_j \cap \mathrm{Soc}(G)$ so $K_i \cap C_i = 1$.

If $C_i = 1$ then $\{H_j | j \neq i\}$ corresponds to a faithful representation of degree smaller than $\{H_1, \ldots, H_r\}$ contrary to assumption. Hence C_i is non-trivial for each i.

Let $P_i = C_1 C_2 \cdots C_i$. If $P_i = P_{i+1}$ for some i then $C_{i+1} \leq C_1 C_2 \cdots C_i$. But $C_1, \ldots, C_i \leq K_{i+1}$ so $C_{i+1} \leq K_{i+1}$. With $C_{i+1} \cap K_{i+1} = 1$ this implies $C_{i+1} = 1$ which is false. Hence $P_i < P_{i+1} \leq \mathrm{Soc}(G)$. This gives an increasing sequence $P_1 < P_2 < \cdots < P_r$ of normal subgroups of G contained in $\mathrm{Soc}(G)$ with $r > k$. This is impossible so we must have $r \leq k$. □

Corollary 1.2.4
If G has simple socle then any minimal representation of G corresponds to $\{H\}$ where H is a core-free ($\mathrm{core}_G(H) = 1$) subgroup of G maximal order.

Proof: By the above proposition any minimal representation of G must be transitive so must correspond to $\{H\}$ for some core-free H. If H is not of maximal order then there is some core-free K such that $[G : K] < [G : H]$. In particular $\{H\}$ does not correspond to a minimal representation. Hence H is of largest order. □

1.3 A Brief Review

This area of study splits naturally into the study of group quotients and group extensions. We study group quotients as when working with a group G it is often helpful to do some work in a quotient G/N of G. We study group extensions in the hope that we may compute $\mu(G)$ by describing G as a group extension. In the case G is simple, $\mu(G)$ is known, which we discuss later in this section.

We will therefore review results which concern group quotients and group extensions in their respective chapters. In this section we discuss the remaining miscellaneous results.

1.3.1 Simple Groups

We begin with possibly the most important result of this section, the minimal degrees of all simple groups. The following table, compiled from [10] and [6], gives the minimal degrees of all finite simple groups. We then give two results which are shown by a systemic check of the table.

Group	Conditions	Minimal Degree
C_p	p prime	p
A_n	$n \geq 5$	n
$\mathrm{PSL}_n(q)$	$(n,q) \notin \{(2,5),(2,7),(2,9),(2,11),(4,2)\}$	$\frac{q^n-1}{q-1}$
$\mathrm{PSL}_2(5)$		5
$\mathrm{PSL}_2(7)$		7
$\mathrm{PSL}_2(9)$		6
$\mathrm{PSL}_2(11)$		11
$\mathrm{PSL}_4(2)$		8
$\mathrm{PSp}_{2m}(q)$	$m \geq 2$, $q > 2$, $(m,q) \neq (2,3)$	$\frac{q^{2m}-1}{q-1}$
$\mathrm{PSp}_{2m}(2)$	$m \geq 3$	$2^{m-1}(2^m-1)$
$\mathrm{PSp}_4(3)$		27
$\mathrm{P\Omega}_{2m+1}(q)$	$m \geq 3$, $q \geq 5$	$\frac{q^{2m}-1}{q-1}$
$\mathrm{P\Omega}_{2m+1}(3)$	$m \geq 3$	$\frac{3^{m-1}(3^m-1)}{2}$
$\mathrm{P\Omega}^+_{2m}(q)$	$m \geq 4$, $q \geq 4$	$\frac{(q^m-1)(q^{m-1}+1)}{q-1}$
$\mathrm{P\Omega}^+_{2m}(3)$	$m \geq 4$	$\frac{3^{m-1}(3^m-1)}{2}$
$\mathrm{P\Omega}^+_{2m}(2)$	$m \geq 4$	$2^{m-1}(2^m-1)$
$\mathrm{P\Omega}^-_{2m}(q)$	$m \geq 4$	$\frac{(q^m+1)(q^{m-1}-1)}{q-1}$
$\mathrm{PSU}_3(q)$	$q \neq 5$	q^3+1
$\mathrm{PSU}_3(5)$		50
$\mathrm{PSU}_4(q)$		$(q+1)(q^3+1)$
$\mathrm{PSU}_n(q)$	either $n \geq 5$ odd or n even and $q \neq 2$	$\frac{(q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})}{q^2-1}$
$\mathrm{PSU}_{2m}(2)$	$m \geq 3$	$\frac{2^{2m-1}(2^{2m}-1)}{3}$
$G_2(q)$	$q > 4$	$\frac{q^6-1}{q-1}$
$G_2(3)$		351
$G_2(4)$		416
$F_4(q)$		$\frac{(q^{12}-1)(q^4+1)}{q-1}$
$E_6(q)$		$\frac{(q^9-1)(q^8+q^4+1)}{q-1}$
$E_7(q)$		$\frac{(q^{14}-1)(q^9+1)(q^5+1)}{q-1}$
$E_8(q)$		$\frac{(q^{30}-1)(q^{12}+1)(q^{10}+1)(q^6+1)}{q-1}$
${}^2B_2(q)$	$q = 2^f$, f odd	q^2+1
${}^2G_2(q)$	$q = 3^f$, f odd	q^3+1
${}^3D_4(q)$		$(q^8+q^4+1)(q+1)$
${}^2E_6(q)$		$\frac{(q^{12}-1)(q^6-q^3+1)(q^4+1)}{q-1}$
${}^2F_4(q)$	$q = 2^f$, $q \neq 2$	$(q^6+1)(q^3+1)(q+1)$
${}^2F_4(2)'$		1600

Group	Conditions	Minimal Degree
M_{11}		11
M_{12}		12
M_{22}		22
M_{23}		23
M_{24}		24
HS		100
J_2		100
Co_1		98280
Co_2		2300
Co_3		276
McL		275
Suz		1782
He		2058
HN		1140000
Th		143127000
Fi_{22}		3510
Fi_{23}		31671
Fi'_{24}		306936
B		13571955000
M		97239461142009186000
J_1		266
$O'N$		122760
J_3		6156
Ru		4060
J_4		173067389
Ly		8835156

Proposition 1.3.1
If S is a simple group then $|\mathrm{Out}(S)| \leq \mu(S)$.

Proof: This is a systematic check, where throughout we assume p is prime:
For a cyclic simple group $S = C_p$ we have $|\mathrm{Out}(S)| = p - 1 < p = \mu(S)$.

For $S = A_n$ with $n \geq 5$, if $n \neq 6$ then $|\mathrm{Out}(S)| = 2 < n = \mu(S)$ and if $n = 6$ then $|\mathrm{Out}(S)| = 4 < 6 = \mu(S)$.

For $S = \mathrm{PSL}_2(q)$, $S = \mathrm{PSp}_{2m}(q)$ or $S = \mathrm{P}\Omega_{2m+1}(q)$ with $q = p^f$ with p prime we have $|\mathrm{Out}(S)| \leq 2f < \mu(S)$.

For $S = \mathrm{PSL}_n(q)$ and $n > 2$, $q = p^f$ where p is a prime we have that $|\mathrm{Out}(S)| = 2f \gcd(n, q-1) < \mu(S)$.

For $S = \mathrm{P}\Omega^+_{2m}(q)$ and $q = p^f > 2$ we have $|\mathrm{Out}(S)| \leq 24f < \mu(S)$.

For $S = \mathrm{P}\Omega^+_{2m}(2)$ we have $|\mathrm{Out}(S)| \leq 6 < \mu(S)$.

For $S = \mathrm{P}\Omega^-_{2m}(q)$ and $q = p^f$ we have $|\mathrm{Out}(S)| \leq 4f < \mu(S)$.

For $S = \mathrm{PSU}_n(q)$ and $q^2 = p^f$ we have $|\mathrm{Out}(S)| = f \gcd(n+1, q+1) < \mu(S)$.

If S is one of the remaining simple groups of Lie type then, with $q = p^f$, we have $|\mathrm{Out}(S)| \leq 6f < \mu(S)$.

For a sporadic simple group S we have $|\mathrm{Out}(S)| \leq 2 < \mu(S)$. □

Proposition 1.3.2
If S is a non-abelian simple group then $\mu(\mathrm{Aut}(S)) \leq \frac{28}{9}\mu(S)$.

Proof: This is given as a corollary of Proposition 2.2 in [3]. □

1.3.2 Meet-Irreducible Groups

Definition 1.3.1 (meet-irreducible)
A subgroup H of G is called meet-irreducible *in G if for any $K_1, K_2 \leq G$ we have*

$$H = K_1 \cap K_2 \Rightarrow H = K_1 \text{ or } H = K_2$$

Meet-irreducible subgroups were first used in the study of minimal degrees by Johnson [16] (who confusingly called such subgroups primitive). Proofs in this section follow those by Johnson with minor changes to notation. The interest in meet-irreducible subgroups comes from the following Lemma.

Lemma 1.3.3
Suppose $R = \{H_1, \ldots, H_k\}$ is a faithful permutation representation of a finite group G. If $H_i = K_1 \cap K_2$ for some $i \in [k]$ and $H_i < K_j \leq G$ for $j \in \{1, 2\}$ then R^+ is a faithful representation of G where

$$R^+ = \{H_1 \ldots H_{i-1}, K_1, K_2, H_{i+1} \ldots H_k\}$$

and $\deg(R^+) \leq \deg(R)$.

Proof: Immediately R^+ is faithful as

$$1 = \mathrm{core}_G(\cap_{j=1}^k H_j) = \mathrm{core}_G(\cap_{j \neq i} H_j \cap K_1 \cap K_2)$$

For the degree

$$\begin{aligned}
\deg(R) - \deg(R^+) &= [G : H_i] - [G : K_1] - [G : K_2] \\
&= [G : H_i]\left(1 - \tfrac{1}{[K_1 : H]} - \tfrac{1}{[K_2 : H]}\right) \\
&\geq [G : H_i]\left(1 - \tfrac{1}{2} - \tfrac{1}{2}\right) = 0
\end{aligned}$$

□

Corollary 1.3.4
Given a finite group G and suppose $R = \{H_1, \ldots, H_k\}$ is minimal representation of G with k maximal. Then each H_i is meet-irreducible in G.

Proof: Suppose H_i is not meet-irreducible for some i. Then there are some $K_1, K_2 \leq G$ with $H_i < K_j$ for each j and $H_i = K_1 \cap K_2$. By Lemma 1.3.3 we have a faithful representation R^+ of G with $k+1$ orbits and $\deg(R^+) \leq \deg(R)$. As R is minimal, so is R^+, contradicting the assumption that k is maximal. □

It is worth noting that, as subgroups containing H_i correspond to blocks in the orbit defined by H_i, we can rephrase the results of this section as follows:

- Fix a finite group G, $H < G$ a faithful representation G^Ω of G and an orbit $\Delta \subseteq \Omega$ of G.
- H is meet-irreducible if and only if $H < \cap_{H < K \leq G} K$.
- If Δ_1, Δ_2 are distinct non-trivial blocks of G^Δ with $\Delta_1 \cap \Delta_2$ a singleton, then the induced action of G on $\Omega' = (\Omega \setminus \Delta) \cup \mathcal{B}_{\Delta_1} \cup \mathcal{B}_{\Delta_2}$ is faithful and $|\Omega'| \leq |\Omega|$.
- G has a minimal representation such that the action of G on each orbit is either primitive or contains a unique minimal block.

1.3.3 Compression Ratio

Definition 1.3.2
The compression ratio *of a finite group G is* $\mathrm{cr}(G) = \frac{|G|}{\mu(G)}$.

The notion of the compression ratio was suggested by Becker [2]. It can be thought of as a measure of how 'easy' a group is to represent as a permutation representation and acts as convenient notation. For example an important result by Johnson is the classification of finite groups with $\mathrm{cr}(G) = 1$ [16] which we give below with a lower bound on $\mathrm{cr}(G)$ for G with $\mathrm{cr}(G) \neq 1$ as proven by Becker in [2].

Theorem 1.3.5
Let G be a finite group. Then $\mathrm{cr}(G) = 1$ if and only if G is one of the following:

1. *Cyclic group of prime power order.*
2. *Generalised quaternion group of order 2^n $(n \geq 3)$.*
3. *The Klein-4 group.*

Furthermore if $\mathrm{cr}(G) \neq 1$ then $\mathrm{cr}(G) \geq 1.2$ and if $|G|$ is odd then $\mathrm{cr}(G) \geq 1.5$.

Notably the two lower bounds on $\mathrm{cr}(G)$ are obtained by $G = C_6$ and $G = C_3 \times C_3$ respectively.

1.4 Summary

Here we summarise the major results of this thesis.

1.4.1 Summary of Chapter 2

The results of chapter 2 concern group quotients and are published in [4, 5]. Given a finite group G and a normal subgroup N of G we call G exceptional and N distinguished in G if $\mu(G) < \mu(G/N)$.

In [9] Easdown and Praeger show that the least power 2^k of 2 such that there exists an exceptional group G with $|G| = 2^k$ is 2^5. They also note that for an arbitrary prime p there are no exceptional groups of order p^3 and there is always an exceptional group of order p^6. They then raise the question of whether there are exceptional groups of order p^4 or p^5 for odd primes. We answer this as follows:

Theorem 1.4.1
Let p be an odd prime. Then there are no exceptional groups of order p^4.

Theorem 1.4.2
Let p be prime and

$$G = \langle g, h | g^{p^2} = h^{p^2} = [g,h]^p = 1 \ , \ [[g,h],g] = [[g,h],h] = g^p \rangle$$

$$N = \langle g^p h^p \rangle$$

Then

$$G \cong (C_{p^2} \rtimes C_p) \rtimes C_{p^2}$$

$$\mu(G) \leq 2p^2$$

$$\mu(G/N) = p^3$$

Corollary 1.4.3
Let p be an odd prime and G, N be defined as in Theorem 1.4.2. Then G is exceptional with distinguished subgroup N.

In [18] it is shown that if G/N has no abelian normal subgroup then N is not distinguished. We prove a dual result:

Theorem 1.4.4
Let G be a finite group with N a normal subgroup of G. If N has no abelian chief factors then N is not distinguished in G.

1.4.2 Summary of Chapter 3

The results of chapter 3 concern quasisimple groups. A group G is quasisimple if it is perfect and $G/Z(G)$ is simple. Quasisimple groups can also be defined as the non-trivial quotients of Schur covers of nonabelian simple groups.

We begin by studying the minimal degree of the two cover $2 \cdot A_n$ of the alternating group A_n. This is done both algorithmically, computing $\mu(2 \cdot A_n)$ explicitly for $n \leq 850$, then theoretically to compute $\mu(2 \cdot A_n)$ for all n. The following table shows $\mu(2 \cdot A_n)$ for $n \geq 5$.

n	$\mu(2 \cdot A_n)$	core-free subgroup
5	24	5
6	80	3^2
7	240	7.3
8	240	$\mathrm{PSL}(2,7)$
9	240	$\mathrm{PSL}(2,8).3$
10	2400	$\mathrm{PSL}(2,8).3$
11	5040	M_{11}
12	60480	M_{11}
13	786240	M_{11}
14	3669120	$M_{11} \times 3$
15	55036800	$M_{11} \times 3$
16	370656000	$\mathrm{PSL}(2,7)^2.2$
17	1400256000	$\mathrm{PSL}(2,7) \times \mathrm{PSL}(2,8).3$
18	2800512000	$(\mathrm{PSL}(2,8).3)^2$
19	53209728000	$(\mathrm{PSL}(2,8).3)^2$
20	203164416000	$M_{11} \times \mathrm{PSL}(2,8).3$
21	4266452736000	$M_{11} \times \mathrm{PSL}(2,8).3$
22	17919101491200	M_{11}^2
23	412139334297600	M_{11}^2
24	1295295050649600	$A_{12} \times 2$
25	32382376266240000	$A_{12} \times 2$
26	129529505064960000	A_{13}
27	1050040772352000000	$(\mathrm{PSL}(2,8).3) \wr 3$
≥ 28, $\equiv 0,1 \bmod 8$	${}^{n!}/_{\lfloor \frac{n}{2} \rfloor !}$	$A_{\lfloor \frac{n}{2} \rfloor}$
≥ 28, $\not\equiv 0,1 \bmod 8$	${}^{2(n!)}/_{\lfloor \frac{n}{2} \rfloor !}$	$A_{\lfloor \frac{n}{2} \rfloor} \times 2$

We then go on study the Schur covers of classical groups. The computation of $\mu(G)$ when G is the Schur cover of an arbitrary classical simple group is beyond the scope of this thesis. However the author suspects that with enough time they could all be computed by carefully adapting the computation of minimal degrees of classical simple groups in [7, 20]. This is done in the case $G = \mathrm{SL}_n(q)$ as shown in the table below.

We fix the primes $p_1, \dots, p_{k_0}$ dividing $|Z(H)|$ and for each i fix e_i such that $q-1 = p_i^{e_i} t_i$ with $p_i \nmid t_i$. Note that H_i are defined in chapter 3, but are difficult to define succinctly so we omit the definition of H_i here.

(n,q)	$\mu(SL_n(q))$	Representation
$(2,2)$	3	$\{C_2\}$
$(2,3)$	8	$\{C_3\}$
$(2,5)$	24	$\{C_5\}$
$(2,9)$	80	$\{C_3 \times C_3\}$
$(4,2)$	8	A_6
(n,q) not above, $k_0 = 0$	$\frac{q^n-1}{q-1}$	Stabiliser of point in action on $\mathrm{PG}(n-1,q)$
(n,q) not above, $k_0 > 0$	$\frac{q^n-1}{q-1}\sum_{i\in[k_0]} p_i^{e_i}$	$\{H_i \mid i \in [k_0]\}$

Finally we study the schur covers of sporadic simple groups. These are included just for completeness and the computation uses a relatively naive algorithm to obtain minimal degrees. However where maximal subgroups of a sporadic simple group S are available on MAGMA we can compute the minimal degree of the Schur cover G of that simple group. These are given in the table below - note that we include S if and only if $S \neq G$ and leave blank the minimal degrees where maximal subgroups of S are not available in MAGMA.

S	Schur Multiplier	$\mu(G)$	Representation
M_{12}	C_2	24	$\{M_{11}\}$
M_{22}	C_{12}	5622	$\{3 \cdot A_6, ((C_4 : C_8) : A_5) : C_2\}$
J_2	C_2	200	$\{U_3(3)\}$
J_3	C_3	18468	$\{\mathrm{PSL}_2(16) : 2\}$
Co_1	C_2	196560	$\{Co_2\}$
Fi_{22}	C_6	213488	$\{C_3 \times O_7(3), (C_2 \times O_8^+(2)) : 6\}$
Fi'_{24}	C_3	920808	$\{Fi_{23}\}$
HS	C_2	704	$\{U_3(5)\}$
McL	C_3	66825	$\{2 \cdot \mathrm{PSL}_3(4)\}$
Ru	C_2	16240	$\{^2F_4(2)\}$
Suz	C_6	70866	$\{C_3 \times U_5(2), 2 \cdot G_2(4)\}$
$O'N$	C_3	368280	$\{\mathrm{PSL}_3(7) : 2\}$
B	C_2		

Chapter 2

Quotients

In this chapter we present two new results concerning exceptional groups.

Definition 2.0.1
Let G be a finite group. If there exists $N \trianglelefteq G$ with $\mu(G/N) > \mu(G)$ then we call G exceptional *and N* distinguished *in G.*

An early example of an exceptional group is given by Neumann [22] and described in more generality in [13]. They let G be the direct product of $k > 1$ copies of D_8, the dihedral group of order 8. One can show that $\mu(G) = 4k$ and that there is a central subgroup N of G of order 2^{k-1} such that $\mu(G/N) = 2^{k+1}$.

It is in this sense that $\mu(G/N)$ can be exponential in $\mu(G)$. It is shown in [13] that if G is nilpotent then $\mu(G/N) \leq 4.5^{\mu(G)}$.

2.1 Background Results

We present in this section existing results for the rest of the chapter, beginning with those on minimal exceptional p-groups.

Theorem 2.1.1
If G is exceptional then $|G| \geq 32$. This bound is obtained only in the following cases:

$$G \cong \langle x, y | x^8 = y^4 = 1, x^y = x^{-1} \rangle$$

$$G \cong \langle x, y, n | x^8 = n^2 = 1, y^2 = x^4, x^y = x^{-1}n, n^x = n^y = n \rangle$$

Proof: Theorem 1.5 of [9]. □

Theorem 2.1.2
Fix a prime p. Suppose $G \leq S_n$, P is a Sylow p-subgroup of G and Q an abelian p-quotient of G. If kp is the number of points in $[n]$ moved by P then $|Q| \leq p^k$.

Proof: This is taken from the main Theorem of [17]. □

Lemma 2.1.3
A distinguished quotient cannot be cyclic or elementary abelian.

Proof: This proof is taken from [9, 17]. Fix a finite group G and $N \trianglelefteq G$. Assume G is acting on Ω with $|\Omega| = \mu(G)$.

If G/N is cyclic then $G/N = \langle Ng \rangle$ for some $g \in G$. In particular we have $\mu(G) \geq \langle g \rangle \geq \langle Ng \rangle = \mu(G/N)$. Hence G/N is not distinguished.

If G/N is elementary abelian then $|G/N| = p^r$ and $\mu(G) = rp$ for some r and some prime p. If P is a Sylow p-subgroup of G and moves kp elements of Ω then $kp \leq \mu(G)$ and, by Theorem 2.1.2, $p^r \leq p^k$ so $r \leq k$. This gives $\mu(G/N) = rp \leq kp \leq \mu(G)$ so G/N is not distinguished. □

Lemma 2.1.4
Fix an exceptional group G such that no subgroup or quotient of G is exceptional and fix a distinguished subgroup N of G. Suppose $X_1, \ldots, X_r$ are the orbits of a minimal representation of G. Then N acts intransitively and non-trivially on each X_i.

Proof: Lemma 1.2 of [9]. □

Theorem 2.1.5
Let $p > 2$ be prime. The following lists all isomorphism types of groups of order p^3:

- C_{p^3}
- $C_{p_2} \times C_p$
- $C_p \times C_p \times C_p$
- $C_{p^2} \rtimes C_p \cong \langle x, y | x^{p^2} = y^p = 1, x^y = x^{1+p} \rangle$
- $(C_p \times C_p) \rtimes C_p \cong \langle x, y, z | x^p = y^p = z^p = 1, x^y = x^z = x, y^z = xy \rangle$

Proof: This is taken from section 4.4 in [12]. □

Lemma 2.1.6
Suppose H is a finite group with $|H| = p^k$ where $k \leq p$. Then for any $u, v \in H$ there is some $c \in [H, H]$ such that $(uv)^p = u^p v^p c^p$.

Proof: This is noted as a result of Corollary 12.3.1 in [12]. □

In the last section of this chapter we will show that normal subgroups with no abelian chief factors are not distinguished. This result has been published in [5]. The following is an analogous result, given as Theorem 1 in [18].

Theorem 2.1.7
Fix a finite group G and $N \trianglelefteq G$. If G/N has no non-trivial abelian normal subgroup then N is not distinguished.

A corollary of this, or of our result that normal subgroups with no abelian chief factors are not distinguished, is that a group with no abelian chief factors is not exceptional. In fact, both N and G/N must contain an abelian chief factor.

2.2 Minimal Exceptional p-Groups

As noted in the background results, previous work by Easdown and Praeger proves that an exceptional 2-group of least order is of order 2^5 and gives examples of exceptional groups of order 2^5. They note the existence of an exceptional group of order p^6 for any prime p and raise the question of whether an exceptional group of order p^5 exists. In this section, for all primes $p \geq 3$, we describe an exceptional group of order p^5 and prove that no exceptional group of order p^4 exists. These results are published in [4].

2.2.1 No Exceptional Groups of Order p^4

The case $p = 2$ is a corollary of Theorem 2.1.1. Fix prime $p \geq 3$.

If G is a p-group of order at most p^3 then for any non-trivial $N \trianglelefteq G$ we have $|G/N| \leq p^2$ which implies G/N is either cyclic or elementary abelian, so not distinguished by Lemma 2.1.3. Therefore any exceptional p-group G has order at least p^4.

For the remainder of this section, assume G is exceptional of order p^4 with N a distinguished subgroup of G. If $|G/N| \leq p^2$ then, by Lemma 2.1.3, G/N is not distinguished. Hence $|G/N| = p^3$ and $|N| = p$.

Fix a minimal faithful permutation representation of G, $\rho : G \to \mathrm{Sym}(X)$ with orbits $X_1, \ldots, X_k$ and for each i fix $H_i = G_\alpha$ for some $\alpha \in X_i$.

Lemma 2.2.1
(Immediate results): $N \leq Z(G)$ and $|X_i| = p^2$ for each i.

Proof: Each normal subgroup of a p-group intersects the center of the group non-trivially, so $N \leq Z(G)$.

By Lemma 2.1.4, N acts intransitively and non-trivially on each X_i so $|X_i| \geq p^2$. Also $|X_i| \leq \mu(G) < \mu(G/N) \leq |G/N| = p^3$, so $|X_i| = p^2$. $\square$

Theorem 2.2.2
There are no exceptional groups of order p^4.

Proof: Note that, as $|X_i| = p^2$ for each i, $\mu(G) \geq p^2$. Using $|G/N| = p^3$, we consider the 5 possible isomorphism classes of G/N given in Theorem 2.1.5.

By Lemma 2.1.3, distinguished quotients cannot be cyclic or elementary abelian. This excludes $G/N \cong C_p \times C_p \times C_p$ and $G/N \cong C_{p^3}$.

If $G/N \cong C_{p^2} \rtimes C_p$ with generators x, y and $x^y = x^{1+p}$, then $\langle y \rangle$ is a core-free subgroup of G/N (e.g. $y^{x^{-1}} = yx^y x^{-1} = yx^p$). Therefore G/N acts faithfully on the right cosets of $\langle y \rangle$ giving $\mu(G/N) \leq [G/N : \langle y \rangle] = p^2 \leq \mu(G)$ so N is not distinguished.

If $G/N \cong (C_p \times C_p) \rtimes C_p$ with generators x, y, z and $x^z = xy$, $y^z = y$ then $\langle x \rangle$ is a core-free subgroup of G/N. As in the last case, this implies N is not distinguished.

So we are left with $G/N \cong C_{p^2} \times C_p$. The minimal degree for abelian groups is well-known (see for example [9]) - In this case $\mu(G/N) = p^2 + p$. Consider the preimage H of C_{p^2} in G. Since N is central and C_{p^2} is cyclic, H is abelian of order p^3 containing an element of order p^2. This means $H \cong C_{p^3}$ or $H \cong C_{p^2} \times C_p$. In either case $\mu(G) \geq \mu(H) \geq p^2 + p = \mu(G/N)$ so N is not distinguished. $\square$

2.2.2 An Exceptional Group of order p^5

Fix a prime $p \geq 3$. For this section let G be the group generated by g, h subject to the following relations:

$$g^{p^2} = h^{p^2} = [g, h]^p = 1$$
$$[[g, h], g] = [[g, h], h] = g^p$$

Also, let N be the subgroup generated by $g^p h^p$. We show that $|G| = p^5$, $N \leq Z(G)$, $\mu(G) \leq 2p^2$ and $\mu(G/N) = p^3$. Thus G is exceptional with distinguished subgroup N. For $p = 2$, two exceptional groups of order p^5 exist and are given in Theorem 2.1.1.

Proposition 2.2.3
We can identify G with $(C_{p^2} \rtimes C_p) \rtimes C_{p^2}$ where the two copies of C_{p^2} are generated by g and h respectively and C_p is generated by $[g, h]$. In particular $|G| = p^5$

Proof: Straightforward calculations give $g^{[g,h]} = g[g, [g, h]] = g[[g, h], g]^{-1}$ so the relations on G give $g^{[g,h]} = g^{1-p}$. Thus $[g, h]$ normalises $\langle g \rangle$. Moreover $\langle [g, h] \rangle \cong C_p$ and $[g, h]$ does not commute with g so $\langle [g, h] \rangle \cap \langle g \rangle$ is trivial and $\langle g, [g, h] \rangle \cong C_{p^2} \rtimes C_p$.

A similar calculation gives $g^h = g[g,h]$ and $[g,h]^h = [g,h][[g,h],h] = [g,h]g^p$. To see that $\langle g, [g,h]\rangle \cap \langle h\rangle$ is trivial notice that $G/\langle g,[g,h]\rangle$ has generator h and relations $h^{p^2} = 1$, so $h^p \notin \langle g, [g,h]\rangle$. Hence $G \cong (C_{p^2} \rtimes C_p) \rtimes C_{p^2}$. $\square$

Proposition 2.2.4
$\langle g^p, h^p\rangle = Z(G)$. In particular $N \leq Z(G)$.

Proof: We begin by showing that $g^p \in Z(G)$. Using the identification given in Proposition 2.2.3, it is a standard result that $Z(C_{p^2} \rtimes C_p) = \langle g^p\rangle$ (to see this, you can check that $g^p \in Z(C_{p^2} \rtimes C_p)$, then note that $|Z(C_{p^2} \rtimes C_p)| = p$ otherwise $C_{p^2} \rtimes C_p$ would be abelian). Now, $Z(C_{p^2} \rtimes C_p) = \langle g^p\rangle$ is characteristic in $C_{p^2} \rtimes C_p$, so fixed by h under conjugation. There are no automorphisms of $\langle g^p\rangle$ of order p, so h must commute with g^p. Therefore $g^p \in Z(G)$.

We show by induction on i that $g^{h^i} = g[g,h]^i g^{\frac{1}{2}i(i-1)p}$. Therefore $g^{h^p} = g$ and $h^p \in Z(G)$. Note that $[g,h]^h = [g,h][[g,h],h] = [g,h]g^p$.

$$\begin{aligned} g^{h^{i+1}} &= (g[g,h]^i g^{\frac{1}{2}i(i-1)p})^h \\ &= g^h([g,h]^i)^h g^{\frac{1}{2}i(i-1)p} \\ &= g[g,h]^{i+1} g^{ip} g^{\frac{1}{2}i(i-1)p} \\ &= g[g,h]^{i+1} g^{\frac{1}{2}i(i+1)p} \end{aligned}$$

To see $\langle g^p, h^p\rangle = Z(G)$, consider $G/\langle g^p, h^p\rangle$. It is easy to see that this is isomorphic to $(C_p \times C_p) \rtimes C_p$, where the generators of the C_p are the images of g, $[g,h]$ and h. Following a similar argument as for $C_{p^2} \rtimes C_p$, $Z(G/\langle g^p, h^p\rangle)$ is the cyclic group generated by the image of $[g,h]$. If $|Z(G)| > p^2$ then this implies $[g,h] \in Z(G)$, but this is not true (e.g. $[[g,h],h] = g^p$) so $Z(G) = \langle g^p, h^p\rangle$. $\square$

Proposition 2.2.5
$\mu(G) \leq 2p^2$.

Proof: To show this, we describe a faithful representation of G of degree $2p^2$.

Let $H_1 = \langle g, [g,h]\rangle$ and $H_2 = \langle gh^{-1}, [g,h]\rangle$. Consider the natural action of G on the set of right cosets $G/H_1 \sqcup G/H_2$. This is faithful if and only if $\mathrm{core}_G(H_1 \cap H_2)$ is trivial.

It is clear from the presentation that $G/Z(G) = (C_p \times C_p) \rtimes C_p$. It is a standard result that this group has exponent p, so $(gh^{-1})^p \in Z(G)$. Following the identification in Proposition 2.2.3, $(gh^{-1})^p$ is non-trivial as its image in $G/(C_{p^2} \times C_p)$ is non-trivial, so gh^{-1} has order p^2.

From the above, it follows that $H_1 \cap H_2 = \langle [g,h]\rangle$ so $\mathrm{core}_G(H_1 \cap H_2)$ is trivial and that $|H_1| = |H_2| = p^3$ so $|G/H_1 \sqcup G/H_2| = 2p^2$ as required. $\square$

Proposition 2.2.6
$\mu(G/N) = p^3$.

Proof: The quotient G/N can be described with generators $a = Ng, b = Nh$ and relations

$$a^{p^2} = b^{p^2} = a^p b^p = [a,b]^p = 1$$

$$[[a,b],a] = [[a,b],b] = a^p$$

Noting that $a^p = b^{-p}$ it is immediate that $a^p \in Z(G)$. Consider $(G/N)/\langle a^p \rangle$ which can be described with generators $x = a\langle a^p \rangle$, $y = b\langle a^p \rangle$ and relations

$$x^p = y^p = [x,y]^p = [[x,y],x] = [[x,y],y] = 1$$

This is a presentation for $(C_p \times C_p) \rtimes C_p$. It is a standard result, with this presentation, that $Z((C_p \times C_p) \rtimes C_p) = [x,y]$. In particular, if $|Z(G/N)| > p$ then $[a,b] \in Z(G/N)$ which is not true, so $Z(G/N) = \langle a^p \rangle$.

Since any normal subgroup of a p-group intersects the center non-trivially, this means any non-trivial normal subgroup of G/N contains $Z(G/N)$. Any minimal representation of G/N is therefore given by the coset action of G/N on some core-free subgroup of G/N of largest order.

Suppose K is some such subgroup. Noting that $\langle [a,b] \rangle$ is core-free, we must have $|K| \geq p$. If K meets $\langle a \rangle$ or $\langle b \rangle$ non-trivially then it meets $Z(G/N)$ non-trivially.

Consider $K \cap \langle a, [a,b] \rangle$, this must be trivial or cyclic of order p. If it is trivial then K is isomorphic to its image in $(G/N)/\langle a, [a,b] \rangle$ which has order p so $\mu(G) = [G : K] = p^3$. So suppose $K \cap \langle a, [a,b] \rangle$ is generated by $a^i[a,b]^j$ for some i, j. If $p \nmid i$ then using $a^{a^{-1}b} = a[a,b]$ and $[a,b]^{a^{-1}b} = [a,b]$ we can find an appropriate conjugate of K in G containing a^i, contradicting the fact K is core-free. Therefore $K \cap \langle a, [a,b] \rangle = \langle a^{ip}[a,b] \rangle$ for some i. Since $[a,b]^b = [a,b]a^p$, we may consider instead $K^{b^{p-i}}$ so we may assume $K \cap \langle a, [a,b] \rangle = \langle [a,b] \rangle$.

Now suppose that $K > \langle [a,b] \rangle$. If $|K| = p^3$ then K is maximal and therefore normal in G/N contrary to assumption. Therefore $|K| = p^2$, so K is abelian. In particular $K \leq C_{G/N}([a,b])$. Clearly $[a,b], a^p \in C_{G/N}([a,b])$ and it is easy to check that $ab^{-1} \in C_{G/N}([a,b])$, so $C_{G/N}([a,b]) = \langle [a,b], ab^{-1}, a^p \rangle$ and $K = \langle [a,b], ab^{-1}x \rangle$ for some $x \in Z(G/N)$.

Note that $[G,G] = \langle [a,b], a^p \rangle \cong C_p \times C_p$. If $p \geq 5$ then, by Lemma 2.1.6, this gives $(ab^{-1})^p = a^p b^{-p} = a^{p^2}$. In the case $p = 3$ we can calculate $(ab^{-1})^3$ as follows.

$$a^b = a[a,b]$$

$$\begin{aligned} a^{b^2} &= a^b[a,b]^b \\ &= a[a,b]^2 a^3 \end{aligned}$$

$$\begin{aligned} (ab^{-1})^3 &= aa^b a^{b^2} b^{-3} \\ &= a^2[a,b]a[a,b]a^3b^{-3} \\ &= a^3[a,b]^a[a,b]a^3b^{-3} \\ &= a^3[a,b]a^3[a,b]a^3b^{-3} = b^{-3} \end{aligned}$$

In either case, $(ab^{-1}x)^p = (ab^{-1})^p \notin \langle [a,b] \rangle$, contradicting the earlier result that $|K| = p^2$. Therefore $K = \langle [a,b] \rangle$ and $\mu(G/N) = [G:K] = p^3$. □

2.3 Normal Subgroups With No Abelian Chief Factors Are Not Distinguished

Throughout we assume each group G is finite and that $G \leq S_{\mu(G)}$. We call G *D-minimal* if G is of least order such that there exists some distinguished $N \trianglelefteq G$ with no abelian composition factors.

Proposition 2.3.1
Let $N_0 \trianglelefteq G$ be distinguished, $N \trianglelefteq G$ and $N \leq N_0$ then either N is distinguished or N_0/N is distinguished in G/N.

Proof: If N_0/N is not distinguished in G/N then

$$\mu(G) < \mu(G/N_0) = \mu\left(\frac{G/N}{N_0/N}\right) \leq \mu(G/N)$$

Hence N is distinguished. □

Lemma 2.3.2
Let N, L, K be normal subgroups in G with N minimal and non-abelian. Then $N(K \cap L) = NK \cap NL$.

Proof: Clearly $N(K \cap L) \subseteq NK \cap NL$.

If $N \leq L$ or $N \leq K$ then the result is the modular law for groups, so assume $N \cap K = N \cap L = 1$

We first consider orders:

$$\begin{aligned} |N(K\cap L)| &= |N||K\cap L| \\ &= \tfrac{|N||K||L|}{|KL|} \\ |NK\cap NL| &= \tfrac{|NK||NL|}{|NKL|} \\ &= \tfrac{|N||K||L||N\cap KL|}{|KL|} \end{aligned}$$

So, if $N(K\cap L)\neq NK\cap NL$ then $|N\cap KL|>1$ and therefore $N\subseteq KL$. However as N and K are normal subgroups in G with $N\cap K=1$, $N\subseteq C_G(K)$. Similarly $N\subseteq C_G(L)$ so $N\subseteq C_G(KL)\leq C_G(N)$ contradicting the assumption that N is non-abelian. Hence $N(K\cap L)=NK\cap NL$. □

Proposition 2.3.3

If G is D-minimal with non-abelian distinguished minimal normal subgroup N, then G is transitive.

Proof: Let $\{H_1,\dots,H_k\}$ define a minimal permutation representation of G of degree $\mu(G)$. Denote $K_i=\mathrm{core}_G(H_i)$, so $\cap_{i=1}^k K_i=1$. The action of G/K_i on the right cosets of H_i then defines a minimal representation of G/K_i (if $\{H_{i0}/K_i,\dots,H_{ik_i}/K_i\}$ defines a representation of smaller degree then replacing H_i with $H_{i0},\dots,H_{ik_i}$ defines a representation of G of degree strictly less than $\mu(G)$).

Suppose that $k>1$, so $|K_i|>1$ for each i. As G is D-minimal we have $\mu(G/NK_i)\leq\mu(G/K_i)$. This means that there is some $\{H_{i0},\dots,H_{ik_i}\}$ for each i with

$$\sum_{j=1}^{k_i}[G:H_{ii_j}]\leq[G:H_i]$$

$$\mathrm{core}_G(\cap_{j=1}^{k_i}(H_{ii_j}))=NK_i$$

In particular

$$\sum_{i=1}^{k}\sum_{j=1}^{k_i}[G:H_{ii_j}]\leq\sum_{i=1}^{k}[G:H_i]=\mu(G)$$

$$\mathrm{core}_G(\cap_{i=1}^{k}\cap_{j=1}^{k_i}(H_{ii_j}))=\cap_{i=1}^{k}NK_i$$

Using Lemma 2.3.2 inductively then gives

$$\mathrm{core}_G(\cap_{i=1}^{k}\cap_{j=1}^{k_i}(H_{ii_j}))=N\cap_{i=1}^{k}K_i=N$$

so $\{H_{ii_j}\}$ defines a faithful representation of G/N of degree at most $\mu(G)$ contradicting the assumption that N is distinguished. Hence $k=1$ and G is transitive. □

Proposition 2.3.4
If G has a non-abelian distinguished minimal normal subgroup N, then $C_G(N)$ is non-trivial.

Proof: As N is a minimal normal subgroup, $N = S^k$ for some simple group S. If $C_G(N) = 1$ then the action of G on N by conjugation gives an embedding of G/N in $\mathrm{Out}(N) \cong \mathrm{Out}(S) \wr S_k$. Hence $\mu(G/N) \leq \mu(\mathrm{Out}(S) \wr S_k) \leq k\mu(\mathrm{Out}(S))$. For each simple group S, $\mathrm{Out}(S)$ and $\mu(S)$ are known (see for example [6]) and one can check that $\mu(\mathrm{Out}(S)) \leq \mu(S)$. It is also shown in [9] that if $T_1, \dots, T_r$ are simple groups then $\mu(T_1 \times \cdots \times T_r) = \mu(T_1) + \cdots + \mu(T_r)$. So $\mu(G/N) \leq k\mu(\mathrm{Out}(S)) \leq k\mu(S) = \mu(N) \leq \mu(G)$ contradicting the assumption that N is distinguished. Hence $C_G(N)$ is non-trivial. □

We will use the following result (see for example [25] Proposition 12.1) without further reference.

Proposition 2.3.5
Suppose G is transitive and $B_\Gamma = \{\Gamma_1, \dots, \Gamma_r\}$ forms a block system for G. Then G embeds into $(G_{\Gamma_1})^{\Gamma_1} \wr G^{B_\Gamma}$.

Proposition 2.3.6
If G is D-minimal and has a non-abelian distinguished minimal normal subgroup N then N is transitive.

Proof: By Proposition 2.3.3, G is transitive. Suppose N is intransitive. The orbits of N form a block system $B_\Gamma = \{\Gamma_1, \dots, \Gamma_r\}$ of G in Ω. We may therefore embed $\phi : G \hookrightarrow (G_{\Gamma_1})^{\Gamma_1} \wr G^{B_\Gamma}$.

Let $N_1 = N^{\Gamma_1} \trianglelefteq (G_{\Gamma_1})^{\Gamma_1}$ and $M = N_1^r \trianglelefteq (G_{\Gamma_1})^{\Gamma_1} \wr G^{B_\Gamma}$. Now, N is a direct product of isomorphic simple groups, so $M \cap \phi(G)$ is a direct product of isomorphic simple groups. Also $\phi(N)$ is normal in $M \cap \phi(G)$ and a subdirect product of $M \cap \phi(G)$. Hence $\phi(N) = M \cap \phi(G)$. Therefore $G/N \cong \phi(G)/\phi(N)$ embeds into

$$\frac{(G_{\Gamma_1})^{\Gamma_1} \wr G^{B_\Gamma}}{M} \cong \frac{(G_{\Gamma_1})^{\Gamma_1}}{N_1} \wr G^{B_\Gamma}$$

This gives

$$\mu(G/N) \leq \mu\left(\frac{(G_{\Gamma_1})^{\Gamma_1}}{N^{\Gamma_1}}\right) \frac{\mu(G)}{|\Gamma_1|}$$

If $\mu((G_{\Gamma_1})^{\Gamma_1}) < |\Gamma_1|$ then

$$\mu(G) \leq \mu((G_{\Gamma_1})^{\Gamma_1} \wr G^{B_\Gamma}) < |\Gamma_1||B_\Gamma| = \mu(G)$$

which is absurd. So $\mu((G_{\Gamma_1})^{\Gamma_1}) = |\Gamma_1|$.

If N_1 is not distinguished in $(G_{\Gamma_1})^{\Gamma_1}$ then $\mu((G_{\Gamma_1})^{\Gamma_1}/N_1) \leq |\Gamma_1|$. Therefore

$$\mu(G/N) \leq \mu\left(\frac{(G_{\Gamma_1})^{\Gamma_1}}{N_1} \wr G^{B_\Gamma}\right) \leq |\Gamma_1||B_\Gamma| = \mu(G)$$

so N is not distinguished. Hence N^{Γ_1} distinguished in $(G_{\Gamma_1})^{\Gamma_1}$.

This contradicts the assumption that G is D-minimal. Hence N must be transitive. □

We use the following result (see for example [26] Proposition 4.3) without further reference.

Proposition 2.3.7
Suppose $N \leq G$ is transitive. Then $C_G(N)$ is semiregular.

Proposition 2.3.8
Suppose G is D-minimal with non-abelian distinguished minimal normal subgroup N, then N is not simple.

Proof: Suppose such an N is simple. By Propositions 2.3.3 and 2.3.6 G and N are transitive. Let H be the stabiliser of some point in Ω, so $G = HN$. In particular $G/N \cong H/(H \cap N)$ so

$$\mu(H) \leq \mu(G) < \mu(G/N) = \mu(H/(H \cap N))$$

and $H \cap N$ is distinguished in H. Also $\mu(G) = [G : H] = [N : H \cap N]$.

As $C = C_G(N)$ is semiregular, $H \cap C = 1$. In particular H embeds into G/C which in turn embeds into $\mathrm{Aut}(N)$ via conjugation. Let $H_{\mathrm{Inn}(N)}$ be the elements of H which act on N via inner automorphisms. This gives $H \cap N \trianglelefteq H_{\mathrm{Inn}(N)}$.

The image of $H_{\mathrm{Inn}(N)}$ in $\mathrm{Aut}(N)$ is strictly contained in $\mathrm{Inn}(N)$. Indeed, by assumption if $H \cap N$ is trivial then

$$\mu(G/N) = \mu(H/(H \cap N)) = \mu(H) \leq \mu(G)$$

contrary to assumption. So $H \cap N$ is non-trivial. If the image of $H_{\mathrm{Inn}(N)}$ in $\mathrm{Aut}(N)$ is $\mathrm{Inn}(N)$ then simplicity of N implies $H \cap N = N$ contradicting the fact that H is core-free. Hence the image of $H_{\mathrm{Inn}(N)}$ in $\mathrm{Aut}(N)$ is strictly contained in $\mathrm{Inn}(N)$.

This means $H_{\mathrm{Inn}(N)}$ is isomorphic to a core-free subgroup of N. Hence $|H_{\mathrm{Inn}(N)}| \leq |N|/\mu(N)$. We also have, by definition of $H_{\mathrm{Inn}(N)}$ that $H/H_{\mathrm{Inn}(N)}$ embeds into $\mathrm{Out}(N)$. By Proposition 1.3.1 $|\mathrm{Out}(N)| < \mu(N)$. This gives

$$|H/(H \cap N)| = \frac{|H|}{|H_{\mathrm{Inn}(N)}|}\frac{|H_{\mathrm{Inn}(N)}|}{|H \cap N|} \leq \frac{|\mathrm{Out}(N)|}{\mu(N)}\frac{|N|}{|H \cap N|} < \mu(G)$$

This means $\mu(G/N) = \mu(H/(H \cap N)) < \mu(G)$ contrary to assumption. We must therefore have that N is not simple. □

Lemma 2.3.9

Suppose $G = HN$ where $\{H\}$ defines a minimal representation of G, $N \trianglelefteq G$ and $Z(N) = 1$. Denote $C = C_G(N)$ and $H_{\mathrm{Inn}(N)}$ the subgroup of H which acts on N by conjugation inducing inner automorphisms of N.

Then $C \cong H_{\mathrm{Inn}(N)}/(H \cap N)$.

If further N is a distinguished minimal normal subgroup of G then $\mu(G) = |C|\mu(G/C)$.

Proof: Define a group homomorphism $\phi : H_{\mathrm{Inn}(N)} \to C$ as follows. If $h \in H_{\mathrm{Inn}(N)}$ then, as $Z(N) = 1$, there is a unique $n_h \in N$ such that, for all $x \in N$, $x^h = x^{n_h}$. In particular, for all $x \in N$, $x^{hn_h^{-1}} = x$ so $c_h = hn_h^{-1} \in C$. Define $\phi(h) = c_h$. To see ϕ is a homomorphism notice that

$$c_{h_1}c_{h_2} = h_1n_1^{-1}h_2n_2^{-1} = h_1h_2(n_1^{-1})^{h_2}n_2^{-1} = c_{h_1h_2}$$

To see ϕ is surjective suppose $c \in C$. As $G = HN$ we have $c = hn$ for some $h \in H$, $n \in N$. In particular h acts on N identically under conjugation to n^{-1} so $h \in H_{\mathrm{Inn}(N)}$ and $c = \phi(h)$. Finally $h \in \ker(\phi)$ if and only if $hn_h^{-1} = 1$ if and only if $h = n_h$ if and only if $h \in H \cap N$. This gives $C \cong H_{\mathrm{Inn}(N)}/(H \cap N)$.

Now suppose further that N is a distinguished minimal normal subgroup of G.

Let Γ be an orbit of C under the representation defined by $\{H\}$. We have, by Proposition 2.3.7, that C is semiregular so $H \cap C = 1$ and $|\Gamma| = |C|$. Also Γ forms a block for the action of G so G embeds into $(G_\Gamma)^\Gamma \wr G^{\mathcal{B}_\Gamma}$. This gives

$$\mu(G) \leq \mu((G_\Gamma)^\Gamma \wr G^{\mathcal{B}_\Gamma}) \leq \mu((G_\Gamma)^\Gamma)\mu(G^{\mathcal{B}_\Gamma}) \leq |\Gamma|\frac{\mu(G)}{|\Gamma|} = \mu(G)$$

Hence $\mu((G_\Gamma)^\Gamma) = |\Gamma| = |C|$ and $\mu(G^{\mathcal{B}_\Gamma}) = \mu(G)/|C|$. It suffices then to show that $G^{\mathcal{B}_\Gamma} \cong G/C$. The action $G^{\mathcal{B}_\Gamma}$ is defined by $\{HC\}$ so it suffices to show $\mathrm{core}_G(HC) = C$. Immediately $C \leq \mathrm{core}_G(HC)$. Suppose $K \leq HC$ with $K \trianglelefteq G$. If $K \cap N = N$ then K is transitive so HC and therefore C is transitive. But then N is contained in the center of a transitive normal subgroup C, so $N \cap H = 1$ and $\mu(G/N) = \mu(H) \leq \mu(G)$ contrary to assumption. Hence $K \cap N = 1$. Hence $K \leq C$. This gives $\mathrm{core}_G(HC) = C$ and completes the proof. $\square$

Theorem 2.3.10

Given a finite group G and distinguished normal subgroup $N \trianglelefteq G$, N must have an abelian chief factor.

Proof: We consider a counterexample (G, N) such that G is of least order. In particular G is D-minimal and N has no abelian composition factors. Let N_0

be a minimal normal subgroup of G contained in N. As G is D-minimal, N/N_0 is not distinguished in G/N_0, so by Proposition 2.3.1 N_0 is distinguished in G. Replacing N with N_0 if necessary we may assume N is minimal.

By Propositions 2.3.8, 2.3.3 and 2.3.6 N is not simple and G and N are transitive. In particular we may denote $N = T_1 \times \cdots \times T_k$ with $k > 1$ where for some simple T we have $T_i \cong T$ for each i.

Let H be the stabiliser of some point in Ω, so $G = HN$. In particular $\mu(G) = [G : H] = [N : H \cap N]$ and $G/N \cong H/(H \cap N)$ so $H \cap N$ is distinguished in H.

Let $C = C_G(N)$. Then $H \cap C = 1$ so H embeds into G/C which in turn embeds into $\mathrm{Aut}(N) \cong \mathrm{Aut}(T) \wr S_k$ via conjugation. Also by Lemma 2.3.9, $C \cong H_{\mathrm{Inn}(N)}/(H \cap N)$ and $\mu(G) = |C|\mu(G/C)$. Together this gives

$$\begin{aligned} |N| &= |N \cap H|\mu(G) \\ &= |N \cap H||C|\mu(G/C) \\ &\leq |N \cap H||C|k\mu(\mathrm{Aut}(T)) \\ &= |H_{\mathrm{Inn}(N)}|k\mu(\mathrm{Aut}(T)) \end{aligned}$$

Let $\phi : G \to S_k$ be the natural map on G through $\mathrm{Aut}(N)$ and define $\psi : H_{\mathrm{Inn}(N)} \to \mathrm{Aut}(T)$ by the conjugation of T_1 by $H_{\mathrm{Inn}(N)}$. Since N is minimal, $\phi(G)$ and therefore $\phi(H)$ is transitive. This means the action of $H_{\mathrm{Inn}(N)}$ on each T_i by conjugation has isomorphic image in $\mathrm{Aut}(T)$. This gives $|H_{\mathrm{Inn}(N)}| \leq |\psi(H_{\mathrm{Inn}(N)})|^k$ and therefore

$$\frac{|T|}{|\psi(H_{\mathrm{Inn}(N)})|} \leq \left(\frac{|N|}{|H_{\mathrm{Inn}(N)}|}\right)^{\frac{1}{k}} \leq k^{\frac{1}{k}}\mu(\mathrm{Aut}(T))^{\frac{1}{k}}$$

We show here that $\frac{|T|}{|\psi(H_{\mathrm{Inn}(N)})|} < \mu(T)$ and therefore that $\psi(H_{\mathrm{Inn}(N)}) \cong T$. We begin with the small cases, $T = A_5, A_6$.

If $T = A_5$ then $k^{\frac{1}{k}}\mu(\mathrm{Aut}(T))^{\frac{1}{k}} = k^{\frac{1}{k}}5^{\frac{1}{k}} < 5$.

If $T = A_6$ then $k^{\frac{1}{k}}\mu(\mathrm{Aut}(T))^{\frac{1}{k}} = k^{\frac{1}{k}}10^{\frac{1}{k}} < 6$.

For all other simple groups $\mu(T) \geq 7$. By Proposition 1.3.2 we have $\mu(\mathrm{Aut}(T)) \leq \frac{28}{9}\mu(T)$.

Let $f(x) = x^k - \frac{28}{9}kx$ so $f(x) > 0$ if and only if $\left(\frac{28}{9}\right)^{\frac{1}{k}} k^{\frac{1}{k}} x^{\frac{1}{k}} < x$. For $x \geq 7$, $f'(x) = kx^{k-1} - \frac{28}{9}k > 0$ so if $f(7) > 0$ then $f(x) > 0$ for $x \geq 7$. One can check $f(7) > 0$. Hence $\frac{|T|}{|\psi(H_{\mathrm{Inn}(N)})|} \leq \left(\frac{28}{9}\right)^{\frac{1}{k}} k^{\frac{1}{k}}\mu(T)^{\frac{1}{k}} < \mu(T)$. This completes the proof that $\psi(H_{\mathrm{Inn}(N)}) \cong T$.

This means $H_{\mathrm{Inn}(N)}$ is a subdirect product of $N \cong T^k$ so is isomorphic to T^r for some r. Also $H \cap N \trianglelefteq H_{\mathrm{Inn}(N)}$, so has no abelian chief factors. But $H \cap N$ is distinguished in H contradicting the fact that G is D-minimal and completing the proof. $\square$

Chapter 3

Quasisimple Groups

In this chapter we consider group extensions $1 \to N \to E \to G \to 1$ and study the following question. If $\mu(G)$ and $\mu(N)$ are known then what can we say about $\mu(E)$?

This question has been studied in many papers. It is shown in [27] for example that if G and H are nilpotent then $\mu(G \times H) = \mu(G) + \mu(H)$ - this is generalised in [2] to groups with central socle. Easedown and Hendrikson have provided the most in depth study of semidirect products in [8]. So it remains to consider non-split extensions. The simplest such extensions are perhaps quasisimple groups.

A *quasisimple* group is a perfect central extension of a simple group. The Schur cover of a non-abelian simple group is such a group (in fact quasisimple groups are precisely the non-trivial quotients of Schur covers of simple groups). We consider here some Schur covers of non-abelian simple groups. Recall that the minimal degrees of simple groups are known (see Table in section 1.3.1).

We begin with some immediate general results.

Lemma 3.0.1
Suppose G is quasi-simple with center Z. If $K < G$ then $ZK < G$. In particular if $K \lhd G$ then $K \leq Z$.

Proof: Suppose $ZK = G$. Then $G = [G,G] = [ZK, ZK] = [K,K] \leq K$. Hence if $K < G$ then $ZK < G$. If further $K \lhd G$ then $KZ \lhd G$. The image of KZ in G/Z is a proper normal subgroup of G/Z and is therefore trivial. Hence $K \leq Z$. $\square$

Proposition 3.0.2
Suppose G is quasi-simple with center Z. Denote $S = G/Z$. Then

$$\mu(G) \geq \mu(Z)\mu(S)$$

Proof: Suppose $\{H_1, \ldots, H_k\}$ defines a minimal representation of G.

By Lemma 3.0.1, $\mathrm{core}_G(H_i) \leq Z$ so $\mathrm{core}_G(H_i) = H_i \cap Z$ for each i. Since $\{H_1, \ldots, H_k\}$ is a faithful representation of G, $1 = \cap_{i=1}^k \mathrm{core}_G(H_i) = \cap_{i=1}^k H_i \cap Z$. In particular $\{H_1 \cap Z, \ldots, H_k \cap Z\}$ defines a faithful representation of Z. This implies that $\sum_{i=1}^k [Z : H_i \cap Z] \geq \mu(Z)$.

Also by Lemma 3.0.1, $H_i Z < G$ for each i. Let K_i be the image of $H_i Z$ in S so $K_i < G/Z$. As S is simple $\mathrm{core}_S(K_i) = 1$ so $\{K_i\}$ is a faithful representation of S and $[S : K_i] \geq \mu(S)$.

Together this gives

$$\begin{aligned} \mu(G) &= \textstyle\sum_{i=1}^k [G : H_i] \\ &= \textstyle\sum_{i=1}^k [G : H_i Z][H_i Z : H_i] \\ &= \textstyle\sum_{i=1}^k [S : K_i][H_i : H_i \cap Z] \\ &\geq \mu(S)\mu(Z) \end{aligned}$$

□

3.1 The Two Cover of the Alternating Group

In this section we describe for all positive n a core-free subgroup of $2 \cdot A_n$ of largest order. One minimal permutation representation of $2 \cdot A_n$ is then the coset action of $2 \cdot A_n$ on this subgroup.

Throughout a *'largest core-free subgroup'* means a core-free subgroup of largest order.

In order to bound the order of some core-free subgroups of $2 \cdot A_n$ we will need the following bounds by Maróti and Robbins - it is worth noting that the bound by Robbins is related to Stirling's approximation. We use these bounds without further reference.

Theorem 3.1.1
Let $G \leq S_n$ be primitive with $A_n \not\leq G$. Then $|G| < 3^n$. If further $n > 24$ then $|G| < 2^n$.

Proof: [19] (Corollary 1.2). □

Theorem 3.1.2

$$n\log(n) - n + \frac{1}{2}\log(2\pi n) + \frac{1}{12n+1} < \log(n!) < n\log(n) - n + \frac{1}{2}\log(2\pi n) + \frac{1}{12n}$$

Proof: Direct corollary of [23]. □

A Brief Description of $2 \cdot A_n$

There are multiple ways to approach $2 \cdot A_n$. We will find it most useful to view it as a subgroup of $2 \cdot S_n^-$, but it is defined to be the universal cover (or Schur cover) of the alternating group A_n for all $n > 7$ and for $n \in \{4, 5\}$. This means that for $n > 7$ and for $n \in \{4, 5\}$, $2 \cdot A_n$ is the unique non-split central extension of A_n by the cycle group of order 2, C_2:

$$1 \to C_2 \to 2 \cdot A_n \to A_n \to 1$$

The symmetric group S_n has two such extensions, $2 \cdot S_n^+$ and $2 \cdot S_n^-$, each of which contains $2 \cdot A_n$ as a subgroup. The author found $2 \cdot S_n^-$ slightly more convenient, so we will only define here $2 \cdot S_n^-$.

The following presentations are well-known for S_n and $2 \cdot S_n^-$:

$$\begin{aligned} S_n \cong \quad & \langle s_1, \ldots, s_{n-1} | s_i^2 = (s_j s_{j+1})^3 = (s_k s_l)^2 = 1 \\ & i, l, k \in [n-1], j \in [n-2], l - k \geq 2 \rangle \end{aligned}$$

$$\begin{aligned} 2 \cdot S_n^- \cong \quad & \langle s_1, \ldots, s_{n-1}, z | s_i^2 = (s_j s_{j+1})^3 = (s_k s_l)^2 = z, z^2 = 1 \\ & i, l, k \in [n-1], j \in [n-2], l - k \geq 2 \rangle \end{aligned}$$

From now on we use s_i as element of $2 \cdot S_n^-$. In particular, s_i is in the preimage of $(i, i+1)$. We denote $t_i = s_{i+1} s_i$ for $i = 1, \ldots, n-2$, so that t_i is in the preimage of $(i, i+1, i+2)$.

Proposition 3.1.3
Let $g \in S_n$ have order d.

1. *If d is odd then there is some $h \in 2 \cdot S_n^-$ in the preimage of g of order $2d$. The other element in the preimage is $h^{d+1} = hz$ which has order d.*

2. *If d is even then there is some $h \in 2 \cdot S_n^-$ in the preimage of g of order $2d$ if and only if both both elements in the preimage have order $2d$ if and only if $g^{d/2}$ consists of r transpositions where $r \equiv 1$ or 2 (mod 4).*

Proof: 1. Let h be in the preimage of g. If h has order d replace it with hz.

2. As we condition only on $g^{d/2}$ we may restrict to the case $d = 2$.

Let $h \in 2 \cdot S_n^-$ be in the preimage of g. Clearly h has order 4 if and only if hz does if and only if $h^2 = z$. Moreover g has order 2 so is the product of r disjoint transpositions. In particular there is some $x \in S_n$ such that $g^x = (1, 2)(3, 4) \cdots (2r-1, 2r)$. Order is preserved under conjugation and for $y \in 2 \cdot S_n^-$ in the preimage of x we have that h^y is in the preimage of g^x so we may assume $g = (1, 2)(3, 4) \cdots (2r-1, 2r)$ so $h \in \{s_1 s_3 \ldots s_{2r-1}, s_1 s_3 \ldots s_{2r-1} z\}$. For $r > 1$ denote $h_{-1} = s_1 s_3 \ldots s_{2r-3}$

We now use induction on r. For $r = 1$ we have $h^2 = s_1^2 = z$ - one of the defining relations of $2 \cdot S_n^-$. For $r > 1$ notice that the relation $(s_i s_j)^2 = z$ gives $s_i s_j = s_j s_i z$ for $j \geq i + 2$. Using this and $s_{2r-1}^2 = z$ to remove s_{2r-1} gives:

$$\begin{aligned} h^2 &= (s_1 \cdots s_{2r-1})^2 \\ &= (s_1 \cdots s_{2r-3})^2 z^r \\ &= h_{-1}^2 z^r \end{aligned}$$

Hence if r is even then $h^2 = h_{-1}^2$ and if r is odd then $h^2 = h_{-1}^2 z$ and the result follows. $\square$

This result will make determining whether subgroups are core-free much easier later. It also allows us to use some tidier notation for elements of $2 \cdot A_n$. Denote by $[x_1, \ldots, x_d]$ an element in the preimage of $(x_1, \ldots, x_d)$ such that if d is odd then the order of $[x_1, \ldots, x_d]$ is $2d$. If d is even then this does not uniquely determine $[x_1, \ldots, x_d]$, so when using this notation we do have to be careful that the choice does not affect the argument.

Corollary 3.1.4
Fix $n > 7$ or $n \in \{4, 5\}$. Denoting

$$\begin{aligned} 2 \cdot S_n^- \cong \quad & \langle s_1, \ldots, s_{n-1}, z | s_i^2 = (s_j s_{j+1})^3 = (s_k s_l)^2 = z, z^2 = 1 \\ & i, l, k \in [n-1], j \in [n-2], l - k \geq 2 \rangle \end{aligned}$$

and $t_i = s_{i+1} s_i$ we have

$$2 \cdot A_n \cong \langle t_1, \ldots, t_{n-2} \rangle$$

Proof: The image of $\langle t_1 \ldots, t_{n-2} \rangle$ in S_n is clearly A_n and by Proposition 3.1.3 $t_i^3 = z$. $\square$

For $n \in \{1, 2, 3, 6\}$ it then makes sense to define

$$2 \cdot A_n = \langle z, t_1, \ldots, t_{n-2} \rangle \leq 2 \cdot S_n^-$$

where we include z to signify that $2 \cdot A_1$ and $2 \cdot A_2$ are non-trivial.

Proposition 3.1.3 also justifies the following definition:

Definition 3.1.1
Suppose $K < 2 \cdot A_n$. We call K almost core-free *when if $g \in K$ has image in A_n of order 2 then g also has order 2.*

Clearly core-free subgroups are almost core-free. It is conjectured that almost core-free subgroups are also core-free.

Setting Up

A core-free subgroup $K < 2 \cdot A_n$ is isomorphic to its image in A_n. We will therefore refer to properties of any core-free subgroup K as if it is acting on $\{1, \ldots, n\}$. For example, whether K is transitive or intransitive on $\{1, \ldots, n\}$.

We begin by describing an important core-free subgroup of $2 \cdot A_n$. Let $k = \lfloor \frac{n}{2} \rfloor$ and define:

$$B_n = \langle t_1 t_{k+1}, t_2 t_{k+2}, \ldots, t_{k-2} t_{2k-2} \rangle$$

Proposition 3.1.5
B_n is core-free and isomorphic to A_k.

Proof: Let $u_i = t_i t_{k+i}$. We show by induction on r that

$$u_{i_1} \cdots u_{i_r} = t_{i_1} \cdots t_{i_r} t_{k+i_1} \cdots t_{k+i_r}$$

So if $u_{i_1} \cdots u_{i_r} \in \{1, z\}$ then, checking its image in A_n, $\epsilon = t_{i_1} \cdots t_{i_r} \in \{1, z\}$. By construction $t_1, \ldots, t_{k-2}$ satisfy the same relations (adding k to each index) as $t_{k+1}, \ldots, t_{2k-2}$ so $t_{k+i_1} \cdots t_{k+i_r} = \epsilon$ and $u_{i_1} \cdots u_{i_r} = \epsilon^2 = 1$ so $z \notin B_n$.

The case $r = 1$ is immediate so consider $r > 1$. If $i \in \{1, \ldots, k-2\}$ and $j \in \{k+1, \ldots, 2k-2\}$ then, using $(s_a s_b)^2 = z$ for $b - a > 2$, we obtain

$$\begin{aligned} t_i t_j &= s_{i+1} s_i s_{j+1} s_j \\ &= z^4 s_{j+1} s_j s_{i+1} s_i \\ &= t_j t_i \end{aligned}$$

so

$$\begin{aligned} u_{i_1} \cdots u_{i_r} &= u_{i_1} \cdots u_{i_{r-1}} t_{i_r} t_{k+i_r} \\ &= t_{i_1} \cdots t_{i_{r-1}} t_{k+i_1} \cdots t_{k+i_{r-1}} t_{i_r} t_{k+i_r} \\ &= t_{i_1} \cdots t_{i_r} t_{k+i_1} \cdots t_{k+i_r} \end{aligned}$$

□

This gives us some immediate information about a largest core-free subgroup for sufficiently large n.

Corollary 3.1.6
Let $n > 24$. If a core-free subgroup K is transitive then $|K| < |B_n|$ or K is imprimitive.

Proof: We have $|B_n| = \frac{k!}{2}$ and, for $n > 24$, primitive groups either contain the alternating group or are of order at most 2^n.

We show by induction that $2^n < \frac{k!}{2}$. This is a straightforward calculation for $n \in \{25, 26\}$ and, for $n > 26$,

$$2^{n+2} = 4 \cdot 2^n < (k+1)\frac{k!}{2} = \frac{(k+1)!}{2}$$

Hence a largest core-free subgroup K can only be primitive if $K = A_n$, but then $[1,2][3,4] \in K$ so K is not core-free. Hence K is imprimitive. □

3.1.1 Computing Largest Core-Free Subgroups

We describe in this section an algorithm which, for each n, computes an upper bound on the orders of core-free subgroups of $2 \cdot A_n$. We then provide explicit descriptions of core-free subgroups of $2 \cdot A_n$ which attain these bounds, except when $n \in \{16, 21\}$. In these cases the proposed algorithm does not give a tight bound, but a largest core-free subgroup can be found by a naive search over conjugacy classes of subgroups. We describe a largest core-free subgroup in all cases.

Example MAGMA code can be found in Appendix A.

Algorithm Outline

The algorithm is inductive. For each n we compute three lists, PCFs(n), TCFs(n), FCFs(n), ACFs(n). These stand for "Primitive Core-Frees", "Transitive Core-Frees", "Fixed orbit length Core-Frees" and "All Core-Frees" respectively. The lists satisfy the following properties (throughout we identify K with its image in S_n and when referring to any one list, we use xCFs(n)):

- Elements of xCFs(n) are of the form (a, b, c) with $a, b, c \in \mathbb{N}$.

  ....

- Suppose $K < 2 \cdot A_n$ is core-free and primitive then there is some $(a, b, n) \in$ PCFs(n) with $|K| \leq a$, $|N_{S_n}(K)| \leq b$.
- Suppose $K < 2 \cdot A_n$ is core-free and transitive then there is some $(a, b, n) \in$ TCFs(n) with $|K| \leq a$, $|N_{S_n}(K)| \leq b$.
- Suppose $K < 2 \cdot A_n$ is core-free with all orbits of length c then there is some $(a, b, c) \in$ FCFs(n) with $|K| \leq a$, $|N_{S_n}(K)| \leq b$.
- Suppose $K < 2 \cdot A_n$ is core-free with minimal orbit of length d then there is some $(a, b, c) \in$ ACFs(n) with $|K| \leq a$, $|N_{S_n}(K)| \leq b$ and $d \leq c$.

The largest a appearing in some (a, b, c) in ACFs(n) then gives our upper bound on the order of core-free subgroups.

We use the term algorithm here loosely. In fact we outline four algorithms, one for each list. We use PCFs(n) to construct TCFs(n), TCFs(n) to construct FCFs(n) and FCFs(n) to construct ACFs(n).

For smaller n (how small varies between lists) we will need to put in more work to get the bounds lower and for larger n we are able use weaker bounds that require less work. We will mostly be able to avoid testing if a subgroup of $2 \cdot A_n$ is core-free, which can be very hard. When we do have to test a subgroup, instead of testing whether a group is core-free we use Proposition 3.1.3 to test whether the group is almost core-free.

Building PCFs(n)

The following result makes building this list for small n very easy.

Lemma 3.1.7
Suppose P is a primitive subgroup of S_n not containing A_n of largest order. Then P is self normalising.

Proof: For $n \leq 4$ no such subgroup exists so $n \geq 5$. As $1 \neq P \ngeq A_n$ we have $N_{S_n}(P) \notin \{S_n, A_n\}$, but $N_{S_n}(P)$ is primitive of order at least $|P|$, so we must have $N_{S_n}(P) = P$. □

Corollary 3.1.8
If P is a proper primitive subgroup of A_n of largest order then $|N_{S_n}(P)| \leq 2|P|$.

Proof: Immediately $N_{S_n}(P)$ is primitive. Moreover $N_{S_n}(P) \cap A_n$ is a subgroup of A_n containing P. Hence $N_{S_n}(P) \cap A_n$ is primitive so must equal P by Lemma 3.1.7, which gives the result. □

For small n it is feasible to check all primitive subgroups and for those P which are almost core-free add $(|P|, |N_{S_n}(P)|, n)$ to PCFs(n). For slightly larger n we can look for the largest primitive proper subgroup P of A_n (if one exists) and add $(|P|, 2|P|, n)$ to PCFs(n). For large n it suffices to use an exponential bound on primitive subgroups of S_n not containing A_n and add $(2^n, 2^n, n)$ to PCFs(n). See the `buildPCFs` function in Appendix A as example MAGMA code which does this.

Building TCFs(n)

We begin by using brute force to build TCFs(n) for small n. Naively we would consider all (conjugacy classes of) subgroups of A_n and for each almost core-free subgroup T add $(|T|, |N_{S_n}(T)|, n)$ to TCFs(n). There are several easy ways to implement improvements to this.

First notice that if we know some transitive almost core-free subgroup T and for some other transitive almost core-free U we have $|N_{S_n}(U)| \leq |T|$ then we need only add $(|T|, |N_{S_n}(T)|, n)$ to TCFs(n). Also if $N_{S_n}(T)$ has a normal almost core-free subgroup $U > T$ then we need only add $(|U|, |N_{S_n}(U)|, n)$ to TCFs(n). This suggests searching for normalisers of almost core-free subgroups instead of just almost core-free subgroups.

To this end we begin with a queue $Q = (S_n)$. At each step we take the largest subgroup G of S_n in Q, assume it is a normaliser of an almost core-free transitive subgroup of $2 \cdot A_n$, find the largest such subgroup T of G (if it exists) and add $(|T|, |G|, n)$ to $\mathrm{TCFs}(n)$. We then replace G with its transitive maximal subgroups. We stop when $|G| < |T|$ for some $(|T|, b, n) \in \mathrm{TCFs}(n)$.

To see that this works, notice that if T is an almost core-free transitive subgroup then either its normaliser is never considered, in which case there is some $(|U|, b, n) \in \mathrm{TCFs}(n)$ with $|N_{S_n}(T)| \leq |U|$, or it is considered, so $(|U|, |N_{S_n}(T)|, n) \in \mathrm{TCFs}(n)$ where U is the largest normal almost core-free subgroup of $N_{S_n}(T)$. In any case there is some $(a, b, n) \in \mathrm{TCFs}(n)$ with $|T| \leq a$ and $|N_{S_n}(T)| \leq b$ as required.

By trial and error, the most efficient method for replacing $G \in Q$ with its maximal subgroups seems to be to order the maximal subgroups of G by their size and insert them into Q maintaining the order of subgroups in Q. See the `bruteTCFs` function in Appendix A as example MAGMA code which does this. Notably this function actually adds $(|T|, |G|, n)$ for every normal subgroup T of G - one can check that adding additional elements to $\mathrm{TCFs}(n)$ does not stop $\mathrm{TCFs}(n)$ having the required properties.

For larger n this brute force method is impractically slow. Instead we make assumptions on the structure of a given transitive almost core-free subgroup T to bound $|T|$ and $|N_{S_n}(T)|$. If T is primitive then there is some $(a, b, n) \in \mathrm{PCFs}(n)$ with $|T| \leq a$ and $|N_{S_n}(T)| \leq b$ so we begin by adding $\mathrm{PCFs}(n)$ to $\mathrm{TCFs}(n)$ and assume hereafter that T is an almost core-free imprimitive subgroup. Denote by Γ a minimal block of T.

Case $|\Gamma| = 2$

We begin with the case $|\Gamma| = 2$ (in particular n is even). Relabelling if necessary we can assume that $\mathcal{B}_\Gamma = \{\Gamma_i | i \in \{1, \ldots, \frac{n}{2}\}\}$ with $\Gamma_i = \{2i-1, 2i\}$.

Definition 3.1.2
Let $x = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$ then we define the (Hamming) weight of x is $\mathrm{ham}(x) = \sum_{x_i=1} 1$. That is the number of x_i which are 1.

Lemma 3.1.9
Fix n even and let K be a core-free subgroup of $2 \cdot A_n$ fixing each Γ_i. The following table bounds $|K|$ for various values of n.

n	$\|K\|$
≤ 6	1
≥ 8	$\leq 2^{\frac{n}{2}-3}$
≥ 10	$\leq 2^{\frac{n}{2}-4}$
≥ 18	$\leq 2^{\frac{n}{2}-5}$
≥ 22	$\leq 2^{\frac{n}{2}-6}$

Proof: First note that we may identify $(2i-1, 2i)$ with the i^{th} standard basis vector of $\mathbb{F}_2^{\frac{n}{2}}$ therefore K with a subgroup of $\mathbb{F}_2^{\frac{n}{2}}$. Proposition 3.1.3 implies that if $x \in K$ then $\mathrm{ham}(x)$ is divisible by 4.

Suppose that $|K| = 2^r$. We consider a matrix, B, the rows of which form a basis of K. After a change of basis if necessary,

$$B := (I_r|B')$$

As every row of B must have weight divisible by 4 the result for $n \leq 6$ follows immediately and the weight of each row in B' must be 3 (mod 4). If two rows of B' are equal then the sum of the two corresponding rows in B has weight 2 and K is not core-free, so any two rows of B' are distinct.

If $r = \frac{n}{2} - 3$ then the only possible row in B' is $(1, 1, 1)$. Therefore B has at most 1 row so $r \leq 1$ which gives $n \leq 8$. Hence the result for $n \geq 10$.

If $r = \frac{n}{2} - 4$ then the only possible rows in B' are $(0, 1, 1, 1)$, $(1, 0, 1, 1)$, $(1, 1, 0, 1)$ and $(1, 1, 1, 0)$. Therefore B has at most 4 rows so $r \leq 4$ which gives $n \leq 16$. This gives the result for $n \geq 18$.

If $r = \frac{n}{2} - 5$ then we may assume without loss of generality that the top row x of B' is $(0, 0, 1, 1, 1)$. Consider a second row y. If x and y both have a 1 in the same k entries then $\mathrm{ham}(x + y) = 6 - 2k$. This means we must have $k = 2$ and we may assume without loss of generality that $y = (1, 0, 1, 1, 0)$. Similarly a third row z must have a 1 exactly two of the entries for which x does and exactly two of the entries for which y does. We therefore have $z \in \{(0, 1, 1, 1, 0), (1, 0, 1, 0, 1), (1, 0, 0, 1, 1)\}$. Hence B can have at most 5 rows. This gives $r \leq 5$ and therefore $n \leq 20$, concluding the proof for $n \geq 22$. $\square$

Lemma 3.1.9 provides a bound on $|T_{\mathcal{B}_\Gamma}|$ so we turn our attention to $T^{\mathcal{B}_\Gamma}$ - we immediately have that this is transitive. If $T^{\mathcal{B}_\Gamma}$ is primitive and does not contain the alternating group then we bound $|T^{\mathcal{B}_\Gamma}|$ by the order of the largest such group if $\frac{n}{2} \leq 24$ and $2^{\frac{n}{2}}$ if $\frac{n}{2} > 24$.

Lemma 3.1.10
Let $n \geq 10$ and $\rho = (1,2)(3,4)\cdots(n-1,n)$.

If $T^{\mathcal{B}_\Gamma}$ contains the alternating group then either $T_{(\mathcal{B}_\Gamma)}$ is trivial and $T^{\mathcal{B}_\Gamma} \cong S_{\frac{n}{2}}$ or $T_{(\mathcal{B}_\Gamma)} = \{1,\rho\}$ and $T^{\mathcal{B}_\Gamma} \cong A_{\frac{n}{2}}$. In either case $8|n$ and $N_{S_n}(T)$ is isomorphic to a subgroup of $S_{\frac{n}{2}} \times C_2$.

If we drop the assumption that T is core-free and assume only that $T_{(\mathcal{B}_\Gamma)}$ is core-free then we still have $T_{(\mathcal{B}_\Gamma)} \subseteq \{1,\rho\}$.

Proof: We begin without the assumption that T is core-free. Suppose that $T_{(\mathcal{B}_\Gamma)} \not\subseteq \{1,\rho\}$. Let $1 \neq g \in T_{(\mathcal{B}_\Gamma)}$ be the product of as few transpositions as possible. Without loss of generality $g = (1,2)\cdots(r-1,r)$ for some $r < n$ with $8 \mid r$. As $T^{\mathcal{B}_\Gamma}$ contains the alternating group there is some $h \in T$ with image $(\Gamma_1,\Gamma_2)(\Gamma_{\frac{r}{2}},\Gamma_{\frac{r}{2}+1})$ in $T^{\mathcal{B}_\Gamma}$. This gives $gg^h = (r-1,r)(r+1,r+2)$ so $T_{(\mathcal{B}_\Gamma)}$ is not core-free. Hence $T_{(\mathcal{B}_\Gamma)} \subseteq \{1,\rho\}$.

From here we assume T is core-free.

To show that $N_{S_n}(T)$ is isomorphic to a subgroup of $S_{\frac{n}{2}} \times C_2$, it will be convenient to define

$$S = \langle (2i-1,2i+1,2i+3)(2i,2i+2,2i+4) | i \in \{1,\ldots,\frac{n}{2}-2\}\rangle \cong A_{\frac{n}{2}}$$

We will show that in any case, relabelling if necessary, $S \leq T$ and use this to show that $N_{S_n}(T)$ is isomorphic to a subgroup of $S_{\frac{n}{2}} \times C_2$ at the end.

First suppose $T^{\mathcal{B}_\Gamma} = S_{\frac{n}{2}}$. Recall that we identify T with its image in A_n and that $\mathcal{B}_\Gamma = \{\{2i-1,2i\} | i \in \{1,\ldots,\frac{n}{2}\}\}$. Then there is some $g \in T$ with image (Γ_1,Γ_2) in $T^{\mathcal{B}_\Gamma}$.

We claim that either g acts trivially on each Γ_i for $i > 2$ or g acts nontrivially on all Γ_i for $i > 2$. Suppose otherwise, then without loss of generality g acts trivially on Γ_3 and nontrivially on Γ_4. Fix $h \in T$ with image (Γ_3,Γ_4) in $T^{\mathcal{B}_\Gamma}$. Then $gg^h \in T_{(\mathcal{B}_\Gamma)}$ acts non-trivially on $\{1,\ldots,8\}$ and trivially on $\{9,\ldots,n\}$ contradicting the fact that $T_{(\mathcal{B}_\Gamma)} \subseteq \{1,\rho\}$. Hence the claim holds.

After swapping 3 and 4 if necessary we either have $g^{\{1,2,3,4\}} = (1,3,2,4)$ or $g^{\{1,2,3,4\}} = (1,4)(2,3)$. In the first case $g^2 = (1,2)(3,4)$ and T is not corefree so $g^{\{1,2,3,4\}} = (1,4)(2,3)$. If g acts trivially on each Γ_i for $i > 2$ then $g = (1,4)(2,3)$ so again T is not core-free. Hence $g = (1,4)(2,3)(5,6)\cdots(n-1,n)$. This implies $8|n$. If $T_{(\mathcal{B}_\Gamma)} = \{1,\rho\}$ then $g\rho = (1,3)(2,4)$ contradicting the assumption that T is core-free, so if $T^{\mathcal{B}_\Gamma} = S_{\frac{n}{2}}$ then $T_{(\mathcal{B}_\Gamma)}$ is trivial.

Fix $g_1 = g$. For each $i \in \{1,\ldots,\frac{n}{2}-1\}$ let $g_i \in T$ have image $(\Gamma_i,\Gamma_{i+1}) \in T$. As in the calculation of g, swapping $2i+1$ and $2i+2$ if necessary we have $g_i^{\{2i-1,2i,2i+1,2i+2\}} = (2i-1,2i+2)(2i,2i+1)$ and $g_i^{\Gamma_j} = (2j-1,2j)$ for $j \notin \{i,i+1\}$. This gives $g_{i+1}g_i = (2i-1,2i+1,2i+3)(2i,2i+2,2i+4)$, so $S \leq T$.

Now suppose $T^{\mathcal{B}_\Gamma} = A_{\frac{n}{2}}$. Consider $g \in T$ with image $(\Gamma_1, \Gamma_2, \Gamma_3)$ in $T^{\mathcal{B}_\Gamma}$. Replacing g with g^4 we may assume g has order 3. After swapping 3 and 4 or 5 and 6 as necessary, this means $g = (1,3,5)(2,4,6)$.

Similarly we may find $h_r \in T$ with image $(\Gamma_1, \Gamma_3, \Gamma_r)$ in $T^{\mathcal{B}_\Gamma}$ for each $r > 6$. After swapping $r-1$ and r if necessary we have $h_r = (1,3,r-1)(2,4,r)$ or $h_r = (1,4,r-1)(2,3,r)$. If $h_r = (1,4,r-1)(2,3,r)$ then we have that $gh_r^{-1} = (1,2)(3,5,r-1,4,6,r)$. But then $(gh_r^{-1})^3 = (1,2)(3,4)(5,6)(r-1,r)$ contradicting the fact that $T_{(\mathcal{B}_\Gamma)} \subseteq \{1, \rho\}$. Hence $h_r = (1,3,r-1)(2,4,r)$. Notice that $g, h_8, \ldots, h_n$ fix $\{1,3,\ldots,n-1\}$ and generate $T^{\mathcal{B}_\Gamma}$.

If $T_{(\mathcal{B}_\Gamma)}$ is trivial then T is intransitive. We must therefore have $T_{(\mathcal{B}_\Gamma)} = \{1, (1,2)(3,4)\cdots(n-1,n)\}$ and therefore $8|n$. Notice also that $S = \langle g, h_8, \ldots, h_n\rangle$ so $S \leq T$.

Now, we have $S \leq T$ in each case. In particular S is core-free. In fact S is the unique non-abelian minimal normal subgroup of T so S is characteristic in T and therefore $N_{S_n}(T) \leq N_{S_n}(S)$.

Let $S' = \langle (2i-1, 2i+1)(2i, 2i+2) | i \in \{1, \ldots, \frac{n}{2}-1\}\rangle$. Immediately we have $S' \cong S_{\frac{n}{2}}$ and $S' \leq N_{S_n}(S)$. Let $x \in N_{S_n}(S)$ and fix $s \in S'$ such that $\{2i, 2i-1\}^s = \{2i, 2i-1\}^x$ for $i \in \{1, \ldots, \frac{n}{2}\}$. Then $y = xs^{-1}$ fixes $\{2i, 2i-1\}$ for $i \in \{1, \ldots, \frac{n}{2}\}$. Suppose $y \neq 1$. If $y \neq \rho$ then we may assume, relabelling if necessary, that $y^{\{1,2,3,4,5,6,7,8\}} \in \{(1,2), (1,2)(5,6), (1,2)(3,4)(5,6)\}$. Note that $z = (1,3)(2,4)(5,7)(6,8) \in S$ and, as $y \in N_{S_n}(S)$, we have $z^y z \in S$. Now,

$$z^y \in \{(1,4)(2,3)(5,7)(6,8), (1,4)(2,3)(5,8)(6,7), (1,3)(2,4)(5,8)(6,7)\}$$

which gives

$$z^y z \in \{(1,2)(3,4), (1,2)(3,4)(5,6)(7,8), (5,6)(7,8)\} \subseteq S_{(\mathcal{B}_\Gamma)}$$

Recalling that $S_{(\mathcal{B}_\Gamma)} \leq T_{(B_\Gamma)} \subseteq \{1, \rho\}$ this is a contradiction. Hence $y = \rho$ which is in the centraliser of S'. Hence $N_{S_n}(S) = \langle y\rangle S' \cong S_{\frac{n}{2}} \times C_2$. $\square$

The final case to consider is when $T^{\mathcal{B}_\Gamma}$ is imprimitive. This can only happen if $\frac{n}{2}$ is not prime and $T^{\mathcal{B}_\Gamma}$ must have some minimal block of length $s \neq 1$ properly dividing $\frac{n}{2}$. For each such s we obtain a naive bound

$$T \leq |T_{(\mathcal{B}_\Gamma)}|(s!)^{\frac{n}{2s}} \frac{n}{2s}!$$

Typically Lemma 3.1.9 is sufficient at this point, but we do need to strengthen this slightly in the case $s = \frac{n}{4}$. To this end we give a corollary of Lemma 3.1.10.

Corollary 3.1.11
Let $n \geq 20$. Suppose $T^{\mathcal{B}_\Gamma}$ is imprimitive with minimal block Δ of length $\frac{n}{4}$. Then either $|T^{\mathcal{B}_\Gamma}| \leq 2|P|^2$ for some primitive group P of degree $\frac{n}{4}$ not containing the alternating group or $|T_{(\mathcal{B}_\Gamma)}| \leq 2^{\frac{n}{4}+1}$.

Proof: Let $N = T_{(\mathcal{B}_\Gamma)}$. Relabelling if necessary $\Delta = \{\{1,2\},\ldots,\{\frac{n}{2}-1,\frac{n}{2}\}\}$. In particular $N_{(\{\frac{n}{2}+1,\ldots,n\})} \cong (N_{(\{\frac{n}{2}+1,\ldots,n\})})^{\{1,\ldots,\frac{n}{2}\}}$ is an almost core-free normal subgroup of $(T_\Delta)^{\{1,\ldots,\frac{n}{2}\}}$. As Δ is a minimal block, $(T_\Delta)^\Delta$ must be primitive.

If $(T_\Delta)^\Delta$ does not contain the alternating group then for some primitive P we have $|T^{\mathcal{B}_\Gamma}| \leq |(T_\Delta)^\Delta \wr S_2| = 2|P|^2$.

If however $(T_\Delta)^\Delta$ does contain the alternating group then by Lemma 3.1.10 $|(N_{(\{\frac{n}{2}+1,\ldots,n\})})| \leq 2$ so $|N| = |N_{(\{\frac{n}{2}+1,\ldots,n\})}||N^{\{\frac{n}{2}+1,\ldots,n\}}| \leq 2^{\frac{n}{4}+1}$. □

Case $|\Gamma| = 3$

In this case we note that a Sylow 2-subgroup of $T_{(\mathcal{B}_\Gamma)}$ is a core-free subgroup of $2 \cdot A_{\frac{2n}{3}}$. Using this, Lemma 3.1.9 give us the following result.

Lemma 3.1.12
The following table bounds $T_{(\mathcal{B}_\Gamma)}$ for various values of n. Note that n is divisible by 3 by assumption.

n	$\lvert T_{(\mathcal{B}_\Gamma)}\rvert$
≤ 9	1
≥ 12	$\leq 2^{\frac{n}{3}-3} * 3^{\frac{n}{3}}$
≥ 15	$\leq 2^{\frac{n}{3}-4} * 3^{\frac{n}{3}}$
≥ 27	$\leq 2^{\frac{n}{3}-5} * 3^{\frac{n}{3}}$
≥ 33	$\leq 2^{\frac{n}{3}-6} * 3^{\frac{n}{3}}$

We also need an analogue of Lemma 3.1.10.

Lemma 3.1.13
Let $n \geq 15$. Then $T^{\mathcal{B}_\Gamma}$ does not contain the alternating group.

Proof: Without loss of generality assume T has blocks $\Gamma_i = \{3i-2, 3i-1, 3i\}$ for $i \in \{1,\ldots,\frac{n}{3}\}$.

Suppose $T^{\mathcal{B}_\Gamma}$ contains the alternating group. Then there is some $x \in T$ with image $(\Gamma_1,\Gamma_2,\Gamma_4)$ in $T^{\mathcal{B}_\Gamma}$ and some $y \in T$ with $(\Gamma_1,\Gamma_3,\Gamma_4)$ in $T^{\mathcal{B}_\Gamma}$. Replacing x with x^4 and y with y^4 then relabelling if necessary, we have that x^{Γ_i} and y^{Γ_i} are each of order 1 or 3 for $i > 4$.

This means that $z = (xy)^3$ has image $(\Gamma_1, \Gamma_2)(\Gamma_3, \Gamma_4)$ in $T^{\mathcal{B}_\Gamma}$ and z has order a power of 2. After relabelling if necessary, the only possible values for z are then $(1,4)(2,5)(3,6)(7,10)(8,11)(9,12)$, $(1,4,2,5)(3,6)(7,10)(8,11)(9,12)$ and $(1,4,2,5)(3,6)(7,10,8,11)(9,12)$.

The first two cases immediately imply, by Proposition 3.1.3, that T is not core-free. In the third case $z^2 = (1,2)(4,5)(7,8)(10,11)$. Since $n \geq 15$ there is some $g \in T$ with image $(\Gamma_1, \Gamma_2)(\Gamma_4, \Gamma_5)$ in $T^{\mathcal{B}_\Gamma}$ so, relabelling if necessary, $(z^2(z^2)^g)^3 = (10,11)(13,14)$ again implying that T is not core-free.

Hence $T^{\mathcal{B}_\Gamma}$ does not contain the alternating group. □

We then use the following bounds if $T^{\mathcal{B}_\Gamma}$ is primitive and imprimitive with minimal block of length s respectively. Note that $P(n)$ denotes an upper bound on the order of primitive groups of degree n not containing the alternating group.

$$|T| \leq |T_{(\mathcal{B}_\Gamma)}| P\left(\frac{n}{3}\right)$$
$$|T| \leq |T_{(\mathcal{B}_\Gamma)}| (s!)^{\frac{n}{3s}} \frac{n}{3s}!$$

Case $|\Gamma| = 4$

For $n > 56$ it turns out sufficient to note that T is contained in a subgroup G of S_n isomorphic to $S_4 \wr S_{\frac{n}{4}}$ and that G has a subgroup H isomorphic to $S_2^{\frac{n}{2}}$. By Lemma 3.1.9 $|T \cap H| \leq 2^{\frac{n}{2}-6}$ so $|T| \leq (4!)^{\frac{n}{4}} (\frac{n}{4})!/2^6$.

For $n \leq 56$ we use a brute force method. One can do this by starting with $G \cong S_4 \wr S_{\frac{n}{4}}$, then successively taking maximal subgroups to find those transitive subgroups with minimal block of length 4 which are almost core-free.

Case $|\Gamma| > 4$

Let $\mathcal{B}_\Gamma = \{\Gamma_1, \ldots, \Gamma_r\}$ and note that T_{Γ_i} is core-free with $(T_{\Gamma_i})^{\Gamma_i} \cong (T_{\Gamma_j})^{\Gamma_j}$ for all i, j. Moreover $(T_{\Gamma_i})^{\Gamma_i}$ is primitive and $(T_{(\{1,\ldots,n\}\setminus\Gamma_i)})^{\Gamma_i}$ is core-free in $2 \cdot A_{|\Gamma|}$ and normal in $(T_{\Gamma_i})^{\Gamma_i}$ so $(T_{(\{1,\ldots,n\}\setminus\Gamma_i)})^{\Gamma_i}$ is either trivial or transitive. We first study the case $(T_{\Gamma_i})^{\Gamma_i}$ contains the alternating group.

Lemma 3.1.14
Suppose $G \leq 2 \cdot A_n$ is core-free and acts on $\{1, \ldots, n\}$ with orbits $\Gamma_1, \ldots, \Gamma_r$ each of length $d \geq 5$ with $G^{\Gamma_i} \geq A_d$.

Then we can partition $\{1, \ldots, r\}$ into sets $J_1, \ldots, J_t$ for some t such that for each J_i, G acts diagonally on $\{\Gamma_j | j \in J_i\}$ and $|J_i|$ is even.

In particular $|G| \leq (d!)^{\frac{n}{2d}}$. Moreover $A_d^t \trianglelefteq G$ with each copy of A_d acting non-trivially on the Γ_i in exactly one J_j.

Proof: This is an application of Lemma 4.4 in [1].

Consider $T_1 \times \cdots \times T_r \leq S_n$ with $T_i \cong A_d$ acting non-trivially only on Γ_i. As $G^{\Gamma_i} \geq A_d$, $[G,G]$ is a subdirect product of $T_1 \times \cdots \times T_r$. Lemma 4.4 in [1] implies then that $[G,G] = \prod_{i=1}^t M_i$ where M_i is a full diagonal subgroup of $\prod_{j \in J_i} T_j$ with the J_i partitioning $\{1, \ldots, r\}$.

To see $|J_i|$ is even, consider $g \in M_i$ with g^{Γ_j} a product of two transpositions for $j \in J_i$. Then g is a product of $2|J_i|$ transpositions, so by Lemma 3.1.3 $|J_i|$ is even. □

Corollary 3.1.15

If $(T_{\Gamma_i})^{\Gamma_i}$ contains the alternating group then either

$$|T| \leq |N_{S_n}(T)| \leq (|\Gamma|!)^{\frac{n}{2|\Gamma|}}(\frac{n}{|\Gamma|})!$$

or

$$|N_{S_n}(T)| \leq (\frac{n}{2})!$$

If further $|\Gamma| = \frac{n}{2}$ then $8|n$ and $|T| \leq (\frac{n}{2})!$.

Proof: Denoting $d = |\Gamma|$ we have, by Lemma 3.1.14, that T has a normal subgroup $M \cong M_1 \times \cdots \times M_t$ for some $t \leq \frac{n}{2d}$ with $M_i \cong A_d$. We note that $T \leq N_{S_n}(T)$. As $N_{S_n}(M)$ fixes cycle type of elements in A_d, $N_{S_n}(M)/C_{S_n}(M)$ embeds into $S_d \wr S_t$.

Suppose that $1 \neq g \in C_{S_n}(M)$. Then renumbering if necessary we have that g moves a point in Γ_1 and T_1 acts non-trivially on Γ_1. Since $T_1^g = T_1$ we must have $\Gamma_1^g = \Gamma_i$ for some i on which T_1 acts non-trivially. If $i = 1$ then g^{Γ_1} commutes with $T_1^{\Gamma_1}$ which is impossible. Hence $C_{S_n}(M)$ is determined by its action on $\mathcal{B}_\Gamma$ and has orbits of length $\frac{r}{t}$.

We now consider $N_{S_n}(T)$. This will permute the minimal normal subgroups of T with simple factors isomorphic to A_d. Extend M to $N = M_1 \times \cdots \times M_s$ with $s \geq t$ and $M_i \cong A_d$, the subgroup generated by such minimal normal subgroups. For $i > t$, $M_i \leq C_{S_n}(M)$, so $C_{S_n}(M) \geq A_d^{s-t}$. This has minimal degree $(s-t)d$ so $\frac{n}{d} = |\mathcal{B}_\Gamma| \geq (s-t)d$. Also if $s > t$ then $d|\frac{r}{t}$ and as $n = rd$, $d^2|n$.

Now, $N_{S_n}(T) \leq N_{S_n}(N)$ so $|N_{S_n}(T)/C_{S_n}(T)| \leq |S_d \wr S_s|$. We also have $C_{S_n}(T) \leq C_{S_n}(M)$. Hence we have

$$|N_{S_n}(T)| \leq |S_d \wr S_s||C_{S_n}(M)| \leq (d!)^s s! \left(\frac{r}{t}\right)!^t$$

subject to $\frac{n}{d} \geq (s-t)d$, $\frac{n}{td} \geq 2$ and if $s > t$ then $\frac{r}{t} \geq d$. Assume $s > t$ (recall that this implies $d^2|n$). For fixed t this is maximised by $s = \frac{n}{d^2} + t$ so

$$|N_{S_n}(T)| \leq (d!)^{\frac{n}{d^2}+t} \left(\frac{n}{d^2} + t\right)! \left(\frac{r}{t}\right)!^t$$

which one can check is maximised by $t = \frac{r}{d}$ or $t = 1$. Noting that $n = rd$, $t = \frac{r}{d}$ gives

$$\begin{aligned} |N_{S_n}(T)| &\leq (d!)^{\frac{n}{d^2}+\frac{r}{d}}\left(\frac{n}{d^2}+\frac{r}{d}\right)!(d!)^{\frac{r}{d}} \\ &= (d!)^{\frac{3n}{d^2}}\left(\frac{2n}{d^2}\right)! \end{aligned}$$

Immediately for $d \geq 6$ this implies $|N_{S_n}(T)| \leq (|\Gamma|!)^{\frac{n}{2|\Gamma|}}(\frac{n}{|\Gamma|})!$. The case $d = 5$ can also be checked using Theorem 2. The case $t = 1$ gives

$$|N_{S_n}(T)| \leq (d!)^{\frac{n}{d^2}+1}\left(\frac{n}{d^2}+1\right)!\left(\frac{n}{d}\right)!$$

One can check this is maximised by $d = 5$ so

$$|N_{S_n}(T)| \leq (5!)^{\frac{n}{25}+1}\left(\frac{n}{25}+1\right)!\left(\frac{n}{5}\right)!$$

which one can check is less than $\lfloor\frac{n}{2}\rfloor!$.

If instead $s = t$ then

$$|N_{S_n}(T)| \leq (d!)^t t! \left(\frac{r}{t}\right)!^t$$

One can check that this is maximised by $t = 1$ or $t = \frac{r}{2}$. If $t = 1$ then

$$|N_{S_n}(T)| \leq (d!)\left(\frac{n}{d}\right)!$$

If instead $t = \frac{r}{2}$ then

$$|N_{S_n}(T)| \leq (d!)^{\frac{n}{2d}}\left(\frac{n}{2d}\right)!(2!)^{\frac{n}{2d}} < (d!)^{\frac{n}{2d}}\left(\frac{n}{d}\right)!$$

Now suppose $|\Gamma| = \frac{n}{2}$. If $T_{(\mathcal{B}_\Gamma)} \cong S_{|\Gamma|}$ then it contains an element of the form $(a_1, a_2)(a_3, a_4)$ and T is not core-free. Hence $T_{(\mathcal{B}_\Gamma)} \leq A_{|\Gamma|}$ which gives the bound. So suppose further that $8 \nmid n$.

If $|T^{\mathcal{B}_\Gamma}| = 2$ then either $T \cong A_{\frac{n}{2}} \times S_2$ or $T \cong S_{\frac{n}{2}}$. In either case T contains an element of order 2 which swaps Γ_1 and Γ_2 so, relabelling if necessary, we have $(1, \frac{n}{2}+1)\cdots(\frac{n}{2}, n) \in T$. But this is a product of $\frac{n}{2}$ transpositions and $4 \nmid \frac{n}{2}$ contradicting the assumption T is almost core-free. Hence $T^{\mathcal{B}_\Gamma} = 1$ and $T = T_{(\mathcal{B}_\Gamma)}$ is intransitive contrary to assumption. This completes the proof. $\square$

This leaves the case $(T_{\Gamma_i})^{\Gamma_i}$ does not contain the alternating group. We note that $|\Gamma| \geq 5$ and T imprimitive implies that $n \geq 10$.

If $N_{S_n}(T)$ is primitive then, as $T \trianglelefteq N_{S_n}(T)$, $N_{S_n}(T)$ does not contain A_n so one can check $|N_{S_n}(T)| < \lfloor\frac{n}{2}\rfloor!$ for $n > 16$. If $10 \leq n \leq 16$ then we may bound $|T|$ and $|N_{S_n}(T)|$ by looping over primitive groups not containing the alternating group and finding their largest imprimitive normal subgroups - as T is imprimitive, we may assume n is not prime.

If $N_{S_n}(T)$ is imprimitive with minimal block Δ of length d then T also fixes Δ. Choosing Δ appropriately we may assume $\Gamma \subseteq \Delta$. In particular $(N_{S_n}(T)_\Delta)^\Delta$ does not contain the alternating group and $|N_{S_n}(T)| \leq P^{\frac{n}{d}} \left(\frac{n}{d}\right)!$ where P is an upper bound on the order of a primitive group of degree d. This turns out to be a sufficient bound for $|T|$ for $n > 36$.

For $10 \leq n \leq 36$ note that $|\Gamma|$ divides $|\Delta|$ and $T_D = (T_{(\{1,\ldots,n\}\setminus\Gamma)})^\Gamma$ is either trivial or a transitive core-free subgroup of A_d with $N_{S_{|\Gamma|}}(T_D)$ primitive and not containing A_d. We have $|T_{\mathcal{B}_\Gamma}| \leq |T_D||N_{S_n}(T_D)|^{\frac{n}{|\Gamma|}-1}$ and T fixing both $\mathcal{B}_\Gamma$ and $\mathcal{B}_\Delta$ so T maps into $S_{\frac{d}{|\Gamma|}} \wr S_{\frac{n}{d}}$ with kernel $T_{\mathcal{B}_\Gamma}$. Note that if $|\Gamma|$ is odd then, as $T \leq A_n$, this map cannot be surjective.

If T_D is trivial then

$$|T| \leq \frac{1}{(2, |\Gamma|) - 1} P^{\frac{n}{|\Gamma|}-1} \left(\frac{d}{|\Gamma|}\right)!^{\frac{n}{d}} \left(\frac{n}{d}\right)!$$

where P is an upper bound on the order of primitive groups of degree $|\Gamma|$ not containing $A_{|\Gamma|}$. If T_D is non-trivial then

$$|T| \leq \frac{1}{(2, |\Gamma| - 1)} |T_D|(|N_{S_{|\Gamma|}}(T_D)|)^{\frac{n}{|\Gamma|}-1} \left(\frac{d}{|\Gamma|}\right)!^{\frac{n}{d}} \left(\frac{n}{d}\right)!$$

See the `buildTCFs` function in Appendix A for example MAGMA code which implements the above bounds for constructing TCFs(n). See also the `PrimBound` function which returns an upper bound on the order of a primitive group of degree n which does not contain the alternating group.

Building FCFs(n)

The method we describe here constructs FCFs(n) and ACFs(n) simultaneously as the construction of FCFs(n) will use ACFs(i) for some $i < n$.

In order to obtain sufficiently tight bounds on the order of core-free subgroups of $2\cdot A_n$ with fixed orbit length in practical time we need the following somewhat cumbersome definition and lemma.

Definition 3.1.3

Fix $s \in \mathbb{N}$ and d the largest proper divisor of s and let $M \leq S_s$. We say M is close to S_s if one of the following hold:

- *$A_s \leq M$.*
- *M is imprimitive with a minimal block Δ of length d and $A_d \leq (M_\Delta)^\Delta$.*

Lemma 3.1.16
Suppose $F \leq A_n$ is core-free with orbits $\Gamma_1, \ldots, \Gamma_r$ all the same length $s \geq 5$ then we are in at least one of the following cases. The conditions give restrictions on F and a bound (ϕ, ψ) means $|F| \leq \phi$ and $|N_{S_n}(F)| \leq \psi$ - we say $(|F|, |N_{S_n}(F)|)$ is bounded by (ϕ, ψ). Where necessary we write ψ in terms of ϕ.

Case	Conditions	Bounds (ϕ, ψ)
1	$2 \mid r$	$\left(\frac{1}{2}(s!)^{\left(\frac{r}{2}\right)} \,,\, (s!)^{\left(\frac{r}{2}\right)} r! \right)$
2	$2 \mid r$, $(*)$	$\left((s!)^{\left(\frac{r}{2}-2\right)}\|F_0\|\|N_{S_s}(F_0)\| \,,\, 2(s!)^{\left(\frac{r}{2}-2\right)}\left(\frac{r}{2}-2\right)!\|N_{S_s}(F_0)\|^2 \right)$
3	$2 \mid r$	$\left((s!)^{\left(\frac{r}{2}-2\right)}\left[(d!)^{\frac{s}{2d}}\left(\frac{s}{d}\right)!\right]^2 \,,\, 2\left(\frac{r}{2}-2\right)!\phi \right)$
4	$2 \mid r$	$\left((s!)^{\left(\frac{r}{2}-2\right)}\|M\|^2 \,,\, 2(s!)^{\left(\frac{r}{2}-2\right)}\left(\frac{r}{2}-2\right)!\|M\|^2 \right)$
5	$2 \nmid r$, $(*)$	$\left((s!)^{\left(\frac{r-1}{2}\right)}\|F_0\| \,,\, (s!)^{\left(\frac{r-1}{2}\right)}\left(\frac{r-1}{2}\right)!\|N_{S_s}(F_0)\| \right)$
6	$2 \nmid r$	$\left((s!)^{\left(\frac{r-1}{2}\right)}(d!)^{\frac{s}{2d}}\left(\frac{s}{d}\right)! \,,\, (s!)^{\left(\frac{r-1}{2}\right)}\left(\frac{r-1}{2}\right)!(d!)^{\frac{s}{2d}}\left(\frac{s}{d}\right)! \right)$
7	$2 \nmid r$	$\left((s!)^{\left(\frac{r-1}{2}\right)} \,,\, (s!)^{\left(\frac{r-1}{2}\right)}\left(\frac{r-1}{2}\right)!\|M\| \right)$
8	$2 \mid \left(\frac{n}{d}\right)$	$\left((d!)^{\frac{n}{2d}}\left[\left(\frac{s}{d}\right)!\right]^{r-1} \,,\, (d!)^{\frac{n}{2d}}\left[\left(\frac{s}{d}\right)!\right]^{r} r! \right)$
9	$2 \nmid \left(\frac{n}{d}\right)$, $(*)$	$\left((d!)^{\left(\frac{n-s}{2d}\right)}\left[\left(\frac{s}{d}\right)!\right]^{r-1}\|F_0\| \,,\, \left(\frac{r-1}{2}\right)!\|N_{S_s}(F_0)\|\phi/\|F_0\| \right)$
10	$2 \nmid \left(\frac{n}{d}\right)$	$\left((d!)^{\left(\frac{n-s}{2d}\right)}\left[\left(\frac{s}{d}\right)!\right]^{r-1} \,,\, \left(\frac{r-1}{2}\right)!\|M\|\phi \right)$
11	$(*)$	$\left(\|F_0\|\|N_{S_s}(F_0)\|^{r-1} \,,\, \|N_{S_s}(F_0)\|^{r} r! \right)$
12		$\left(\|M\|^{r-1} \,,\, \|M\|^{r} r! \right)$

where F_0, d and M are defined as follows:

- *d is the largest proper divisor of s.*
- *M is a transitive subgroup of S_s of largest order such that M is not close to S_s.*
- *Denote $F_i = F_{(\cup_{j \neq i} \Gamma_j)}$ for $1 \leq i \leq r$ and identify F_i as a subgroup of S_s through its action on Γ_i. If some F_i is non-trivial then denote by F_0 the non-trivial F_i with largest normaliser in S_s. The condition $(*)$ is that some F_i is non-trivial.*

Proof: We continue to identify F_i with its action on Γ_i. As F^{Γ_i} is transitive, the orbits of F_i form a block system of F^{Γ_i}. In particular F_i is core-free of fixed orbit length and $F^{\Gamma_i} \leq N_{S_s}(F_i)$.

We order the Γ_i such that F^{Γ_i} contains the alternating group if and only if $1 \leq i \leq t_0$ and F^{Γ_i} is imprimitive and close to S_s if and only if $t_0+1 \leq i \leq t_0+t_1$. Note that this means F^{Γ_i} is close to S_s if and only if $1 \leq i \leq t_1$.

Bounds on the first t_1 components

It is easily seen that $F_{(\cup_{i=t_0+1}^{r}\Gamma_i)}$, identified with its action on $\cup_{i=1}^{t_0}\Gamma_i$, satisfies the conditions of Lemma 3.1.14 and that therefore t_0 is even and

$$|F^{\cup_{i=1}^{t_0}\Gamma_i}| \leq (s!)^{\frac{t_0}{2}}$$

$$|N_{S_{st_0}}(F^{\cup_{i=1}^{t_0}\Gamma_i})| \leq (s!)^{\frac{t_0}{2}} t_0!$$

Partition $\cup_{i=t_0+1}^{t_1}\Gamma_i$ into blocks $\Delta_1, \ldots, \Delta_k$ of F^{Γ_i} of length d for $i = t_0+1, \ldots, t_1$ and let $\Omega = \{\Delta_i | i \in \{1, \ldots, k\}\}$. Let

$$\overline{F} = (F_{\cup_{i \notin \{t_0+1,\ldots,t_1\}}\Gamma_i})^{\cup_{i=t_0+1}^{t_1}\Gamma_i}$$

Then either $s \in \{6, 8, 9\}$ or $\overline{F}_\Omega$ satisfies Lemma 3.1.14. If $s \in \{6, 8, 9\}$ then one can check that $|F^{\Gamma_i}| < |M|$. If $\overline{F}_\Omega$ satisfies Lemma 3.1.14 then $\frac{st_1}{d}$ is even and

$$|\overline{F}| \leq |F^{\cup_{i=t_0+1}^{t_1}\Gamma_i}| \leq (d!)^{\frac{st_1}{2d}} \left[\left(\frac{s}{d}\right)!\right]^{t_1}$$

In either case

$$|F^{\cup_{i=t_0+1}^{t_1}\Gamma_i}| \leq \max\left(|M|^{t_1}, (d!)^{\frac{st_1}{2d}} \left[\left(\frac{s}{d}\right)!\right]^{t_1}\right)$$

It will also be important to note that

$$|F^{\cup_{i=t_0+2}^{t_1}\Gamma_i}| \leq \max\left(|M|^{t_1-1}, (d!)^{\frac{st_1}{2d}} \left[\left(\frac{s}{d}\right)!\right]^{t_1-1}\right)$$

Full bounds

We now have all the information we need to obtain the above bounds. To do this clearly we pair the orbits of F, $(\Gamma_1, \Gamma_2), (\Gamma_3, \Gamma_4), \ldots$ with Γ_r left unpaired if r is odd. Due to our ordering of the orbits, $F^{\Gamma_{2i-1}}$ contains the alternating group if and only if $F^{\Gamma_{2i}}$ contains the alternating group. Also if $2 \nmid \left(\frac{s}{d}\right)$ then t_1 is even so we have that $F^{\Gamma_{2i-1}}$ is close to S_s if and only if $F^{\Gamma_{2i}}$ is.

In bounding (ϕ, ψ) we want to know which of the following is largest:

1. $(s!)^{\frac{1}{2}}$
2. $|N_{S_s}(F_0)|$
3. $(d!)^{\frac{s}{2d}} \left(\frac{s}{d}\right)!$
4. $|M|$

We bound (ϕ, ψ) then as follows:

Case: $t_0 = r$

By Lemma 3.1.14, $2 \mid r$ and F embeds into $(S_s)^{\frac{r}{2}}$. Also $F \leq A_n$ so

$$|F| \leq \frac{1}{2}(s!)^{\frac{r}{2}}$$

It is easy to check that $N_{S_n}(F)$ preserves the partion of $\{1, \ldots, n\}$ defined by the orbits of F and, using Lemma 3.1.14, that the subgroup of $N_{S_n}(F)$ which fix the orbits of F also embeds into $(S_s)^{\frac{r}{2}}$. Therefore

$$|N_{S_n}(F)| \leq (s!)^{\frac{r}{2}} r!$$

This gives us case **1** in the statement of the Lemma.

Case: $(s!)^{\frac{1}{2}}$ **is largest**

The case $t_0 = r$ has been dealt with so we suppose that F^{Γ_r} does not contain the alternating group. We consider $|F| = |F^{\cup_{i=1}^{r-2}\Gamma_i}||F_{\left(\cup_{i=1}^{r-2}\Gamma_i\right)}|$ if r is even and $|F| = |F^{\cup_{i=1}^{r-1}\Gamma_i}||F_{\left(\cup_{i=1}^{r-1}\Gamma_i\right)}|$ if r is odd.

If r is even then $|F^{\cup_{i=1}^{r-2}\Gamma_i}| \leq (s!)^{(\frac{r}{2}-2)}$. Bounding $|F_{\left(\cup_{i=1}^{r-2}\Gamma_i\right)}|$ then gives case **2**, **3** or **4** in the statement of the Lemma as follows. We know $F^{\Gamma_{r-1}}$ and F^{Γ_r} do not contain the alternating group so we consider which of $|N_{S_s}(F_0)|$, $(d!)^{\frac{s}{2d}}\left(\frac{s}{d}\right)!$ or $|M|$ is largest. If $|M|$ or $(d!)^{\frac{s}{2d}}\left(\frac{s}{d}\right)!$ is largest or $F_{\Gamma_{r-1}}$ and F_{Γ_r} are trivial then

$$|F_{\left(\cup_{i=1}^{r-2}\Gamma_i\right)}| \leq |N_{S_{2s}}(F_{\left(\cup_{i=1}^{r-2}\Gamma_i\right)})| \leq \max\left(|M|, (d!)^{\frac{s}{2d}}\left(\frac{s}{d}\right)!\right)^2$$

giving case **3** or **4** in the statement of the Lemma. If $|N_{S_s}(F_0)|$ is largest and at least one of $F_{\Gamma_{r-1}}$ and F_{Γ_r} is non-trivial then

$$|F_{\left(\cup_{i=1}^{r-2}\Gamma_i\right)}| \leq |F_0||N_{S_s}(F_0)|$$

$$|N_{S_{2s}}(F_{\left(\cup_{i=1}^{r-2}\Gamma_i\right)})| \leq |N_{S_s}(F_0)|^2$$

giving case **2** in the statement of the Lemma.

If r is odd then $|F^{\cup_{i=1}^{r-1}\Gamma_i}| \leq (s!)^{\frac{r-1}{2}}$. Bounding $|F_{\left(\cup_{i=1}^{r-1}\Gamma_i\right)}|$ then gives case **5**, **6** or **7** in the statement of the Lemma.

Case: F_i **is non-trivial for all** i

Reordering if necessary we may assume that $|F_1| \leq |F_i|$ for all i. Then

$$|F| \leq |F_1| \prod_{i=2}^{r} |F^{\Gamma_i}| \leq |F_0||N_{S_s}(F_0)|^{r-1}$$

$$|N_{S_n}(F)| \leq |N_{S_s}(F_0)|^r$$

which gives case **11** in the statement of the Lemma.

Case: $(d!)^{\frac{s}{2d}}\left(\frac{s}{d}\right)!$ is largest

The case F_i is non-trivial for all i has been dealt with so we may assume F_1 is trivial. The case $t_0 = r$ has also been dealt with so we may assume F^{Γ_r} does not contain the alternating group. If $\frac{n}{d}$ is even then our bounds on the first t_1 components and the bound

$$|F| \leq |F_1||F^{\cup_{i=2}^{r}\Gamma_i}|$$

gives us case **8**.

If $\frac{n}{d}$ is odd and all F_i are trivial then $|F^{\Gamma_r}| \leq |M|$ so the bound

$$|F| \leq |F_r||F^{\cup_{i=1}^{r-1}\Gamma_i}|$$

gives us case **10**.

If $\frac{n}{d}$ is odd and some F_i is non-trivial then reordering if necessary we may assume that F_r is non-trivial. In this case the bound

$$|F| \leq |F_r||F^{\cup_{i=1}^{r-1}\Gamma_i}|$$

gives us case **9**.

Case: $|N_{S_s}(F_0)|$ is largest

The bound $|F| \leq |F_1| \prod_{i=2}^{r} |F^{\Gamma_i}|$ gives us case **11**.

Case: $|M|$ is largest

The case F_i is non-trivial for all i has been dealt with so we may assume F_1 is trivial. The bound $|F| \leq |F_1| \prod_{i=2}^{r} |F^{\Gamma_i}|$ then gives us case **12**. □

This allows us to construct FCFs(n) inductively. For small n however, these bounds are insufficient for $s = 2, 3$, so we use brute force methods. For $s = 2$ notice that F must be an elementary abelian subgroup of a Sylow 2-subgroup of A_n so we loop over such subgroups. For $s = 3$ notice that a Sylow 3-subgroup P of F must be an elementary abelian subgroup of a Sylow 3-subgroup of A_n. Looping over such P, a Sylow 2-subgroup of F normalises P, so we loop over the Sylow 2-subgroups of the normaliser of P in S_n. See functions `BruteFCFs2` and `BruteFCFs3` in Appendix A which implement these brute force methods.

Building ACFs(n)

Suppose $G \leq 2 \cdot A_n$ is core-free and suppose a shortest orbit of G has length s. Let Γ be the union of orbits of G of length s and $\Delta = \{1, \ldots, n\} \setminus \Gamma$. We then have $|G| \leq |G_{(\Delta)}||G^{\Delta}|$ and $|G| \leq |G_{(\Gamma)}||G^{\Gamma}|$ which gives

$$|G| \leq \min(|G_{(\Delta)}||G^{\Delta}|, |G_{(\Gamma)}||G^{\Gamma}|)$$

where notably $G_{(\Gamma)}$ can be identified as a core-free subgroup of $2 \cdot A_{n-|\Gamma|}$ with $G^{\Delta} \leq N_{S_{n-|\Gamma|}}(G_{(\Gamma)})$ and $G_{(\Delta)}$ can be identified as a core-free subgroup of $2 \cdot A_{|\Gamma|}$ with fixed orbit length and $G^{\Gamma} \leq N_{S_{|\Gamma|}}(G_{(\Delta)})$. Hence we may proceed inductively. We do so conditioning on $|\Gamma|$. If $|\Gamma| = n$ then G has fixed orbit length, so we initialise $\mathrm{ACFs}(n) = \mathrm{TCFs}(n)$ and loop over $1 \leq |\Gamma| < n$.

See functions `buildFCFs` and `buildACFs` in Appendix A which construct $\mathrm{FCFs}(n)$ and $\mathrm{ACFs}(n)$.

Optimisation and Results

As given above, the size of these lists builds up rapidly. We can dramatically reduce the lengths of these lists by removing redundant elements. That is if $(a, b, c), (d, e, f) \in x\mathrm{CFs}(n)$ with $a \leq d$, $b \leq e$ and $c \leq f$ then we may remove (a, b, c) and the required properties of $x\mathrm{CFs}(n)$ still hold - in this case we call (a, b, c) redundant. This can be done in several ways; see functions `CFSortReduce` and `CFSecondReduce` in Appendix A which achieve this and leave the list sorted in a way favoured by the author. The author found it necessary to check that (a, b, c) is not redundant before adding it to $\mathrm{ACFs}(n)$ in order for the algorithm to run in practical time.

This algorithm has been used to bound the size of a core-free subgroup of $2 \cdot A_n$ for $n \leq 850$ as given in the following table. The bound is sharp for $n \notin \{16, 21\}$, but a maximal core-free subgroup can be found in this case. In all cases we give the structure of some maximal core-free subgroup. To save space, we do not write $\mu(2 \cdot A_n)$ here - see the table in section 1.4.2 for a full list of $\mu(2 \cdot A_n)$ for $n \geq 5$.

n	bound	core-free subgroup
1	1	1
2	1	1
3	3	3
4	3	3
5	5	5
6	9	3^2
7	21	7.3
8	168	$\mathrm{PSL}(2,7)$
9	1512	$\mathrm{PSL}(2,8).3$
10	1512	$\mathrm{PSL}(2,8).3$
11	7920	M_{11}
12	7920	M_{11}
13	7920	M_{11}
14	23760	$M_{11} \times 3$
15	23760	$M_{11} \times 3$
16	56448	$\mathrm{PSL}(2,7)^2.2$
17	245016	$\mathrm{PSL}(2,7) \times \mathrm{PSL}(2,8).3$
18	2286144	$(\mathrm{PSL}(2,8).3)^2$
19	2286144	$(\mathrm{PSL}(2,8).3)^2$
20	11975040	$M_{11} \times \mathrm{PSL}(2,8).3$
21	11975040	$M_{11} \times \mathrm{PSL}(2,8).3$
22	62726400	M_{11}^2
23	62726400	M_{11}^2
24	479001600	$A_{12} \times 2$
25	479001600	$A_{12} \times 2$
26	3113510400	A_{13}
27	10369949184	$(\mathrm{PSL}(2,8).3) \wr 3$
≥ 28, $\not\equiv 0,1 \bmod 8$	$\lfloor \frac{n}{2} \rfloor!/2$	$A_{\lfloor \frac{n}{2} \rfloor}$
≥ 28, $\equiv 0,1 \bmod 8$	$\lfloor \frac{n}{2} \rfloor!$	$A_{\lfloor \frac{n}{2} \rfloor} \times 2$

The function `runTAFs` in Appendix A is example code which runs this algorithm. This function also uses functions `SaveCFs` and `LoadCFs`.

3.1.2 Main Result and Proof

Recall that $[x_1, \ldots, x_d]$ denotes an element in the preimage of $(x_1, \ldots, x_d)$. It turns out that B_n (see Proposition 3.1.5) is almost the best choice for sufficiently large n:

Theorem 3.1.17
Fix $n \geq 28$ and set $k = \lfloor \frac{n}{2} \rfloor$. Define $B_n = \langle t_1 t_{k+1}, t_2 t_{k+2}, \ldots, t_k t_{2k} \rangle$.

If $4|k$ then $\langle B_n, x \rangle \cong A_k \times C_2$, where $x = [1, k+1][2, k+2] \cdots [k, 2k]$, is a largest core-free subgroup of $2 \cdot A_n$. Otherwise B_n is a largest core-free subgroup of $2 \cdot A_n$.

It is worth noting that if $4|k$ then it is possible to construct a core-free subgroup of $2 \cdot A_n$ isomorphic to S_k.

We know B_n is core-free and the fact that $\langle B_n, x \rangle$ is core-free follows from the easy to prove result that $t_i^x = t_{i+k}$ for $i = 1, \ldots, k$ and Proposition 3.1.3.

To show that these are largest core-free subgroups, we first assume a largest core-free subgroup is transitive and therefore imprimitive (see Corollary 3.1.6), then we allow a largest core-free subgroup to be intransitive.

Transitive Case

We show in this section that, for $n \geq 28$, a transitive core-free subgroup K has size at most $|B_n|$ unless $4|k$ and $|K| = |\langle B_n, x \rangle|$ as in Theorem 3.1.17. Using the above algorithm this has been checked for $n \leq 850$ so assume $n > 850$.

We use the following Lemma throughout without further reference.

Lemma 3.1.18
An imprimitive subgroup K of S_n with block Γ embeds into $(K_\Gamma)^\Gamma \wr K^{\mathcal{B}_\Gamma}$.

Proof: For example [25] (corollary 12.3). □

Fix a core-free subgroup K, assume K is transitive and $|K| > |B_n|$. By Lemma 3.1.6 K is imprimitive. Fix a minimal block Γ of K. Letting $r = |\Gamma|$, we deal with $r = 2$ and $r \neq 2$ separately.

$r \neq 2$

Lemma 3.1.19
$r \geq 5$ and $(K_\Gamma)^\Gamma \geq A_r$.

Proof: Recall that we assume $n > 850$.

For $r = 3$ we have $3|n$ and, by Lemma 3.1.18, $|K| \leq 6^{\frac{n}{3}} \left(\frac{n}{3}\right)!$. One can check that this is less than $|B_n|$.

For $r = 4$ we have $4|n$ and, by Lemma 3.1.18, $|K| \leq 24^{\frac{n}{4}} \left(\frac{n}{4}\right)!$. One can check that this is less than $|B_n|$.

So $r \geq 5$. As Γ is a minimal block, $(K_\Gamma)^\Gamma$ is primitive. If $(K_\Gamma)^\Gamma \not\geq A_r$ then $|(K_\Gamma)^\Gamma| < 3^r$, so by Lemma 3.1.18

$$|K| \leq 3^n \left(\frac{n}{r}\right)!$$

One can check, using $r \geq 5$, that this is less than $|B_n|$. This completes the proof. $\square$

If $K_{\mathcal{B}_\Gamma}$ is trivial then $|K| = |K^{\mathcal{B}_\Gamma}| < |B_n|$ so $(K_{\mathcal{B}_\Gamma})^\Gamma$ is a non-trivial normal subgroup of $(K_\Gamma)^\Gamma \geq A_r$. By Lemma 3.1.14 we may therefore partition the orbits of $K_{\mathcal{B}_\Gamma}$ into sets of orbits on which $K_{\mathcal{B}_\Gamma}$ acts diagonally. Since K is transitive, such a set forms a block of $K^{\mathcal{B}_\Gamma}$. Lemma 3.1.14 also tells us that these sets have even length, so n is even.

Let $\Delta_1, \ldots, \Delta_t$ form a block system for $K^{\mathcal{B}_\Gamma}$, we can embed $K^{\mathcal{B}_\Gamma}$ into $S_s \wr S_t$, where $s = |\Delta_i|$. Noting that $t = \frac{n}{rs}$ we have:

$$\begin{aligned}
\log(|K|) &\leq \log\left((r!s!)^{\frac{n}{rs}} \left(\tfrac{n}{rs}\right)!\right) \\
&< f(n,s,r) \\
&= \left(\tfrac{n}{rs} + \tfrac{1}{2}\right)\log(n) + \left(\tfrac{n}{s} - \tfrac{n}{2rs} - \tfrac{1}{2}\right)\log(r) + \left(\tfrac{n}{r} - \tfrac{n}{2rs} - \tfrac{1}{2}\right)\log(s) \\
&\quad -\tfrac{n}{rs} - \tfrac{n}{r} - \tfrac{n}{s} + \left(\tfrac{n}{rs} + \tfrac{1}{2}\right)\log(2\pi) + \tfrac{n}{12r^2s} + \tfrac{n}{12rs^2} + \tfrac{rs}{12n}
\end{aligned}$$

where the second inequality is an application of Theorem 3.1.2.

Lemma 3.1.20
$|K| < |B_n|$ unless $s = 2$, $r = \frac{n}{2}$.

Proof: We exclude the case $s = 2$, $r = \frac{n}{2}$ and maximise $f(n,s,r)$ showing it is less than $\log(|B_n|)$ thereby proving $|K| < |B_n|$ unless $s = 2$, $r = \frac{n}{2}$. Note that $r = \frac{n}{2}$ implies $s = 2$ so we assume for contradiction that $r \leq \frac{n}{3}$.

Fix $r = r_0$ and denote $t = \frac{n}{sr_0}$, so maximising f over s is equivalent to maximising f over t. Rewriting and differentiating, using $1 \leq t \leq \frac{n}{2r_0}$ and $2 \leq r_0 \leq \frac{n}{3}$ (this looser bound will allow us to apply symmetry and obtain the same results for s), we obtain:

$$\begin{aligned}
f(n,s,r_0) &= \left(\tfrac{n}{r_0} + \tfrac{t}{2}\right)\log(n) + \left(-\tfrac{n}{r_0} + r_0 t\right)\log(r_0) + \left(-\tfrac{n}{r_0} + \tfrac{t}{2} + \tfrac{1}{2}\right)\log(t) \\
&\quad -t - \tfrac{n}{r_0} - r_0 t + \left(t + \tfrac{1}{2}\right)\log(2\pi) + \tfrac{t}{12r_0} + \tfrac{t^2 r_0}{12n} + \tfrac{1}{12t} \\
\tfrac{\partial f}{\partial t}(n,s,r_0) &= \tfrac{r_0}{6n}t + \tfrac{1}{2}\log(t) + \left(\tfrac{1}{2} - \tfrac{n}{r_0}\right)\tfrac{1}{t} - \tfrac{1}{12t^2} \\
&\quad +\tfrac{1}{2}\log(n) + r_0\log(r_0) - r_0 + \log(2\pi) - \tfrac{1}{2} + \tfrac{1}{12r_0} \\
\tfrac{\partial^2 f}{\partial t^2}(n,s,r_0) &= \tfrac{r_0}{6n} + \tfrac{1}{2t} - \left(\tfrac{1}{2} - \tfrac{n}{r_0}\right)\tfrac{1}{t^2} + \tfrac{1}{6t^3} \\
&\geq \tfrac{r_0}{6n} + \tfrac{r_0}{n} - \tfrac{1}{2} + \tfrac{n}{r_0} + \tfrac{4r_0^3}{3n^3} > 0
\end{aligned}$$

In particular, as t increases f begins decreasing with respect to t, reaches a minimum, then increases with respect to t. To maximise f we may therefore take s maximal (so $s = \frac{n}{r_0}$) or s minimal (so $s = 2$).

By symmetry, if we fix $s = s_0$ then we may take r maximal ($r = \frac{n}{s_0}$) or r minimal ($r = 5$).

Case: $r \geq \sqrt{n}$ **or** $s \geq \sqrt{n}$

Suppose $r \geq \sqrt{n}$. This gives $1 \leq t \leq \frac{n}{r} \leq \sqrt{n}$. Using this, and recalling $n > 850$, one can check that

$$\frac{\partial f}{\partial t}(n,s,r_0) \geq \frac{1}{2}\sqrt{n}\log(n) - 2\sqrt{n} + \frac{1}{2}\log(n) + \log(2\pi) - \frac{7}{12} + \frac{2}{3\sqrt{n}} + \frac{1}{6n} > 0$$

This means $f(n,s,r) \leq f(n,2,r)$ with equality if and only if $s = 2$, so in maximising $f(n,s,r)$ we may assume $s = 2$. We will deal with r minimal in the case $r < \sqrt{n}$ so taking r maximal we obtain $f(n,s,r) \leq f(n,2,\frac{n}{3})$ which is less than $\log(|B_n|)$ for even $n > 12$. So for maximal f we have $r < \sqrt{n}$.

A similar argument gives $s < \sqrt{n}$.

Case: $r < \sqrt{n}$ **and** $s < \sqrt{n}$

If $s = 2$ then

$$\begin{aligned}
f(n,2,r) &< \left(\tfrac{7n}{20} - \tfrac{\sqrt{n}}{8} + \tfrac{1}{4}\right)\log(n) + \left(\tfrac{n}{5} - \tfrac{\sqrt{n}}{4} - \tfrac{1}{2}\right)\log(2) \\
&\quad -\tfrac{3\sqrt{n}}{2} - \tfrac{n}{2} + \left(\tfrac{n}{10} + \tfrac{1}{2}\right)\log(2\pi) + \tfrac{n}{600} + \tfrac{n}{240} + \tfrac{1}{6\sqrt{n}}
\end{aligned}$$

which is less then $\log(|B_n|)$ for all n. Thus s maximal, so $s = n/r > \sqrt{n}$ contrary to assumption. Hence $|K| < |B_n|$ unless $s = 2$, $r = \frac{n}{2}$. $\square$

We are left then with the case $r = \frac{n}{2}$. Applying Corollary 3.1.15 then gives us the result:

Theorem 3.1.21
For $n \geq 28$, let K a be core-free subgroup of $2 \cdot A_n$. If the natural action of K on $\{1, \ldots, n\}$ is transitive imprimitive with minimal block of size $r > 2$ then either $|K| < |B_n|$ or $8|n$ and $|K| = |\langle B_n, x\rangle|$ (with B_n, x as described in Theorem 3.1.17).

This completes the case $r \neq 2$.

$r = 2$

Theorem 3.1.22
For $n > 28$, let K be a core-free subgroup of $2 \cdot A_n$. If the natural action of K on $\{1, \ldots, n\}$ is transitive imprimitive with minimal block of size $r = 2$ then either $|K| < |B_n|$ or $8 \mid n$ and $|K| = |\langle B_n, x\rangle|$ (with B_n, x as described in Theorem 3.1.17).

Proof: Suppose $|K| \geq |B_n| = (\frac{n}{2})!/2$. Without loss of generality fix a minimal block system, $\mathcal{B}_\Gamma = \{\Gamma_i | i = 1, \ldots, n/2\}$, of K with $\Gamma_i = \{2i-1, 2i\}$.

We first suppose $K_{(\mathcal{B}_\Gamma)}$ is trivial then $K \cong K^{\mathcal{B}_\Gamma} \leq S_{n/2}$. If $|K| = |B_n|$ then $K \cong A_{n/2}$. Consider the elements $\tau_{i,j,k}$ of K which map to $(i,j,k) \in A_{n/2}$ under this isomorphism (that is $\Gamma_i^{\tau_{i,j,k}} = \Gamma_j$, $\Gamma_j^{\tau_{i,j,k}} = \Gamma_k$, $\Gamma_k^{\tau_{i,j,k}} = \Gamma_i$). Since $\tau_{i,j,k}^3 = 1$ we must have that $\tau_{i,j,k}$ acts trivially on Γ_r for $r \notin \{i,j,k\}$. Swapping $3, 4$ and $5, 6$ if necessary $\tau_{1,2,3} = [1,3,5][2,4,6]$.

We show that we may take $\tau_{i,i+1,i+2} = [2i-1, 2i+1, 2i+3][2i, 2i+2, 2i+4]$. Fix $\tau_{j,j+1,j+2}$ for $j < i$. We may swap $2i+3, 2i+4$ without affecting $\tau_{j,j+1,j+2}$ for $j < i$. We can therefore take $\tau_{i,i+1,i+2} = [2i-1, x, 2i+3][2i, y, 2i+4]$ where $\{x, y\} = \{2i+1, 2i+2\}$. If $\tau_{i,i+1,i+2} = [2i-1, 2i+2, 2i+3][2i, 2i+1, 2i+4]$ then $\tau_{i-1,i,i+1}\tau_{i,i+1,i+2} = [2i-3, 2i+2, 2i-2, 2i+1][2i-1, 2i+4, 2i, 2i+3]$ so $1 \neq (\tau_{i-1,i,i+1}\tau_{i,i+1,i+2})^2 \in K_{(\mathcal{B}_\Gamma)}$ contrary to assumption. Hence we have $\tau_{i,i+1,i+2} = [2i-1, 2i+1, 2i+3][2i, 2i+2, 2i+4]$. Since these $\tau_{i,i+1,i+2}$ generate K and fix $\{2, 4, \ldots, n\}$ setwise we dont have K transitive, contrary to assumption. Hence $|K| > |B_n|$.

Since $|K| > |B_n|$ and $K \cong K^{\mathcal{B}_\Gamma} \leq S_{n/2}$ we have $K \cong S_{n/2}$. So there is some $g \in K$ such that $\Gamma_1^g = \Gamma_2$ and $\Gamma_i^g = \Gamma_i$ for $i > 2$. Fix $i, j > 2$, if g acts trivially on Γ_i then, using 3-transitivity of $A_{n/2}$ for $n \geq 10$, fix $h \in A_{n/2}$ which fixes Γ_1, Γ_2 and maps Γ_i to Γ_j then g^h acts trivially on Γ_j, but also g^h has the same image in $K^{\mathcal{B}_\Gamma}$ as g so $g = g^h$. Therefore g either acts non-trivially on all Γ_i for $i \neq 1, 2$ or acts trivially on all Γ_i for $i \neq 1, 2$. After swapping $3, 4$ if necessary, g acts on $\{1, 2, 3, 4\}$ by $(1, 3, 2, 4)$ or by $(1, 3)(2, 4)$. In the first case, $g^2 = [1,2][3,4]$ so $g^4 = z$. In the second, if $g = [1,3][2,4]$ then $g^2 = z$ so $g = [1,3][2,4][5,6]\cdots[n-1,n]$ which gives $g^2 = 1$ if and only if $8|n$, in which case $|K| = |\langle H, x\rangle|$ as required.

We are left with the case $K_{(\mathcal{B}_\Gamma)}$ is non-trivial. Assume first that there exists $1 \neq g \in K_{(\mathcal{B}_\Gamma)}$ with $g \neq [1,2][3,4]\cdots[n-1,n]$ - that is g fixes some Γ_i pointwise. By Proposition 3.1.3, g acts non-trivially on at least four Γ_i's so without loss of generality assume g acts non-trivially on $\Gamma_1, \dots, \Gamma_4$ and trivially on Γ_5.

If $K^{\mathcal{B}_\Gamma}$ is primitive then either $|K| \leq |K_{(\mathcal{B}_\Gamma)}||K^{\mathcal{B}_\Gamma}| \leq 2^{n/2}3^{n/2}$ which is less than $(\frac{n}{2})!/2$, or $K^{\mathcal{B}_\Gamma} \geq A_{n/2}$. So there is some $h \in K$ with image $(2,3)(4,5)$ in $K^{\mathcal{B}_\Gamma}$. This gives $gg^h = [7,8][9,10]$ contrary to Proposition 3.1.3.

If $K^{\mathcal{B}_\Gamma}$ is imprimitive then

$$K \hookrightarrow S_2 \wr (S_s \wr S_{n/2s}) \cong (S_2)^{n/2} \rtimes ((S_s)^{n/s} \rtimes S_{n/2s})$$

where s is the size of the minimal block Δ of $K^{\mathcal{B}_\Gamma}$. This implies that $|K| \leq 2^{n/2}(s!)^{n/2s}(\frac{n}{2s}!)$ and therefore

$$\begin{aligned}\log(|K|) &< f(n,s)\\ &= \tfrac{n}{2}\log(2) + \tfrac{n}{2}\log(s) - \tfrac{n}{2} + \tfrac{n}{4s}\log(2\pi s) + \tfrac{n}{24s^2}\\ &\quad + \tfrac{n}{2s}\log(\tfrac{n}{2s}) - \tfrac{n}{2s} + \tfrac{1}{2}\log\left(\tfrac{\pi n}{s}\right) + \tfrac{s}{6n}\end{aligned}$$

Denoting $t = \frac{n}{s}$,

$$\begin{aligned}f(n,s) &= \tfrac{n}{2}\log(2) - \tfrac{n}{2}\log(\tfrac{t}{n}) - \tfrac{n}{2} - \tfrac{t}{4}\log(\tfrac{t}{2\pi n}) + \tfrac{t^2}{24n}\\ &\quad + \tfrac{t}{2}\log(\tfrac{t}{2}) - \tfrac{t}{2} + \tfrac{1}{2}\log(t\pi) + \tfrac{1}{6t}\\ \frac{\partial f}{\partial t} &= -\tfrac{n}{2t} - \tfrac{1}{4} - \tfrac{1}{4}\log\left(\tfrac{t}{2\pi n}\right) + \tfrac{t}{12n} + \tfrac{1}{2}\log\left(\tfrac{t}{2}\right) + \tfrac{1}{2t} - \tfrac{1}{6t^2}\\ \frac{\partial^2 f}{\partial t^2} &= \tfrac{n}{2t^2} + \tfrac{1}{4t} + \tfrac{1}{12n} - \tfrac{1}{2t^2} + \tfrac{1}{3t^3} > 0\end{aligned}$$

so, assuming $s < \frac{n}{4}$, $f(n,s)$ is maximised by either $s = 2$ or $s = \frac{n}{5}$. One can check that $f(n,2)$ and $f(n,\frac{n}{5})$ are less than $\log(|B_n|)$.

So we are left with the case $s = \frac{n}{4}$. We can then take without loss of generality $\Delta = \{\{1,2\},\{3,4\},\dots,\{\frac{n}{2}-1,\frac{n}{2}\}\}$. As Δ is a minimal block, the action of $(K^{\mathcal{B}_\Gamma})_\Delta$ on Δ is primitive.

Suppose g fixes $\{\frac{n}{2}+1,\dots,n\}$ pointwise. If $g \neq [1,2][3,4]\cdots[\frac{n}{2}-1,\frac{n}{2}]$ then by the above argument for primitive $K^{\mathcal{B}_\Gamma}$ we have, relabelling if necessary, $[7,8][9,10] \in K_{(\mathcal{B}_\Gamma)}$. So $g = [1,2][3,4]\cdots[\frac{n}{2}-1,\frac{n}{2}]$. This means $K_{(\mathcal{B}_\Gamma)}$ is generated by g and some diagonal subgroup of $(C_2)^{n/2} \times (C_2)^{n/2}$. Thus we have $|K| \leq 2^{n/4+2}(\frac{n}{4}!)^2$, which gives

$$\log(|K|) \quad < \quad -\tfrac{3n}{4}\log(2) + \tfrac{n}{2}\log(n) - \tfrac{n}{2} + \log(\pi n) + \tfrac{1}{3n}$$

which is less than $\log(|B_n|)$.

If no such g fixes $\{\frac{n}{2}+1,\ldots,n\}$ pointwise then $K_{(\mathcal{B}_\Gamma)}$ is a diagonal subgroup of $(C_2)^{n/2} \times (C_2)^{n/2}$ so the above inequality holds. Thus we are left with the case $K_{(\mathcal{B}_\Gamma)} = \langle g \rangle$ with $g = [1,2][3,4]\cdots[n-1,n]$, so by Proposition 3.1.3 $8|n$.

If $|K| > |\langle B_n, x\rangle| = (\frac{n}{2})!$ then $K^{(\mathcal{B}_\Gamma)} \cong S_{n/2}$. In particular there is some $h \in K$ with image $(1,2)$ in $K^{(\mathcal{B}_\Gamma)}$. If h has a cycle $[1,3,2,4]$ then $h^4 = z$ so up to permutation of $1,2,3,4$ we have $h = [1,3][2,4]u$ for some $u \in K_{(\mathcal{B}_\Gamma)}$. If $u = 1$ then $h^2 = z$ and if u acts non-trivially on all Γ_i with $i > 2$ then $hug = [1,4][2,3]$ and $(hug)^2 = z$ so without loss of generallity u acts non-trivially on $5,6$ and trivially on $7,8$. There is also some $h' \in K$ with image $(3,4)$ in $K^{(\mathcal{B}_\Gamma)}$. But then $hh^{h'} = [5,6][7,8]$ and $(hh^{h'})^2 = z$. So $|K| \leq |\langle B_n, x\rangle|$ as required. □

Thus we have the following:

Theorem 3.1.23
For $n \geq 28$, let K be a core-free subgroup of $2 \cdot A_n$. If the natural action of K on $\{1,\ldots,n\}$ is transitive then either $|K| < |B_n|$ or $8 \mid n$ and $|K| = |\langle B_n, x\rangle|$ (with B_n, x as described in Theorem 3.1.17).

General Case

Let K be a largest core-free subgroup of $2 \cdot A_n$ and let Γ be a largest orbit of K. Denote $\Delta = \{1,\ldots,n\} \setminus \Gamma$ and $d = |\Gamma|$ and fix $0 < c < \frac{1}{4}$. Recall that we may assume $n > 850$.

Define $L = L(n,d)$ to be a largest core-free subgroup of $2 \cdot A_n$ which has largest orbit Γ in $\{1,\ldots,n\}$ of length d. We maximise $\log(|L|)$ with respect to d.

Lemma 3.1.24
If $d \leq k^{\frac{1}{4}}$ then

$$\log(|L|) \leq \frac{n}{2}\log(k) - 2n + \frac{n}{k^{\frac{1}{4}}}\log(2\pi k^{\frac{1}{4}}) + \frac{n}{6\sqrt{k}}$$

Proof: If $d \leq k^{\frac{1}{4}}$ then we can partition $\{1,\ldots,n\}$ into sets $\Gamma_1,\ldots,\Gamma_r$, each fixed setwise by L, such that $\frac{k^{\frac{1}{4}}}{2} < |\Gamma_i| \leq k^{\frac{1}{4}}$ for each i except possibly one. We can do this by starting with the orbits of L then while there are two fixed sets of order at most $\frac{k^{\frac{1}{4}}}{2}$ we replace them with their union. This allows us to embed L into $S_{|\Gamma_1|} \times \cdots \times S_{|\Gamma_r|}$. There are at most $\frac{2n}{k^{\frac{1}{4}}}$ sets, so $|L| \leq |(k^{\frac{1}{4}})!|^{\frac{2n}{k^{\frac{1}{4}}}}$ giving the result. □

With $k = n$ this is less than $\log(|B_n|)$ for $n > 33$ so we restrict our attention to $d > n^{\frac{1}{4}}$.

Proposition 3.1.25
If $|L|$ is maximised by $d \geq n - \frac{\sqrt{n}}{2}$ then either $8|n$ and $|L|$ is maximised by $d = n$ or $8|n-1$ and $|L|$ is maximised by $d = n-1$. That is $|L| = |\langle B_n, x\rangle|$ as described in Theorem 3.1.17.

Proof: If $d = n-1$ then we may identify L with its action on Γ, so it is a core-free subgroup of $2 \cdot A_{n-1}$. Hence if $d \geq n-1$ then the result follows from Theorem 3.1.23. We can prove the result then by showing $|L| < |B_n|$ if $d \leq n-2$, so assume $d \leq n-2$. Assume also that $|L|$ is maximal.

Note that, with $\Delta = \{1, \ldots, n\} \setminus \Gamma$, $L_{(\Delta)}$ can be identified with its action on Γ.

We first claim that $\log(|L_{(\Delta)}|) \leq \frac{d}{2}\log(d) - \frac{d}{2}\log(2) - \frac{d}{2} + \frac{1}{2}\log(\pi d) + \frac{1}{12d}$. If $L_{(\Delta)}$ is transitive on Γ then, since $d \geq n - \frac{\sqrt{n}}{2} \geq 28$, this bound follows from Theorem 3.1.23 and if $L_{(\Delta)}$ is trivial then the claim is immeditate, so suppose $L_{(\Delta)}$ is non-trivial and intransitive. If L^Γ is primitive then either it contains the alternating group, in which case L is not core-free, or it is bounded by 2^d, in which case the bound follows. So assume L^Γ is imprimitive. We again use a similar argument as in the transitive case. Fix a minimal block Ω of L^Γ contained in an orbit of $L_{(\Delta)}$. If $|\Omega| = 2$ then either $L_{(\Delta)}$ has orbits of length 2 and therefore has size $2^{\frac{d}{2}}$ from which the claim follows, or the orbits form blocks properly containing Ω. In the second case $L_{(\Delta)}$ embeds into a transitive core-free subgroup of $(A_2 \times A_s) \wr A_{d/2s}$ so the claim follows from Theorem 3.1.23. As in Lemma 3.1.19, if $|\Omega| \in \{3, 4\}$ then $|L^\Gamma| \leq |\Omega|!^{\frac{d}{|\Omega|}}(\frac{d}{|\Omega|})!$ from which the claim follows. If $|\Omega| \geq 5$ then following Lemmas 3.1.19 and 3.1.14 there is some $t \leq \frac{d}{2r}$ with $r = |\Omega|$ and block system $\{\Delta_1, \ldots, \Delta_t\}$ of L^Γ where each Δ_i is a union of blocks Ω^g for some $g \in L^\Gamma$. This allows the embedding of L^Γ into $(A_r \times A_s) \wr A_{d/rs}$ (where $|\Delta_i| = rs$) so if $r > 2$ we can use the argument in Lemma 3.1.20 to prove the claim. If $r = 2$ then $L_{(\Delta)}$ embeds into a transitive core-free subgroup $(A_2 \times A_s) \wr A_{d/2s}$ so the claim follows from Theorem 3.1.23. The claim therefore holds.

We now maximise $\log(|L|)$:

$$\begin{aligned}
\log(|L|) &= \log(|L_{(\Delta)}|) + \log(|L^\Delta|) \\
&\leq f(d) \\
&= \tfrac{d}{2}\log(d) - \tfrac{d}{2}\log(2) - \tfrac{d}{2} + \tfrac{1}{2}\log(\pi d) + \tfrac{1}{12d} \\
&\quad + (n-d)\log(n-d) + d - n + \tfrac{1}{2}\log(2\pi(n-d)) + \tfrac{1}{12(n-d)} \\
f'(d) &= \tfrac{1}{2}\log(d) - \tfrac{1}{2}\log(2) + \tfrac{1}{2d} - \tfrac{1}{12d^2} - \log(n-d) - \tfrac{1}{2(n-d)} + \tfrac{1}{12(n-d)^2} \\
f''(d) &= \tfrac{1}{2d} - \tfrac{1}{2d^2} + \tfrac{1}{6d^3} + \tfrac{1}{n-d} - \tfrac{1}{2(n-d)^2} + \tfrac{1}{6(n-d)^3} \\
&> 0
\end{aligned}$$

So f' is increasing. In particular f is maximised by either $d = n - \frac{\sqrt{n}}{2}$ or $d = n-2$. In either case we find $|L| < |B_n|$. $\square$

Proposition 3.1.26
Suppose $n > 13$ and L has an orbit Γ_p with size $d_p > n^{\frac{1}{4}}$ such that L^{Γ_p} contains $A_{|\Gamma_p|}$. Assume further that d_p is maximal under these conditions and that L acts primitively on any orbit of size at least d_p. If $d_p > \frac{1}{2}\left(n - \frac{\sqrt{n}}{2}\right)$, then L acts diagonally as A_{d_p} on Γ_p and some other orbit of size d_p and $|L|$ is maximised by $d = d_p = \frac{n}{2}$ if n even and $d = d_p = \frac{n-1}{2}$ if n odd. That is $|L| = |\langle H\rangle|$ as described in Theorem 3.1.17.

Proof: Fix $g \in L$ which acts non-trivially on Γ_p as an even permutation and acts non-trivially on as few orbits as possible. Denote by L_0 the normal closure $\langle g\rangle^L$ of the subgroup generated by g in L. A quick calculation gives $d_p \geq 5$ so $(L_0)^{\Gamma_p} \cong A_{d_p}$.

Now we study the action of L_0 on other orbits. Let Γ' be the union of orbits on which L_0 acts non-trivially, fix such an orbit Γ_0 and let $d_0 = |\Gamma_0|$. If g acts trivially on Γ_0 then L_0 acts trivially on Γ_0, so g acts non-trivially on Γ_0 - in particular $L_0^{\Gamma_0}$ has A_{d_p} as a chief factor so $d_0 \geq d_p$. As L_0 is normal in L and L acts primitively on Γ_0, $L_0^{\Gamma_0}$ is transitive. If $L_0^{\Gamma_0}$ does not contain A_{d_0} then we have $\frac{d_p!}{2} \leq |L_0^{\Gamma_0}| \leq 3^{d_0}$. This implies

$$\begin{aligned} d_0 &> \tfrac{1}{\log(3)} d_p \log(d_p) \\ &\geq \tfrac{1}{2\log(3)}(n - \tfrac{\sqrt{n}}{2}) \log(\tfrac{1}{2}(n - \tfrac{\sqrt{n}}{2})) \end{aligned}$$

but this gives $d_0 + d_p > n$. Hence we have $L_0^{\Gamma_0} \geq A_{d_0}$ and $d_0 = d_p$ by maximality of d_p.

Now, suppose L_0 does not act diagonally on the orbits contained in Γ'. Then there exists $h \in L_0$ which acts non-trivially on some but not all orbits in Γ'. If h acts non-trivially on Γ_p then it acts non-trivially on all orbits in Γ' (as g acts non-trivially on the least number of orbits), so h acts trivially on Γ_p. But if h acts non-trivially on Γ_0, then $(\langle h\rangle^L)^{\Gamma_0} \geq A_{d_p}$ so there is some element $x \in L$ acting trivially on Γ_p but in the same way as g on Γ_0. This means gx^{-1} acts as an even permutation on Γ_p and acts non-trivially on fewer orbits than g contrary to assumption. This means h acts trivially on all orbits in Γ' contrary to assumption. Hence L_0 acts diagonally on the orbits contained in Γ'. As L_0 is normal in L, any element of L acting non-trivially on Γ' must also act diagonally on the orbits contained in Γ'.

Now, if $2d_p \geq n-1$ then $L \cong B_n$ so suppose $2d_p < n-1$. Denoting $\Delta = \{1, \ldots, n\} \setminus \Gamma'$ we can identify $L_{(\Delta)}$ as a core-free subgroup of $2 \cdot A_{|\Gamma'|}$ by its action on Γ'. Notice that $3d_p > n$ so Γ' contains two orbits. This gives

$$\begin{array}{rcl} \log(|L|) & = & f(d_p) \\ & = & \log(|L_{(\Delta)}|) + \log(|L^{\Delta}|) \\ & \leq & d_p \log(d_p) - d_p + \frac{1}{2}\log(2\pi d_p) + \frac{1}{12 d_p} + (n-2d_p)\log(n-2d_p) \\ & & -(n-2d_p) + \frac{1}{2}\log(2\pi(n-2d_p)) + \frac{1}{12(n-2d_p)} \\ f'(d_p) & = & \log(d_p) + \frac{1}{2d_p} - \frac{1}{12d_p^2} \\ & & -2\log(n-2d_p) - \frac{1}{n-2d_p} + \frac{1}{6(n-2d_p)^2} \end{array}$$

So with $n - \frac{\sqrt{n}}{2} \leq 2d_p \leq n-2$ one can check that

$$\begin{array}{rcl} f'(d_p) & \geq & \log(2n-\sqrt{n}) - \log(n) + \frac{52n^3 - 52n^{\frac{5}{2}} - 75n^2 + 88n^{\frac{3}{2}} - 34n + 24}{12(n-2)(2n-\sqrt{n})^2} \\ & > & 0 \end{array}$$

The bound is therefore increasing with respect to d_p so is maximised my $2d_p = n-2$. Hence (with computer assistance)

$$\begin{array}{rcl} \log(|L|) & \leq & \frac{n-1}{2}\log(n-2) - \frac{n+4}{2}\log(2) + \log(\pi) - \frac{n-2}{2} + \frac{1}{6(n-2)} - 2 + \frac{1}{24} \\ & < & \log(|B_n|) \end{array}$$

Therefore L is maximised by $2d_p \geq n-1$ so $L \cong B_n$. This forces $8 \nmid n$, $8 \nmid n-1$, otherwise $|L| < |\langle B_n, x\rangle|$, so we are done. $\square$

Proof of Theorem 3.1.17: We now have everything we need to prove Theorem 3.1.17. We do this by showing that

- $|L| \leq |B_n|$ if $8 \nmid n$ and $8 \nmid n-1$
- $|L| \leq |\langle B_n, x\rangle|$ if $8|n$ or $8|n-1$

We do this in two steps imposing different restrictions on L. In the first step we 'ignore' small orbits - to be precise, call an orbit Ω *large* if $|\Omega| \geq n^{\frac{1}{4}}$, otherwise we call Ω *small*.

Definition 3.1.4
- *Let $L_P = L_P(n,d)$ be a largest core-free subgroup of $2{\cdot}A_n$ such that the largest orbit, Γ, has size d and for any large orbit Ω of L_P, L_P^{Ω} is primitive but not alternating.*
- *Let $L_I = L_I(n,d;d_p,d_I,b_I)$ be a largest core-free subgroup of $2 \cdot A_n$ with largest orbit d such that:*
  - *A largest orbit Ω for which $L_I^{\Omega} \geq A_{|\Omega|}$ has size d_p. If no orbit satisfies this then we write $d_p = 0$.*
  - *A largest orbit Ω for which L_I^{Ω} is imprimitive has size d_I. If all orbits are primitive write $d_I = 0$.*
  - *Over all orbits Ω for which L_I^{Ω} is imprimitive, the largest minimal block has size b_I. If all orbits are primitive write $b_I = 0$.*

Clearly $\max\{|L_P|\} \leq \max\{|L_I|\} = \max\{|L|\}$. We maximise each in turn, by reducing to the cases of propositions 3.1.25 and 3.1.26 thus proving Theorem 3.1.17.

Lemma 3.1.27
Step 1: Fix $L_P = L_P(n,d)$. Then

$$\log(|L_P|) \leq \frac{n}{2}\log(n) - 2n + n^{\frac{3}{4}}\log(2\pi n^{\frac{1}{4}}) + \frac{\sqrt{n}}{6}$$

In particular $|L| < |B_n|$ so $|L|$ is not maximised by $|L_P|$.

Proof: Let $\Gamma' = \bigcup_{i=1}^{t} \Gamma_i$ where $\Gamma_1, \ldots, \Gamma_t$ are the large orbits of L_P and let $\Delta = \{1,\ldots,n\} \setminus \Gamma'$. Note that $(L_P)_{(\Gamma')} \cong (L_P)^{\Delta}_{(\Gamma')}$, so by Lemma 3.1.24, with $r = |\Gamma'|$,

$$\log(|(L_P)_{(\Gamma')}|) \leq \frac{n-r}{2}\log(n) - 2(n-r) + \frac{n-r}{n^{\frac{1}{4}}}\log(2\pi n^{\frac{1}{4}}) + \frac{n-r}{6\sqrt{n}}$$

Also $|(L_P)^{\Gamma_i}| \leq 3^{|\Gamma_i|}$ so

$$\begin{aligned}
\log(|L_P|) &= \log(|(L_P)_{(\Gamma')}|) + \textstyle\sum_{i=1}^{t} \log(|L_P^{\Gamma_i}|) \\
&\leq f(r) \\
&= \tfrac{n-r}{2}\log(n) - 2(n-r) + \tfrac{n-r}{n^{\frac{1}{4}}}\log(2\pi n^{\frac{1}{4}}) \\
&\quad + \tfrac{n-r}{6\sqrt{n}} + \textstyle\sum_{i=1}^{t} |\Gamma_i|\log(3) \\
&= \tfrac{n-r}{2}\log(n) - 2(n-r) + \tfrac{n-r}{n^{\frac{1}{4}}}\log(2\pi n^{\frac{1}{4}}) \\
&\quad + \tfrac{n-r}{6\sqrt{n}} + r\log(3)
\end{aligned}$$

Suppose $r < n$. Differentiating with respect to r gives

$$\begin{aligned} f'(r) &= -\tfrac{1}{2}\log(n) + 2 - \tfrac{1}{n^{\frac{1}{4}}}\log(2\pi n^{\frac{1}{4}}) - \tfrac{1}{6\sqrt{n}} + \log(3) \\ &< 0 \end{aligned}$$

The above bound is therefore maximised by $r = 0$ which gives

$$\log(|L_P|) \leq \tfrac{n}{2}\log(n) - 2n + n^{\frac{3}{4}}\log(2\pi n^{\frac{1}{4}}) + \tfrac{\sqrt{n}}{6}$$

which is less than $\log(|B_n|)$ so $|L_P| < |B_n|$ and $|L|$ cannot be maximised by $|L_P|$. □

Before Step 2 we need a couple of technical lemmas:

Lemma 3.1.28

Let G be an imprimitive group acting on Ω with chief factor A_m for some $m \geq 5$, $|\Omega| = s$ and for which a minimal block has size strictly less than m. Then either $s = 2m$ and G embeds into $S_2 \wr S_m$ or

$$\log(|G|) \leq \frac{s}{2}\log(\frac{s}{2}) - \frac{s}{2} + \log(\pi\frac{s}{2}) + \frac{1}{3s} + \log(2) + 16$$

n.b. For $s \approx n$ this bound is larger than $\log(|B_n|)$. We don't however compare such a group directly to B_n and this bound will suffice.

Proof: As G is imprimitive we may embed G into $S_r \wr S_{\frac{s}{r}}$ where r is the size of a minimal block of G.

We first assume $r \geq 3$. Let $\tilde{G}$ be the image of G in $S_{\frac{s}{r}}$. By assumption $r < m$, so A_m is not a subgroup of $S_r^{\frac{s}{r}}$ but is a chief factor of G so we must have that A_m is a chief factor of $\tilde{G}$. In particular either $\tilde{G}$ is primitive with either $m = \frac{s}{r}$ or $|\tilde{G}| \leq 3^{\frac{s}{r}}$ or $\tilde{G}$ is imprimitive and embeds into $S_t \wr S_{\frac{s}{rt}}$ for some $t | \frac{s}{r}$ with $t \notin \{1, \frac{s}{r}\}$ and either $m \leq t$ or $m \leq \frac{s}{rt}$. We can check all possible m, r, t explicitly for $s < 666$, so suppose $s \geq 666$.

Using the embedding of G into $S_r \wr S_{\frac{s}{r}}$ with $r < m$ and $m \leq \frac{s}{r}$ we have

$$\begin{aligned} \log(|G|) &\leq \tfrac{s}{r}\log(r!) + \log(\tfrac{s}{r}!) \\ &\leq f(r) \\ &= s\log(r) - s + \tfrac{s}{2r}\log(2\pi r) + \tfrac{s}{12r^2} + \tfrac{s}{r}\log(\tfrac{s}{r}) \\ &\quad -\tfrac{s}{r} + \tfrac{1}{2}\log(2\pi\tfrac{s}{r}) + \tfrac{r}{12s} \\ f'(r) &= \tfrac{s}{r} - \tfrac{s\log(2\pi r)+s}{2r^2} - \tfrac{s}{6r^3} - \tfrac{s}{r^2}\log(\tfrac{s}{r}) - \tfrac{1}{2r} + \tfrac{1}{12s} \\ f''(r) &= -\tfrac{s}{r^2} + \tfrac{2s\log(2\pi r)+s}{2r^3} + \tfrac{s}{2r^4} + \tfrac{2s\log(\frac{s}{r})+s}{r^3} + \tfrac{1}{2r^2} \\ r^2 f'(r) + r^3 f''(r) &= \tfrac{1}{2}s\log(2\pi r) + \tfrac{s}{3r} + s\log(\tfrac{s}{r}) + s + \tfrac{r^2}{12s} > 0 \end{aligned}$$

hence for all r either $f''(r) > 0$ or $f'(r) > 0$ which implies $f(r)$ is maximised by either $r = 3$ or $r = \min\{m-1, \frac{s}{m}\}$. If $m - 1 \leq \frac{s}{m}$ then we can deduce

$r = m-1 \le \sqrt{s+\frac{1}{4}} - \frac{1}{2}$. If $m-1 \ge \frac{s}{m}$ then $r = \frac{s}{m} \le \frac{s}{\sqrt{s+\frac{1}{4}}+\frac{1}{2}} = \sqrt{s+\frac{1}{4}} - \frac{1}{2}$. In either case $r \le \sqrt{s+\frac{1}{4}} - \frac{1}{2}$. One can check that

$$f(3) < f(\sqrt{s}) < \frac{s}{2}\log(\frac{s}{2}) - \frac{s}{2} + \log(\pi\frac{s}{2}) + \frac{1}{3s} + \log(2)$$

for $s \ge 666$.

In the case $r = 2$, if $s \ne 2m$ then the image $\tilde{G}$ of G in $S_{\frac{s}{2}}$ does not contain $A_{\frac{s}{2}}$. If $\tilde{G}$ is primitive then

$$\begin{aligned} \log(|G|) &\le \tfrac{s}{2}\log(2) + \tfrac{s}{3}\log(3) \\ &< \tfrac{s}{2}\log(\tfrac{s}{2}) - \tfrac{s}{2} + \log(\pi\tfrac{s}{2}) + \tfrac{1}{3s} + \log(2) \end{aligned}$$

and if $\tilde{G}$ is imprimitive then one can show, for example as in [14], that

$$\log(|G|) \le \frac{s}{2}\log(\frac{s}{2}) - \frac{s}{2} + \log(\pi\frac{s}{2}) + \frac{1}{3s} + \log(2)$$

as required. □

Lemma 3.1.29

Let G be a largest subgroup of S_r for some r which has maximal orbit of size at most $t \le r$. Then $G \cong S_t^{\lfloor \frac{r}{t} \rfloor} \times S_{r-t\lfloor \frac{r}{t} \rfloor}$.

N.B. We are using group theoretic language here as it fits our purpose, but a natural equivalent statement is:

Fix $t \le n$ and let $x_1 \le \cdots \le x_N \le t$ be an increasing sequence of integers for some N such that $\sum_{i=1}^N x_i = r$, then $\prod_{i=1}^N x_i!$ is maximal subject to these conditions if and only if $x_2 = \cdots = x_N = t$.

Proof: Let G act naturally on Ω with $|\Omega| = r$. We prove this by induction on r, but first deal with the case that G has at most 2 orbits.

If $t = r$ then the largest subgroup is obviously S_r and we are done. If $t < \frac{r}{2}$ then G would have to have at least 3 orbits, so we may take $\frac{r}{2} \le t < r$. Let $x \le y$ be the size of the two orbits of G. This clearly gives $G = x!y!$. If $y < t$ then $\frac{(x-1)!(y+1)!}{x!y!} = \frac{y+1}{x} > 1$ so $|S_{x-1} \times S_{y+1}| > |G|$ contrary to assumption. Hence $y = t$ and we are done. Now we allow G to have more than two orbits.

Fix any orbit Γ of G and denote $x = |\Gamma|$. We must have that $G^{\Omega\setminus\Gamma}$ is a largest subgroup of S_{r-x} so $G^{\Omega\setminus\Gamma} \cong S_t^{\lfloor \frac{r-x}{t} \rfloor} \times S_{r-x-t\lfloor \frac{r-x}{t} \rfloor}$. If $r - x - t\lfloor \frac{r-x}{t} \rfloor = 0$ (that is, if $t|(r-x)$, so $x = r - t\lfloor \frac{r}{t} \rfloor$) then we are done, so suppose not and denote $0 < y = r - x - t\lfloor \frac{r-x}{t} \rfloor < t$ and let Δ be the orbit of G of size y. Clearly $G^{\Gamma\cup\Delta}$ is a largest subgroup of S_{x+y} with maximal orbit of size at most t, so by the case G has at most two orbits, we must have $x = t$ and we are done. □

Lemma 3.1.30
Step 2: Fix $L_I = L_I(n, d; d_p, d_I, b_I)$. Then

$$\log(|L_I|) \leq \frac{n}{2}\log(n) - \frac{n}{2}\log(2) - \frac{n}{2} + \frac{1}{2}\log(\pi n) + \frac{1}{6n} + 3.5$$

For $n \geq 28$, if $|L|$ is maximised by $|L_I|$ then we are in the case of either Proposition 3.1.25 or Proposition 3.1.26.

Proof: We prove this by induction on $m = \max(d_p, b_I)$. Denote

$$\tau(n) = \frac{n}{2}\log(n) - \frac{n}{2}\log(2) - \frac{n}{2} + \frac{1}{2}\log(\pi n) + \frac{1}{6n} + 3.5$$

Note that $\log(|B_n|)$ is less than this bound. If $m < 2$, $d < n^{\frac{1}{4}}$, $d > n - \frac{\sqrt{n}}{2}$ or $d_p > (n - \frac{\sqrt{n}}{2})/2$ then one can check that this holds using bounds in previous results (the worst case is Lemma 3.1.19 '$r \geq 2$'). So suppose either there is a large orbit on which L_I is alternating (so $d_p \geq n^{\frac{1}{4}}$) or a large orbit on which L_I is imprimitive (so $d_I \geq n^{\frac{1}{4}}$ and therefore $b_I \geq 2$). This result can be checked using the above algorithm for $n \leq 850$ so we may assume $n > 850$.

Case 1: $m = \max(d_p, b_I) = 2$

First we assume $\max(d_p, b_I) = 2$, then for every orbit Ω one of the following holds:

- L_I^Ω is primitive and not containing $A_{|\Omega|}$.
- L_I^Ω is imprimitive with minimal block of length 2.

Let Γ be the union of orbits on which L_I acts imprimitively and orbits of length 2. Denote $\Delta = \{1, \ldots, n\} \setminus \Gamma$ and $r = |\Gamma|$. Then for each orbit $\Omega \subseteq \Delta$, L_I^Ω is primitive and not containing $A_{|\Omega|}$ so has order at most $3^{|\Omega|}$. It follows that $|L_I^\Delta| \leq 3^{n-r}$. Since $b_I = 2$ we may partition Γ into pairs, consisting of blocks and minimal orbits, such that the partition is preserved by L_I. This gives an embedding of $(L_I)_{(\Delta)}$ into $S_2 \wr S_{\frac{r}{2}}$. The orbits of L_I are of length at most d_I, so by Lemma 3.1.29 $|(L_I)_{(\Delta)}| \leq |S_2 \wr ((S_{\frac{d_I}{2}})^{\lfloor \frac{r}{d_I} \rfloor} \times S_{\frac{r}{2} - \frac{d_I}{2}\lfloor \frac{r}{d_I} \rfloor})|$.

We now claim $|(L_I)_{(\Delta)}| \leq |S_2^{\frac{r}{4}}||((S_{\frac{d_I}{2}})^{\lfloor \frac{r}{d_I} \rfloor} \times S_{\frac{r}{2} - \frac{d_I}{2}\lfloor \frac{r}{d_I} \rfloor})|$. Consider the intersection N of the image of $(L_I)_{(\Delta)}$ with $(S_2)^{\frac{r}{2}}$. Relabelling if necessary we can have the $\frac{r}{2}$ copies of S_2 generated by $(2i-1, 2i)$ for $i = 1, \ldots, \frac{r}{2}$. Suppose $\{g_1, \ldots, g_v\}$ is a minimal generating set of N. Let c_i be the least element of $\{1, \ldots, r\}$ such that (c_i, c_{i+1}) appears in g_i. Again relabelling if necessary $c_i = 2i-1$ and, replacing g_i with $g_i g_j$ if necessary, we may assume that (c_j, c_{j+1}) appears in g_i if an only if $i = j$. Consider the projections π_1, π_2 of N onto the product of the first v copies of S_2 and the product of the last $\frac{r}{2} - v$ copies respectively. Clearly π_1 is a bijection and $\pi_1(N) = S_2^v$. For $g \in (S_2)^{\frac{r}{2}}$ denote by $\sigma(g)$ the number of transpositions appearing in g. By Proposition 3.1.3, for $g \in N$ we have $4|\sigma(g)$ so $\sigma(\pi_2(g)) \equiv -\sigma(\pi_1(g)) \pmod 4$. Moreover, if $\pi_2(g) = \pi_2(h)$ and $\sigma(\pi_1(g)) \equiv \sigma(\pi_1(h)) \equiv \epsilon \pmod 4$ with $\epsilon \in \{1,3\}$ then $\sigma(gh) \equiv 2 \pmod 4$ contrary to Proposition 3.1.3. This means $\pi_2 \circ \pi_1^{-1}$ restricts to an injective map from the set of odd permutations in S_2^v to those in $S_2^{\frac{r}{2}-v}$. In particular $v \leq \frac{r}{4}$. Hence $|N| \leq 2^{\frac{r}{4}}$, from which the claim follows.

We now split into further cases.

Case 1.a. $d_I \leq \frac{r}{2}$:

If $d_I \leq \frac{r}{2}$ this gives

$$\begin{aligned}
\log(|L_I|) &= f(r) \\
&= \log(|(L_I)_{(\Delta)}|) + \log(|L_I^{\Delta}|) \\
&\leq \log(3^{n-r}) + \log(|S_2^{\frac{r}{4}}||(S_{\frac{r}{4}})^2)|) \\
&\leq (n-r)\log(3) + \tfrac{r}{4}\log(2) + \tfrac{r}{2}\log(\tfrac{r}{4}) - \tfrac{r}{2} + \log(\pi\tfrac{r}{2}) + \tfrac{2}{3r} \\
f'(r) &= -\log(3) + \tfrac{1}{4}\log(2) + \tfrac{1}{2}\log(\tfrac{r}{4}) + \tfrac{1}{2} - \tfrac{2}{3r^2} \\
f''(r) &= \tfrac{1}{2r} + \tfrac{4}{3r^3} > 0
\end{aligned}$$

So the bound begins decreasing, reaches a minimum, then increases and is therefore maximised by $r = n^{\frac{1}{4}}$ or $r = n$. If $r = n^{\frac{1}{4}}$ then

$$\log(|L_I|) \leq (n - n^{\frac{1}{4}})\log(3) + \frac{n^{\frac{1}{4}}}{4}\log(2) + \frac{n^{\frac{1}{4}}}{2}\log(\frac{n^{\frac{1}{4}}}{4}) - \frac{n^{\frac{1}{4}}}{2} + \log(\pi\frac{n^{\frac{1}{4}}}{2}) + \frac{2}{3n^{\frac{1}{4}}}$$

which is less than $\log(|B_n|)$ and therefore $\tau(n)$. If $r = n$ then

$$\log(|L_I|) \leq \frac{n}{4}\log(2) + \frac{n}{2}\log(\frac{n}{4}) - \frac{n}{2} + \log(\pi\frac{n}{2}) + \frac{2}{3n}$$

which is less than $\log(B_n)$ and therefore $\tau(n)$.

Case 1.b. $d_I > \frac{r}{2}$:

So suppose $d_I > \frac{r}{2}$. This means that there is a unique orbit Γ_I of size d_I for which $L_I^{\Gamma_I}$ is imprimitive and any other orbit Ω of size at least d_I is primitive and L_I^{Ω} does not contain $A_{|\Omega|}$. In this case we apply induction to $(L_I)_{(\Gamma_I)}$, so

$$\begin{aligned}
\log(|(L_I)_{(\Gamma_I)}|) \leq\ & \tfrac{n-d_I}{2}\log(n-d_I) - \tfrac{n-d_I}{2}\log(2) - \tfrac{n-d_I}{2} + \\
& \tfrac{1}{2}\log(\pi(n-d_I)) + \tfrac{1}{6(n-d_I)} + 3.5
\end{aligned}$$

$L_I^{\Gamma_I}$ embeds into $S_2 \wr S_{\frac{d_I}{2}}$. Denote by $\tilde{L_I}$ the image of L_I in $S_{\frac{d_I}{2}}$, we again split into cases.

. . . .

Case 1.b.i. $\tilde{L_I}$ imprimitive:

If the image of L_I in $S_{\frac{d_I}{2}}$ is imprimitive then $L_I^{\Gamma_I}$ embeds into $S_2 \wr (S_s \wr S_{\frac{d_I}{2s}})$ for some $s|\frac{d_I}{2}$. This gives the following bound, which we differentiate with respect to $t = \frac{1}{s}$ and maximise with respect to t

$$\begin{array}{rcl}
\log(|L_I^{\Gamma_I}|) & \leq & \frac{d_I}{2}\log(2) + \frac{d_I}{2}\log(s) - \frac{d_I}{2} + \frac{d_I}{4s}\log(2\pi s) + \frac{d_I}{24s^2} \\
 & & + \frac{d_I}{2s}\log(\frac{d_I}{2s}) - \frac{d_I}{2s} + \frac{1}{2}\log(\pi\frac{d_I}{2s}) + \frac{s}{6d_I} \\
 & = & f(t) \\
 & = & \frac{d_I}{2}\log(2) - \frac{d_I}{2}\log(t) - \frac{d_I}{2} - \frac{d_I t}{4}\log(\frac{t}{2\pi}) + \frac{d_I t^2}{24} \\
 & & + \frac{d_I t}{2}\log(\frac{d_I t}{2}) - \frac{d_I t}{2} + \frac{1}{2}\log(\pi\frac{d_I t}{2}) + \frac{1}{6d_I t} \\
f'(t) & = & -\frac{d_I}{2t} - \frac{d_I}{4} - \frac{d_I}{4}\log(\frac{t}{2\pi}) + \frac{d_I t}{12} + \frac{d_I}{2}\log(\frac{d_I t}{2}) + \frac{1}{2t} - \frac{1}{6d_I t^2} \\
f''(t) & = & \frac{d_I}{2t^2} - \frac{d_I}{4t} + \frac{d_I}{12} + \frac{d_I}{2t} - \frac{1}{2t^2} + \frac{1}{3d_I t^3} > 0
\end{array}$$

so the bound is maximised by $s = 2$ or $s = \frac{d_I}{4}$ - recall that we assume $d_I \leq n - \frac{\sqrt{n}}{2}$. If $s = 2$ then we obtain the following bound which we differentiate with respect to d_I.

$$\begin{array}{rcl}
\log(|L_I|) & \leq & f(d_I) \\
 & = & \frac{n-d_I}{2}\log(n-d_I) - \frac{n-d_I}{2}\log(2) - \frac{n-d_I}{2} + \\
 & & \frac{1}{2}\log(\pi(n-d_I)) + \frac{1}{6(n-d_I)} + 3.5 \\
 & & +d_I\log(2) - \frac{13d_I}{32} + \frac{d_I}{8}\log(4\pi) + \frac{d_I}{4}\log(\frac{d_I}{4}) + \frac{1}{2}\log(\pi\frac{d_I}{4}) \\
f'(d_I) & = & -\frac{1}{2}\log(n-d_I) + \frac{1}{2}\log(2) - \frac{1}{2(n-d_I)} + \frac{1}{6(n-d_I)^2} \\
 & & + \log(2) - \frac{13}{32} + \frac{1}{8}\log(4\pi) + \frac{1}{4}\log(\frac{d_I}{4}) + \frac{1}{4} + \frac{1}{2d_I} \\
f''(d_I) & = & \frac{1}{2(n-d_I)} - \frac{1}{2(n-d_I)^2} + \frac{1}{3(n-d_I)^3} + \frac{1}{4d_I} - \frac{1}{2d_I^2} > 0
\end{array}$$

Hence the bound is maximised by either $d_I = n^{\frac{1}{4}}$ or $d_I = n - \frac{\sqrt{n}}{2}$. In either case the bound is less than $\log(|B_n|)$ and therefore $\tau(n)$.

If $s = \frac{d_I}{4}$ then we obtain the following bound which we differentiate with respect to d_I.

$$\begin{array}{rcl}
\log(|L_I|) & \leq & f(d_I) \\
 & = & \frac{n-d_I}{2}\log(n-d_I) - \frac{n-d_I}{2}\log(2) - \frac{n-d_I}{2} + \\
 & & \frac{1}{2}\log(\pi(n-d_I)) + \frac{1}{6(n-d_I)} + 3.5 \\
 & & + \frac{d_I}{2}\log(2) + \frac{d_I}{2}\log(\frac{d_I}{4}) - \frac{d_I}{2} + \log(\pi\frac{d_I}{2}) + \frac{2}{3d_I} \\
 & & +2\log(2) - 2 + \frac{1}{2}\log(\pi 2) + \frac{1}{24} \\
f'(d_I) & = & -\frac{1}{2}\log(n-d_I) + \frac{1}{2}\log(2) - \frac{1}{2(n-d_I)} + \frac{1}{6(n-d_I)^2} \\
 & & +\frac{1}{2}\log(2) + \log(\frac{d_I}{4}) + \frac{1}{d_I} - \frac{2}{3d_I^2} \\
f''(d_I) & = & \frac{1}{2(n-d_I)} - \frac{1}{2(n-d_I)^2} + \frac{1}{3(n-d_I)^3} + \frac{1}{d_I} - \frac{1}{d_I^2} + \frac{4}{3d_I^3} > 0
\end{array}$$

Hence the bound is maximised by either $d_I = n^{\frac{1}{4}}$ or $d_I = n - \frac{\sqrt{n}}{2}$. In either case the bound is less than $\log(|B_n|)$ and therefore $\tau(n)$.

. . . .

Case 1.b.ii. $\tilde{L_I}$ primitive:

So we are left with the case that the image $\tilde{L_I}$ of L_I in $S_{\frac{d_I}{2}}$ is primitive. If $\tilde{L_I}$ does not contain $A_{\frac{d_I}{2}}$ then $|L_I^{\Gamma_I}| \leq 2^{\frac{d_I}{2}} 3^{\frac{d_I}{2}} \leq 2^{\frac{n}{2}} 3^{\frac{n}{2}}$ which is less than $e^{\tau(n)}$ and less than $|B_n|$.

If $\tilde{L_I}$ does contain $A_{\frac{d_I}{2}}$ then we consider the intersection N of $((L_I)_{(\Delta)})^{\Gamma_I}$ with $S_2^{\frac{d_I}{2}}$. Recall that we may assume $d_p \geq n^{\frac{1}{4}}$ or $d_I \geq n^{\frac{1}{4}}$ so, as $d_p = 2$, we have $d_I \geq n^{\frac{1}{4}} > 10$. Also the chief factors of $L_I^{\Gamma \setminus \Gamma_I}$ are all strictly smaller than $A_{\frac{d_I}{2}}$, so we can find a subgroup M of L_I for which $M^{\Gamma \setminus \Gamma_I}$ is trivial and $M^{\Gamma_I} \cong A_{\frac{d_I}{2}}$.

The only possible normal subgroups of $L_I^{\Gamma_I}$ contained in $S_2^{\frac{d_I}{2}}$ and therefore the only choices of N are then of order 1, 2, $2^{\frac{d_I}{2}-1}$ or $2^{\frac{d_I}{2}}$.

Consider the embedding of L_I^{Γ} into $S_2 \wr S_{\frac{r}{2}}$. We split the base $S_2^{\frac{r}{2}}$ into $S_2^{\frac{r-d_I}{2}}$ and $S_2^{\frac{d_I}{2}}$, with $S_2^{\frac{d_I}{2}}$ acting on Γ_I. Let $\sigma_0 : S_2^{\frac{r}{2}} \to S_2^{\frac{r-d_I}{2}}$ and $\sigma_1 : S_2^{\frac{r}{2}} \to S_2^{\frac{d_I}{2}}$ be the natural projections. If N is of order $2^{\frac{d_I}{2}-1}$ or $2^{\frac{d_I}{2}}$ then it contains an element which is the product of exactly two transpositions. Let $g \in (L_I)_{(\Delta)}$ such that $\sigma_1(g)$ is the product of exactly two transpositions. As $M^{\Gamma_I} \cong A_{\frac{d_I}{2}}$, there is some $x \in M$ such that $\sigma_1(g^x)$ and $\sigma_1(g)$ share exactly one transposition, so $\sigma_1(gg^x)$ is a product of two transpositions and $\sigma_0(gg^x) = 1$. This means gg^x is a product of two transpositions contrary to Proposition 3.1.3. Hence $|N| \leq 2$.

We use $|L_I| = |L_I^{\Delta}||(L_I)_{(\Delta)}^{\Gamma_I}||(L_I)_{(\Delta \cup \Gamma_I)}|$. From the above $|(L_I)_{(\Delta)}^{\Gamma_I}| \leq 2|S_{\frac{d_I}{2}}|$ and as noted at the beginning of this case $|L_I^{\Delta}| \leq 3^{n-r}$, so applying induction to $(L_I)_{(\Delta \cup \Gamma_I)}$ by identifying it with its action on $\Gamma \setminus \Gamma_I$ gives

$$\begin{aligned}
\log(|L_I|) &\leq f(d_I, r) \\
&= \tfrac{r-d_I}{2}\log(r-d_I) - \tfrac{r-d_I}{2}\log(2) - \tfrac{r-d_I}{2} + \\
&\quad \tfrac{1}{2}\log(\pi(r-d_I)) + \tfrac{1}{6(r-d_I)} + 3.5 + (n-r)\log(3) \\
&\quad + \log(2) + \tfrac{d_I}{2}\log(\tfrac{d_I}{2}) - \tfrac{d_I}{2} + \tfrac{1}{2}\log(\pi d_I) + \tfrac{1}{6d_I} \\
\tfrac{\partial f}{\partial r} &= \tfrac{1}{2}\log(r-d_I) - \tfrac{1}{2}\log(2) + \tfrac{1}{2(r-d_I)} - \tfrac{1}{6(n-r)^2} - \log(3) \\
\tfrac{\partial^2 f}{\partial r^2} &= \tfrac{1}{2(r-d_I)} - \tfrac{1}{2(r-d_I)^2} + \tfrac{1}{3(n-r)^3} > 0
\end{aligned}$$

so the bound is maximised by $r = d_I$, $r = d_I + 1$ or $r = n$. If $r = n$ then

$$\begin{aligned}
\log(|L_I|) &\leq g(d_I) \\
&= \tfrac{n-d_I}{2}\log(n-d_I) - \tfrac{n-d_I}{2}\log(2) - \tfrac{n-d_I}{2} + \\
&\quad \tfrac{1}{2}\log(\pi(n-d_I)) + \tfrac{1}{6(n-d_I)} + 3.5 \\
&\quad + \log(2) + \tfrac{d_I}{2}\log(\tfrac{d_I}{2}) - \tfrac{d_I}{2} + \tfrac{1}{2}\log(\pi d_I) + \tfrac{1}{6d_I} \\
g'(d_I) &= -\tfrac{1}{2}\log(n-d_I) + \tfrac{1}{2}\log(2) - \tfrac{1}{2(n-d_I)} + \tfrac{1}{6(n-d_I)^2} \\
&\quad + \tfrac{1}{2}\log(\tfrac{d_I}{2}) + \tfrac{1}{2d_I} - \tfrac{1}{6d_I^2} \\
g''(d_I) &= \tfrac{1}{2(n-d_I)} - \tfrac{1}{2(n-d_I)^2} + \tfrac{1}{3(n-d_I)^3} + \tfrac{1}{2d_I} - \tfrac{1}{2d_I^2} + \tfrac{1}{3d_I^3} > 0
\end{aligned}$$

so the bound is maximised by either $d_I = n^{\frac{1}{4}}$ or $d_I = n - \frac{\sqrt{n}}{2}$. In each case the bound is less than $\log(|B_n|)$ and therefore $\tau(n)$. If $r = d_i + 1$ then

$$\begin{array}{lll} \log(|L_I|) & \leq & g(d_I) \\ & & \frac{1}{2}\log(\pi) + \frac{1}{6} + 3 + (n - d_i - 1)\log(3) \\ & & +\frac{1}{2}\log(2) + \frac{d_I}{2}\log(\frac{d_I}{2}) - \frac{d_I}{2} + \frac{1}{2}\log(\pi d_I) + \frac{1}{6d_I} \\ g'(d_I) & = & -\log(3) + \frac{1}{2}\log(\frac{d_i}{2}) + \frac{1}{2d_I} - \frac{1}{6d_I^2} \\ g''(d_I) & = & \frac{1}{2d_I} - \frac{1}{2d_I^2} + \frac{1}{3d_I^3} > 0 \end{array}$$

so the bound is maximised by either $d_I = n^{\frac{1}{4}}$ or $d_I = n - \frac{\sqrt{n}}{2}$. In each case the bound is less than $\log(|B_n|)$ and therefore $\tau(n)$. If $r = d_I$ then

$$\begin{array}{lll} \log(|L_I|) & \leq & g(d_I) \\ & = & (n - d_I)\log(3) + \log(2) + \frac{d_I}{2}\log(\frac{d_I}{2}) - \frac{d_I}{2} + \frac{1}{2}\log(\pi d_I) + \frac{1}{6d_I} \\ g'(d_I) & = & -\log(3) + \frac{1}{2}\log(\frac{d_I}{2}) + \frac{1}{2d_I} - \frac{1}{6d_I^2} \\ g''(d_I) & = & \frac{1}{2d_I} - \frac{1}{2d_I^2} + \frac{1}{3d_I^3} > 0 \end{array}$$

so the bound is maximised by either $d_I = n^{\frac{1}{4}}$ or $d_I = n - \frac{\sqrt{n}}{2}$. In each case the bound is less than $\log(|B_n|)$ and therefore $\tau(n)$.

Case 2: $3 \leq m = \max(d_p, b_I) \leq n^{\frac{1}{3}}$

Let Γ_I be the union of orbits Ω for which $|\Omega| = m$ or L_I^{Ω} is imprimitive with a block of size m, denote $r = |\Gamma_I|$. Note that we may embed $L_I^{\Gamma_I}$ into $S_m \wr S_{\frac{r}{m}}$ to obtain $|L_I^{\Gamma_I}| \leq (m!)^{\frac{r}{m}} \frac{r}{m}!$.

If $r = n$ then

$$\begin{array}{lll} \log(|L_I|) & \leq & g(m) \\ & = & n\log(m) - n + \frac{n}{2m}\log(2\pi m) + \frac{n}{12m^2} \\ & & +\frac{n}{m}\log(\frac{n}{m}) - \frac{n}{m} + \frac{1}{2}\log(2\pi\frac{n}{m}) + \frac{m}{12n} \\ g'(m) & = & \frac{n}{m} + \frac{n}{2m^2} - \frac{n}{2m^2}\log(2\pi m) - \frac{n}{6m^3} \\ & & -\frac{n}{m^2}\log(\frac{n}{m}) - \frac{1}{2m} + \frac{1}{12n} \\ g''(m) & = & -\frac{n}{m^2} - \frac{n}{m^3} - \frac{n}{2m^3} + \frac{n}{m^3}\log(2\pi m) \\ & & +\frac{n}{2m^4} + \frac{n}{m^3} + \frac{2n}{m^3}\log(\frac{n}{m}) + \frac{1}{2m^2} \\ g'(m) + \frac{m}{2}g''(m) & = & \frac{n}{2m} + \frac{n}{4m^2} + \frac{n}{12m^3} - \frac{1}{4m} + \frac{1}{12n} > 0 \end{array}$$

hence either $g'(m) > 0$ or $g''(m) > 0$ which is only possible if the bound is maximised by either $m = 3$ or $m = n^{\frac{1}{3}}$. In each case the bound is below $\log(|B_n|)$.

If $r \leq n - 1$ then we apply induction to $(L_I)_{(\Gamma_I)}$ to assume

$$\log(|(L_I)_{(\Gamma_I)}|) \leq \frac{n-r}{2}\log(n-r) - \frac{n-r}{2}\log(2) - \frac{n-r}{2} + \frac{1}{2}\log(\pi(n-r)) + \frac{1}{6(n-r)} + 3.5$$

Hence

$$\begin{aligned}
\log(|L_I|) &\leq f(r)\\
&= \tfrac{n-r}{2}\log(n-r) - \tfrac{n-r}{2}\log(2) - \tfrac{n-r}{2} + \tfrac{1}{2}\log(\pi(n-r)) + \tfrac{1}{6(n-r)} + 3.5\\
&\quad + r\log(m) - r + \tfrac{r}{2m}\log(2\pi m) + \tfrac{r}{12m^2}\\
&\quad + \tfrac{r}{m}\log(\tfrac{r}{m}) - \tfrac{r}{m} + \tfrac{1}{2}\log(2\pi\tfrac{r}{m}) + \tfrac{m}{12r}
\end{aligned}$$

Differentiating this bound with respect to r gives

$$\begin{aligned}
f'(r) &= -\tfrac{1}{2}\log(n-r) + \tfrac{1}{2}\log(2) - \tfrac{1}{2(n-r)} + \tfrac{1}{6(n-r)^2} + \log(m) - 1 +\\
&\quad \tfrac{1}{2m}\log(2\pi m) + \tfrac{1}{12m^2} + \tfrac{1}{m}\log(\tfrac{r}{m}) + \tfrac{1}{2r} - \tfrac{m}{12r^2}\\
f''(r) &= \tfrac{1}{2(n-r)} - \tfrac{1}{2(n-r)^2} + \tfrac{1}{3(n-r)^3} + \tfrac{1}{rm} - \tfrac{1}{2r^2} + \tfrac{m}{6r^3} > 0
\end{aligned}$$

so the bound is maximised by $r = n-1$ or $r = m$. If $r = n-1$ then

$$\begin{aligned}
\log(|L_I|) &\leq g(m)\\
&= -\tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 3.5\\
&\quad n\log(m) - n + \tfrac{n}{2m}\log(2\pi m) + \tfrac{n}{12m^2}\\
&\quad + \tfrac{n}{m}\log(\tfrac{n}{m}) - \tfrac{n}{m} + \tfrac{1}{2}\log(2\pi\tfrac{n}{m}) + \tfrac{m}{12n}\\
g'(m) &= \tfrac{n}{m} + \tfrac{n}{2m^2} - \tfrac{n}{2m^2}\log(2\pi m) - \tfrac{n}{6m^3}\\
&\quad - \tfrac{n}{m^2}\log(\tfrac{n}{m}) - \tfrac{1}{2m} + \tfrac{1}{12n}\\
g''(m) &= -\tfrac{n}{m^2} - \tfrac{n}{m^3} - \tfrac{n}{2m^3} + \tfrac{n}{m^3}\log(2\pi m)\\
&\quad + \tfrac{n}{2m^4} + \tfrac{n}{m^3} + \tfrac{2n}{m^3}\log(\tfrac{n}{m}) + \tfrac{1}{2m^2}\\
g'(m) + \tfrac{m}{2}g''(m) &= \tfrac{n}{2m} + \tfrac{n}{4m^2} + \tfrac{n}{12m^3} - \tfrac{1}{4m} + \tfrac{1}{12n} > 0
\end{aligned}$$

hence either $g'(m) > 0$ or $g''(m) > 0$ which is only possible if the bound is maximised by either $m = 3$ or $m = n^{\frac{1}{3}}$. In each case the bound is below $\log(|B_n|)$. If $r = m$ then

$$\begin{aligned}
\log(|L_I|) &\leq g(m)\\
&= \tfrac{n-m}{2}\log(n-m) - \tfrac{n-m}{2}\log(2) - \tfrac{n-m}{2}\\
&\quad + \tfrac{1}{2}\log(\pi(n-m)) + \tfrac{1}{6(n-m)} + 3.5\\
&\quad + m\log(m) - m + \tfrac{1}{2}\log(2\pi m) + \tfrac{1}{12m}\\
&\quad -1 + \tfrac{1}{2}\log(2\pi) + \tfrac{1}{12}\\
g'(m) &= -\tfrac{1}{2}\log(n-m) + \tfrac{1}{2}\log(2) - \tfrac{1}{2(n-m)} + \tfrac{1}{6(n-m)^2} + \log(m) + \tfrac{1}{2m} - \tfrac{1}{12m^2}\\
g''(m) &= \tfrac{1}{2(n-m)} - \tfrac{1}{2(n-m)^2} + \tfrac{1}{3(n-m)^3} + \tfrac{1}{m} - \tfrac{1}{2m^2} + \tfrac{1}{6m^3} > 0
\end{aligned}$$

so the bound is maximised by either $m = 3$ or $m = n^{\frac{1}{3}}$. In each case the bound is below $\log(|B_n|)$.

Case 3: $m = \max(d_p, b_I) \geq n^{\frac{1}{3}}$

First suppose there is some orbit Γ_I such that $L_I^{\Gamma_I}$ is imprimitive with minimal block $\Delta \subset \Gamma_I$ of size m such that $((L_I)_\Delta)^\Delta$ does not contain A_m. Then with $r = |\Gamma_I|$ we have $L_I^{\Gamma_I} \leq 3^r(\frac{r}{m}!)$. Recall that we may assume $r \leq n - \frac{n^{\frac{1}{2}}}{2}$. This gives

$$\begin{aligned}
\log(L_I) &= \log((L_I)_{\Gamma_I}) + \log(L_I^{\Gamma_I}) \\
&\leq f(r,m) \\
&= \tfrac{n-r}{2}\log(n-r) - \tfrac{n-r}{2}\log(2) - \tfrac{n-r}{2} + \tfrac{1}{2}\log(\pi(n-r)) + \tfrac{1}{6(n-r)} + 3.5 \\
&\quad + r\log(3) + \tfrac{r}{m}\log(\tfrac{r}{m}) - \tfrac{r}{m} + \tfrac{1}{2}\log(2\pi\tfrac{r}{m}) + \tfrac{m}{12r} \\
\frac{\partial f}{\partial m} &= -\tfrac{r}{m^2}\log(\tfrac{r}{m}) - \tfrac{1}{2m} + \tfrac{1}{12r} < 0
\end{aligned}$$

so $f(r,m)$ is maximised by $m = n^{\frac{1}{3}}$ giving

$$\begin{aligned}
\log(L_I) &\leq g(r) = f(r, n^{\frac{1}{3}}) \\
&= \tfrac{n-r}{2}\log(n-r) - \tfrac{n-r}{2}\log(2) - \tfrac{n-r}{2} + \tfrac{1}{2}\log(\pi(n-r)) + \tfrac{1}{6(n-r)} + 3.5 \\
&\quad + r\log(3) + \tfrac{r}{n^{\frac{1}{3}}}\log(\tfrac{r}{n^{\frac{1}{3}}}) - \tfrac{r}{n^{\frac{1}{3}}} + \tfrac{1}{2}\log(2\pi\tfrac{r}{n^{\frac{1}{3}}}) + \tfrac{n^{\frac{1}{3}}}{12r} \\
g'(r) &= -\tfrac{1}{2}\log(\tfrac{n-r}{2}) - \tfrac{1}{2(n-r)} + \tfrac{1}{6(n-r)^2} \\
&\quad \log(3) + \tfrac{1}{n^{\frac{1}{3}}}\log(\tfrac{r}{n^{\frac{1}{3}}}) + \tfrac{1}{2r} - \tfrac{n^{\frac{1}{3}}}{12r^2} \\
g''(r) &= \tfrac{1}{2(n-r)} - \tfrac{1}{2(n-r)^2} + \tfrac{1}{3(n-r)^3} + \tfrac{1}{rn^{\frac{1}{3}}} - \tfrac{1}{2r^2} + \tfrac{n^{\frac{1}{3}}}{6r^3} > 0
\end{aligned}$$

so $g(r)$ is maximised by either $r = 2n^{\frac{1}{3}}$ or $r = n - \frac{n^{\frac{1}{2}}}{2}$. In both cases the bound is below $\log(|B_n|)$.

....

So we may suppose that every orbit Ω for which L_I^Ω is imprimitive with minimal block of length m satisfies $((L_I)_\Omega)^\Omega \geq A_m$.

Let Γ_I be the union of orbits Ω of L_I for which either L_I^Ω is imprimitive with a minimal block Ω_b of size m or $|\Omega| = m$ and L_I^Ω contains A_m. Let $r = |\Gamma_I|$ and $\mathcal{B}_I = \{\Omega_1, \ldots, \Omega_{\frac{r}{m}}\}$ be a set of disjoint blocks and orbits of size m with $\Gamma_I = \cup_{i=1}^{\frac{r}{m}} \Omega_i$.

We then have that $\left((L_I)_{(\mathcal{B}_I)}\right)^{\Gamma_I}$ contains a subdirect product N of $A_m^{\frac{r}{m}}$ which is normal in L_I. In particular $N \cong A_m^u$ for some u, where each copy of A_m acts diagonally on some of the orbits of $A_m^{\frac{r}{m}}$ and the orbits any two copies of A_m act non-trivially on are distinct.

Case 3.a. $u \leq \frac{r}{2m}$:

Assume $u \leq \frac{r}{2m}$. Then $L_I^{\Gamma_I}$ embeds into $S_m \wr S_{\frac{r}{m}}$ with $|L_I^{\Gamma_I} \cap S_m| \leq (m!)^u$. Letting $t = \frac{1}{m}$ and denoting the following bound on $\log(L_I)$ by $f(t,r,u)$,

$$\begin{array}{rcl}
\log(|L_I|) & = & \log(|(L_I)_{(\Gamma_I)}|) + \log(|L_I^{\Gamma_I}|) \\
& \leq & \frac{n-r}{2}\log(n-r) - \frac{n-r}{2}\log(2) - \frac{n-r}{2} + \frac{1}{2}\log(\pi(n-r)) + \frac{1}{6(n-r)} + 3.5 \\
& & +um\log(m) - um + \frac{u}{2}\log(2\pi m) + \frac{u}{12m} \\
& & +\frac{r}{m}\log(\frac{r}{m}) - \frac{r}{m} + \frac{1}{2}\log(2\pi\frac{r}{m}) + \frac{m}{12r} \\
f(t,r,u) & = & \frac{n-r}{2}\log(n-r) - \frac{n-r}{2}\log(2) - \frac{n-r}{2} + \frac{1}{2}\log(\pi(n-r)) + \frac{1}{6(n-r)} + 3.5 \\
& & -\frac{u}{t}\log(t) - \frac{u}{t} - \frac{u}{2}\log(\frac{t}{2\pi}) + \frac{ut}{12} \\
& & +rt\log(rt) - rt + \frac{1}{2}\log(2\pi rt) + \frac{1}{12rt} \\
\frac{\partial f}{\partial u} & = & -\frac{1}{t}\log(t) - \frac{1}{t} - \frac{1}{2}\log(\frac{t}{2\pi}) + \frac{t}{12} > 0
\end{array}$$

For fixed r, b_I this means $f(t,r,u)$ is maximised by $u = \frac{r}{2m}$. Substituting $u = \frac{r}{2m}$ in we obtain

$$\begin{array}{rcl}
g(t,r) & = & f(t,r,\frac{r}{2m}) \\
& = & \frac{n-r}{2}\log(n-r) - \frac{n-r}{2}\log(2) - \frac{n-r}{2} + \frac{1}{2}\log(\pi(n-r)) + \frac{1}{6(n-r)} + 3.5 \\
& & -\frac{r}{2}\log(t) - \frac{r}{2} - \frac{rt}{4}\log(\frac{t}{2\pi}) + \frac{rt^2}{24} \\
& & +rt\log(rt) - rt + \frac{1}{2}\log(2\pi rt) + \frac{1}{12rt} \\
\frac{\partial g}{\partial t} & = & -\frac{r}{2t} - \frac{r}{4} - \frac{r}{4}\log(\frac{t}{2\pi}) + \frac{rt}{12} + r\log(rt) + \frac{1}{2t} - \frac{1}{12rt^2} \\
\frac{\partial^2 g}{\partial t^2} & = & \frac{r}{2t^2} - \frac{r}{4t} + \frac{r}{12} + \frac{r}{t} - \frac{1}{2t^2} + \frac{1}{6rt^3} > 0
\end{array}$$

Note that if $m > \frac{1}{2}\left(n - \frac{\sqrt{n}}{2}\right)$ then $r > n - \frac{\sqrt{n}}{2}$ so, as $3m > n$ for $n \geq 3$, either Γ_I is a single orbit of size r or Γ_I is a union of two orbits of size m - in either case L_I has no other orbit of size at least m and we can apply Proposition 3.1.25 or Proposition 3.1.26. Hence we may also assume $m \leq \frac{1}{2}\left(n - \frac{\sqrt{n}}{2}\right)$. Therefore $g(t,r)$ is maximised by either $m = 5$ or $m = \frac{1}{2}\left(n - \frac{\sqrt{n}}{2}\right)$ for $r \geq \left(n - \frac{\sqrt{n}}{2}\right)$ and $m = \frac{r}{2}$ if $r \leq \left(n - \frac{\sqrt{n}}{2}\right)$. Testing each case in turn,

$$\begin{array}{rcl}
h(r) & = & f(\frac{1}{5}, r, \frac{r}{10}) \\
& = & \frac{n-r}{2}\log(n-r) - \frac{n-r}{2}\log(2) - \frac{n-r}{2} + \frac{1}{2}\log(\pi(n-r)) + \frac{1}{6(n-r)} + 3.5 \\
& & +\frac{r}{2}\log(5) - \frac{r}{2} + \frac{r}{20}\log(10\pi) + \frac{r}{600} \\
& & +\frac{r}{5}\log(\frac{r}{5}) - \frac{r}{5} + \frac{1}{2}\log(2\pi\frac{r}{5}) + \frac{5}{12r} \\
h'(r) & = & -\frac{1}{2}\log(n-r) + \frac{1}{2}\log(2) - \frac{1}{2(n-r)} + \frac{1}{6(n-r)^2} \\
& & +\frac{1}{2}\log(5) - \frac{1}{2} + \frac{1}{20}\log(10\pi) + \frac{1}{600} + \frac{1}{5}\log(\frac{r}{5}) + \frac{1}{2r} - \frac{5}{12r^2} \\
h''(r) & = & \frac{1}{2(n-r)} - \frac{1}{2(n-r)^2} + \frac{1}{3(n-r)^3} + \frac{1}{5r} - \frac{1}{2r^2} + \frac{5}{6r^3} > 0
\end{array}$$

$$
\begin{aligned}
h(r) &= f(\tfrac{4}{2n-\sqrt{n}}, r, \tfrac{2r}{2n-\sqrt{n}}) \\
&= \tfrac{n-r}{2}\log(n-r) - \tfrac{n-r}{2}\log(2) - \tfrac{n-r}{2} + \tfrac{1}{2}\log(\pi(n-r)) + \tfrac{1}{6(n-r)} + 3.5 \\
&\quad + \tfrac{r}{2}\log(\tfrac{2n-\sqrt{n}}{4}) - \tfrac{r}{2} + \tfrac{r}{2n-\sqrt{n}}\log(\tfrac{\pi(2n-\sqrt{n})}{2}) + \tfrac{2r}{3(2n-\sqrt{n})^2} \\
&\quad + \tfrac{4r}{2n-\sqrt{n}}\log(\tfrac{4r}{2n-\sqrt{n}}) - \tfrac{4r}{2n-\sqrt{n}} + \tfrac{1}{2}\log(\pi\tfrac{8r}{2n-\sqrt{n}}) + \tfrac{2n-\sqrt{n}}{48r} \\
h'(r) &= -\tfrac{1}{2}\log(n-r) + \tfrac{1}{2}\log(2) - \tfrac{1}{2(n-r)} + \tfrac{1}{6(n-r)^2} \\
&\quad + \tfrac{1}{2}\log(\tfrac{2n-\sqrt{n}}{4}) - \tfrac{1}{2} + \tfrac{1}{2n-\sqrt{n}}\log(\tfrac{\pi(2n-\sqrt{n})}{2}) + \tfrac{2}{3(2n-\sqrt{n})^2} \\
&\quad + \tfrac{4}{2n-\sqrt{n}}\log(\tfrac{4r}{2n-\sqrt{n}}) + \tfrac{1}{2r} - \tfrac{2n-\sqrt{n}}{48r^2} \\
h''(r) &= \tfrac{1}{2(n-r)} - \tfrac{1}{2(n-r)^2} + \tfrac{1}{3(n-r)^3} + \tfrac{4}{r(2n-\sqrt{n})} - \tfrac{1}{2r^2} + \tfrac{2n-\sqrt{n}}{24r^3} > 0
\end{aligned}
$$

$$
\begin{aligned}
h(r) &= f(\tfrac{2}{r}, r, 1) \\
&= \tfrac{n-r}{2}\log(n-r) - \tfrac{n-r}{2}\log(2) - \tfrac{n-r}{2} + \tfrac{1}{2}\log(\pi(n-r)) + \tfrac{1}{6(n-r)} + 3.5 \\
&\quad + \tfrac{r}{2}\log(\tfrac{r}{2}) - \tfrac{r}{2} + \tfrac{1}{2}\log(r\pi) + \tfrac{1}{6r} \\
&\quad + 2\log(2) - 2 + \tfrac{1}{2}\log(4\pi) + \tfrac{1}{24} \\
h'(r) &= -\tfrac{1}{2}\log(n-r) + \tfrac{1}{2}\log(2) - \tfrac{1}{2(n-r)} + \tfrac{1}{6(n-r)^2} \\
&\quad + \tfrac{1}{2}\log(\tfrac{r}{2}) + \tfrac{1}{2r} - \tfrac{1}{6r^2} \\
h''(r) &= \tfrac{1}{2(n-r)} - \tfrac{1}{2(n-r)^2} + \tfrac{1}{3(n-r)^3} + \tfrac{1}{2r} - \tfrac{1}{2r^2} + \tfrac{1}{3r^3} > 0
\end{aligned}
$$

This gives the following values of (m, r, u) for which $f(t, r, u)$ is maximised:

- $(5, n^{\frac{1}{4}}, \frac{n^{\frac{1}{4}}}{10})$
- $(5, n, \frac{n}{50})$
- $(5, n-1, \frac{n-1}{10})$
- $(\frac{1}{2}\left(n - \frac{\sqrt{n}}{2}\right), n - \frac{\sqrt{n}}{2}, 1)$
- $(\frac{1}{2}\left(n - \frac{\sqrt{n}}{2}\right), n, \frac{2n}{2n-\sqrt{n}})$
- $(\frac{1}{2}\left(n - \frac{\sqrt{n}}{2}\right), n-1, \frac{2n}{2n-\sqrt{n}})$
- $(\frac{n^{\frac{1}{4}}}{2}, n^{\frac{1}{4}}, 1)$

All are below $\log(|B_n|)$.

Case 3.b. $u > \frac{r}{2m}$:

If $u > \frac{r}{2m}$ then there are at least $2u - \frac{r}{m}$ copies of A_m in N which act non-trivially on just one orbit of $A_m^{\frac{r}{m}}$. By Lemma 3.1.3 any preimage of any such copy of A_m must act on an orbit Ω of L_I not contained in Γ_I. Fix such an Ω.

Let M be a minimal subgroup of $(L_I)_{(\mathcal{B}_I)}$ such that $M^{\Gamma_I} = N$ and denote by $\phi : M \to A_m^{\frac{r}{m}}$ the natural projection defined by action on Γ_I. Denote $N = N_1 \times \cdots \times N_u$ with $N_i \cong A_m$ for each i. Reordering if necessary, we may assume that $\phi^{-1}(N_i)^\Omega > \ker(\phi)^\Omega$ (so $\phi^{-1}(N_i)^\Omega / \ker(\phi)^\Omega \cong A_m$) for $i = 1, \dots, s$ and $\phi^{-1}(N_i)^\Omega = \ker(\phi)^\Omega$ for $i = s+1, \dots, u$.

If $M^\Omega / \ker(\phi)^\Omega \ncong A_m^s$ then $K = \{x \in N_1 \times \cdots \times N_s | \phi^{-1}(x)^\Omega = \ker(\phi)^\Omega\}$ is non-trivial. Relabelling if necessary we may assume that K projects trivially onto $N_1, \dots, N_t$ and projects non-trivially onto $N_{t+1}, \dots, N_s$. Let

$$M_0 = \langle \phi^{-1}(N_1 \times \cdots \times N_t \times N_{s+1} \times \cdots \times N_u), \phi^{-1}(K)^M \rangle$$

Clearly $M_0^{\Gamma_i} = N$ and, using $\phi^{-1}(K)^\Omega = \ker(\phi)^\Omega$, we have $M_0 < M$ contrary to assumption. Hence we have $M^\Omega / \ker(\phi)^\Omega \cong A_m^s$. Let Δ' be the union of orbits of L_I on which M acts non-trivially.

If $g \in (L_I)_{(\mathcal{B}_I)}$ with $g^{\Gamma_I} \neq 1$ then we can choose $h \in M$ with $[h^{\Gamma_I}, g^{\Gamma_I}]$ acts non-trivially on the same blocks in Γ_i as g. Suppose g acts trivially on Δ'. Then so does $[h^{\Gamma_I}, g^{\Gamma_I}]$, but h acts non-trivially only on $\Gamma_I \cup \Delta'$, so $[h^{\Gamma_I}, g^{\Gamma_I}]$ acts non-trivially only on Γ_I. By Lemma 3.1.14, $[h^{\Gamma_I}, g^{\Gamma_I}]$ must act diagonally on some orbits or blocks of size m, so g must also. Therefore if a copy of A_m appearing in $N \cong A_m^u$ acts on only one orbit of $A_m^{\frac{r}{m}}$ then it must act non-trivially on Δ'.

Fix such a copy N_0 of A_m and let $\Delta'' \subseteq \Delta'$ be the union of orbits of L_I on which N_0 acts non-trivially. Fix an orbit $\Omega \subseteq \Delta''$ of L_I. Then since N_0 acts non-trivially on Ω, L_I^Ω has A_m as a chief factor. By Lemma 3.1.28, denoting $s = |\Omega|$ either L_I^Ω is primitive, embeds into $S_2 \wr S_m$ or

$$\log(|L_I^\Omega|) \leq \frac{s}{2}\log(\frac{s}{2}) - \frac{s}{2} + \log(\pi\frac{s}{2}) + \frac{1}{3s} + \log(2) + 16$$

Suppose L_I^Ω embeds into $S_2 \wr S_m$ for each such Ω and let $g_1, g_2 \in N_0$ identify with $(1,2,3)$ and $(3,4,5)$ in A_m respectively. Replacing g_1 and g_2 with g_1^4 and g_2^4 respectively if necessary, the image of g_1 and g_2 in $S_2 \wr S_m$ through each L_I^Ω must, after appropriate numbering, be $(1,3,5)(2,4,6)$ and $(5,7,9)(6,8,10)$ respectively. The image of $g_1(g_1)^{g_2}$ in $S_2 \wr S_m$ through each L_I^Ω is then $(1,7)(2,8)(3,5)(4,6)$, but the image of $g_1(g_1)^{g_2}$ in A_m is $(1,4)(2,3)$. This means that $g_1(g_1)^{g_2}$ is a product of 2 (mod 4) transpositions, contradicting Proposition 3.1.3. Hence there is some orbit, which we denote by Δ, such that, with either L_I^Δ primitive or with $s = |\Delta|$,

$$\log(|L_I^\Delta|) \leq \frac{s}{2}\log(\frac{s}{2}) - \frac{s}{2} + \log(\pi\frac{s}{2}) + \frac{1}{3s} + \log(2) + 16$$

If L_I^Δ is primitive and $L_I^\Delta \geq A_{|\Delta|}$ then $(L_I)_{(\mathcal{B}_I)} \geq A_{|\Delta|}$, $m = |\Delta|$ and L_I^Δ therefore has an orbit of size m containing A_m contrary to assumption. So if L_I^Δ is primitive then L_I^Δ does not contain $A_{|\Delta|}$ and therefore has size at most $3^{|\Delta|}$.

Case 3.b.i L_I^Δ Primitive:

$$\begin{aligned}
\log(|L_I|) &= \log(|(L_I)_{(\Gamma_I\cup\Delta)}|) + \log(|((L_I)_{(\Delta)})^{\Gamma_I}|) + \log(|L_I^\Delta|) \\
&\leq f(r,s,m) \\
&= \tfrac{n-r-s}{2}\log(n-r-s) - \tfrac{n-r-s}{2}\log(2) - \tfrac{n-r-s}{2} \\
&\quad + \tfrac{1}{2}\log(\pi(n-r-s)) + \tfrac{1}{6(n-r-s)} + 3.5 \\
&\quad + \tfrac{r}{2}\log(m) - \tfrac{r}{2} + \tfrac{r}{4m}\log(2\pi m) + \tfrac{r}{24m^2} \\
&\quad + \tfrac{r}{m}\log(\tfrac{r}{m}) - \tfrac{r}{m} + \tfrac{1}{2}\log(2\pi\tfrac{r}{m}) + \tfrac{m}{12r} + s\log(3) \\
\tfrac{\partial f}{\partial s} &= -\tfrac{1}{2}\log(n-r-s) + \tfrac{1}{2}\log(2) - \tfrac{1}{2(n-r-s)} + \tfrac{1}{6(n-r-s)^2} + \log(3) \\
\tfrac{\partial^2 f}{\partial s^2} &= \tfrac{1}{2(n-r-s)} - \tfrac{1}{2(n-r-s)^2} + \tfrac{1}{3(n-r-s)^3} > 0
\end{aligned}$$

so $f(r,s,m)$ is maximised by either $s = m$, $s = n-r-1$ or $s = n-r$. If $s = m$ then

$$\begin{aligned}
g(r,m) &= f(r,m,m) \\
&= \tfrac{n-r-m}{2}\log(n-r-m) - \tfrac{n-r-m}{2}\log(2) - \tfrac{n-r-m}{2} \\
&\quad + \tfrac{1}{2}\log(\pi(n-r-m)) + \tfrac{1}{6(n-r-m)} + 3.5 \\
&\quad + \tfrac{r}{2}\log(m) - \tfrac{r}{2} + \tfrac{r}{4m}\log(2\pi m) + \tfrac{r}{24m^2} \\
&\quad + \tfrac{r}{m}\log(\tfrac{r}{m}) - \tfrac{r}{m} + \tfrac{1}{2}\log(2\pi\tfrac{r}{m}) + \tfrac{m}{12r} + m\log(3) \\
\tfrac{\partial g}{\partial r} &= -\tfrac{1}{2}\log(n-r-m) + \tfrac{1}{2}\log(2) - \tfrac{1}{2(n-r-m)} + \tfrac{1}{6(n-r-m)^2} \\
&\quad + \tfrac{1}{2}\log(m) - \tfrac{1}{2} + \tfrac{1}{4m}\log(2\pi m) + \tfrac{1}{24m^2} + \tfrac{1}{m}\log(\tfrac{r}{m}) + \tfrac{1}{2r} - \tfrac{m}{12r^2} \\
\tfrac{\partial^2 g}{\partial r^2} &= \tfrac{1}{2(n-r-m)} - \tfrac{1}{2(n-r-m)^2} + \tfrac{1}{3(n-r-m)^3} + \tfrac{1}{rm} - \tfrac{1}{2r^2} + \tfrac{m}{6r^3} > 0
\end{aligned}$$

so $g(r,m)$ is maximised by either $r = m$, $r = n-m-1$ or $r = n-m$. If $r = m$ then

$$\begin{aligned}
h(m) &= f(m,m,m) \\
&= \tfrac{n-2m}{2}\log(n-2m) - \tfrac{n-2m}{2}\log(2) - \tfrac{n-2m}{2} \\
&\quad + \tfrac{1}{2}\log(\pi(n-2m)) + \tfrac{1}{6(n-2m)} + 3.5 \\
&\quad + \tfrac{m}{2}\log(m) - \tfrac{m}{2} + \tfrac{1}{4}\log(2\pi m) + \tfrac{1}{24m} \\
&\quad -1 + \tfrac{1}{2}\log(2\pi) + \tfrac{1}{12} + m\log(3) \\
h'(m) &= -\log(n-2m) + \log(2) - \tfrac{1}{n-2m} + \tfrac{1}{3(n-2m)^2} + \tfrac{1}{2}\log(m) + \tfrac{1}{4m} - \tfrac{1}{24m^2} \\
h''(m) &= \tfrac{2}{n-2m} - \tfrac{2}{(n-2m)^2} + \tfrac{4}{3(n-2m)^3} + \tfrac{1}{2m} - \tfrac{1}{4m^2} + \tfrac{1}{12m^3} > 0
\end{aligned}$$

so $h(m)$ is maximised by $m = n^{\frac{1}{3}}$, $m = \frac{n-1}{2}$ or $m = \frac{n}{2}$. In each case the bound is below $\log(|B_n|)$.

If instead $r = n - m - 1$ then, setting $t = \frac{1}{m}$,

$$
\begin{aligned}
h(t) &= f(n-m-1, m, m) \\
&= \tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 3.5 \\
&\quad + \tfrac{(n-m-1)}{2}\log(m) - \tfrac{(n-m-1)}{2} + \tfrac{n-m-1}{4m}\log(2\pi m) + \tfrac{n-m-1}{24m^2} \\
&\quad + \tfrac{n-m-1}{m}\log(\tfrac{n-m-1}{m}) - \tfrac{n-m-1}{m} + \tfrac{1}{2}\log(2\pi\tfrac{n-m-1}{m}) + \tfrac{m}{12(n-m-1)} + m\log(3) \\
&= \tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 3.5 - \tfrac{(n-\frac{1}{t}-1)}{2}\log(t) - \tfrac{(n-\frac{1}{t}-1)}{2} \\
&\quad - (\tfrac{nt}{4} - \tfrac{1}{2} - \tfrac{t}{4})\log(\tfrac{t}{2\pi}) + \tfrac{nt^2}{24} \\
&\quad - \tfrac{t}{24} - \tfrac{t^2}{24} + (nt-1-t)\log(nt-1-t) - (nt-1-t) \\
&\quad + \tfrac{1}{2}\log(2\pi(nt-1-t)) + \tfrac{1}{12(nt-1-t)} + \tfrac{\log(3)}{t} \\
h'(t) &= -\tfrac{n-1}{2t} - \tfrac{1}{2t^2}\log(t) - \tfrac{n}{4} + \tfrac{1}{2t} + \tfrac{1}{4} - (\tfrac{n}{4} - \tfrac{1}{4})\log(\tfrac{t}{2\pi}) + \tfrac{nt}{12} - \tfrac{1}{24} - \tfrac{t}{12} \\
&\quad + (n-1)\log(nt-1-t) + \tfrac{n-1}{2(nt-1-t)} - \tfrac{n-1}{12(nt-1-t)^2} - \tfrac{\log(3)}{t^2} \\
h''(t) &= \tfrac{n-1}{2t^2} - \tfrac{1}{2t^3} + \tfrac{1}{t^3}\log(t) - \tfrac{1}{2t^2} - \tfrac{n}{4t} + \tfrac{1}{4t} + \tfrac{n}{12} - \tfrac{1}{12} \\
&\quad + \tfrac{(n-1)^2}{nt-1-t} - \tfrac{(n-1)^2}{2(nt-1-t)^2} + \tfrac{(n-1)^2}{6(nt-1-t)^3} + \tfrac{2\log(3)}{t^3} > 0
\end{aligned}
$$

so $h(m)$ is maximised by $m = n^{\frac{1}{3}}$ or $m = \frac{n-1}{2}$. In each case the bound is below $\log(|B_n|)$.

If instead $r = n - m$ then, setting $t = \frac{1}{m}$,

$$
\begin{aligned}
h(t) &= f(n-m, m, m) \\
&\quad \tfrac{(n-m)}{2}\log(m) - \tfrac{(n-m)}{2} + \tfrac{n-m}{4m}\log(2\pi m) + \tfrac{n-m}{24m^2} \\
&\quad + \tfrac{n-m}{m}\log(\tfrac{n-m}{m}) - \tfrac{n-m}{m} + \tfrac{1}{2}\log(2\pi\tfrac{n-m}{m}) + \tfrac{m}{12(n-m)} + m\log(3) \\
&= -\tfrac{(n-\frac{1}{t})}{2}\log(t) - \tfrac{(n-\frac{1}{t})}{2} \\
&\quad - (\tfrac{nt}{4} - \tfrac{1}{2})\log(\tfrac{t}{2\pi}) + \tfrac{nt^2}{24} \\
&\quad - \tfrac{t}{24} + (nt-1)\log(nt-1) - (nt-1) \\
&\quad + \tfrac{1}{2}\log(2\pi(nt-1)) + \tfrac{1}{12(nt-1)} + \tfrac{\log(3)}{t} \\
h'(t) &= -\tfrac{n}{2t} - \tfrac{1}{2t^2}\log(t) - \tfrac{n}{4} + \tfrac{1}{2t} + \tfrac{1}{4} - \tfrac{n}{4}\log(\tfrac{t}{2\pi}) + \tfrac{nt}{12} - \tfrac{1}{24} \\
&\quad + n\log(nt-1) + \tfrac{n}{2(nt-1)} - \tfrac{n}{12(nt-1)^2} - \tfrac{\log(3)}{t^2} \\
h''(t) &= \tfrac{n}{2t^2} - \tfrac{1}{2t^3} + \tfrac{1}{t^3}\log(t) - \tfrac{1}{2t^2} - \tfrac{n}{4t} + \tfrac{n}{12} \\
&\quad + \tfrac{n^2}{nt-1} - \tfrac{n^2}{2(nt-1)^2} + \tfrac{n^2}{6(nt-1)^3} + \tfrac{2\log(3)}{t^3} > 0
\end{aligned}
$$

so $h(m)$ is maximised by $m = n^{\frac{1}{3}}$ or $m = \frac{n}{2}$. In each case the bound is below $\log(|B_n|)$.

If instead $s = n - r - 1$ then

$$
\begin{aligned}
g(r,m) &= f(r, n-r-1, m) \\
&= -\tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 3.5 \\
&\quad + \tfrac{r}{2}\log(m) - \tfrac{r}{2} + \tfrac{r}{4m}\log(2\pi m) + \tfrac{r}{24m^2} \\
&\quad + \tfrac{r}{m}\log(\tfrac{r}{m}) - \tfrac{r}{m} + \tfrac{1}{2}\log(2\pi\tfrac{r}{m}) + \tfrac{m}{12r} + (n-r-1)\log(3) \\
\frac{\partial g}{\partial r} &= \tfrac{1}{2}\log(m) - \tfrac{1}{2} + \tfrac{1}{4m}\log(2\pi m) + \tfrac{1}{24m^2} + \tfrac{1}{m}\log(\tfrac{r}{m}) + \tfrac{1}{2r} - \tfrac{m}{12r^2} - \log(3) \\
\frac{\partial^2 g}{\partial r^2} &= \tfrac{1}{mr} - \tfrac{1}{2r^2} + \tfrac{m}{6r^3} > 0
\end{aligned}
$$

so $g(r,m)$ is maximised by $r = m$ or $r = n - m$. If $r = m$ then

$$
\begin{aligned}
h(m) &= f(m, n-m-1, m) \\
&= -\tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 3.5 + \tfrac{m}{2}\log(m) - \tfrac{m}{2} \\
&\quad + \tfrac{1}{4}\log(2\pi m) + \tfrac{1}{24m} - 1 + \tfrac{1}{2}\log(2\pi) + \tfrac{1}{12} + (n-m-1)\log(3) \\
h'(m) &= \tfrac{1}{2}\log(m) + \tfrac{1}{4m} - \tfrac{1}{24m^2} - \log(3)
\end{aligned}
$$

One can check that $h'(m) < 0$ if and only if $m < 9$, so $h(m)$ is maximised by either $m = n^{\frac{1}{3}}$ or $m = \frac{n-1}{2}$. In each case the bound is below $\log(|B_n|)$.

If instead $r = n - m$ then setting $t = \frac{1}{m}$

$$
\begin{aligned}
h(t) &= f(n - t^{-1}, t^{-1} - 1, t^{-1}) \\
&= -\tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 3.5 \\
&\quad - \tfrac{(n-t^{-1})}{2}\log(t) - \tfrac{n-t^{-1}}{2} - \tfrac{nt-1}{4}\log(\tfrac{t}{2\pi}) + \tfrac{nt^2-t}{24} \\
&\quad + (nt-1)\log(nt-1) - (nt-1) + \tfrac{1}{2}\log(2\pi(nt-1)) \\
&\quad + \tfrac{1}{12(nt-1)} + (t^{-1}-1)\log(3) \\
h'(t) &= -\tfrac{n}{2t} - \tfrac{1}{2t^2}\log(t) + \tfrac{1}{4t} - \tfrac{n}{4} - \tfrac{n}{4}\log(\tfrac{t}{2\pi}) + \tfrac{nt}{12} - \tfrac{1}{24} \\
&\quad + n\log(nt-1) + \tfrac{n}{2(nt-1)} - \tfrac{n}{12(nt-1)^2} - \tfrac{1}{t^2}\log(3) \\
h''(t) &= \tfrac{n}{2t^2} - \tfrac{1}{2t^3} + \tfrac{1}{t^3}\log(t) - \tfrac{1}{4t^2} - \tfrac{n}{4t} + \tfrac{n}{12} + \tfrac{n^2}{(nt-1)} - \tfrac{n^2}{2(nt-1)^2} + \tfrac{n^2}{6(nt-1)^3} + \tfrac{2}{t^3}\log(3) \\
&= m^3(\tfrac{n}{2m} + 2\log(3) - \tfrac{1}{2} - \log(m) - \tfrac{1}{4m} - \tfrac{n}{4m^2}) + \tfrac{n}{12} + \tfrac{n^2}{(nt-1)} - \tfrac{n^2}{2(nt-1)^2} + \tfrac{n^2}{6(nt-1)^3}
\end{aligned}
$$

If $m \leq \frac{n}{2\log(n)}$ we can see that $h''(t) > 0$ and if $m \geq \frac{n}{2\log(n)}$ then $\frac{2}{n-1} \leq t \leq \frac{2\log(n)}{n}$ gives

$$
\begin{aligned}
h'(t) \geq &-\tfrac{n(n-1)}{4} - \tfrac{(n-1)^2}{8}\log(\tfrac{2}{n-1}) + \tfrac{n}{8\log(n)} - \tfrac{n}{4} - \tfrac{n}{4}\log(\tfrac{\log(n)}{\pi n}) + \tfrac{n}{6(n-1)} - \tfrac{1}{24} \\
&+ \tfrac{n}{2(2\log(n)-1)} - \tfrac{n}{12(n\frac{2}{n-1}-1)^2} - \tfrac{(n-1)^2}{4}\log(3) \\
> &\ 0
\end{aligned}
$$

so $h(t)$ is maximised by $m = n^{\frac{1}{3}}$. In which case the bound is below $\log(|B_n|)$.

If instead $s = n - r$ then

$$\begin{aligned}
g(r,m) &= f(r, n-r-1, m) \\
&= \tfrac{r}{2}\log(m) - \tfrac{r}{2} + \tfrac{r}{4m}\log(2\pi m) + \tfrac{r}{24m^2} \\
&\quad + \tfrac{r}{m}\log(\tfrac{r}{m}) - \tfrac{r}{m} + \tfrac{1}{2}\log(2\pi\tfrac{r}{m}) + \tfrac{m}{12r} + (n-r)\log(3) \\
\tfrac{\partial g}{\partial r} &= \tfrac{1}{2}\log(m) - \tfrac{1}{2} + \tfrac{1}{4m}\log(2\pi m) + \tfrac{1}{24m^2} + \tfrac{1}{m}\log(\tfrac{r}{m}) + \tfrac{1}{2r} - \tfrac{m}{12r^2} - \log(3) \\
\tfrac{\partial^2 g}{\partial r^2} &= \tfrac{1}{mr} - \tfrac{1}{2r^2} + \tfrac{m}{6r^3} > 0
\end{aligned}$$

so $g(r,m)$ is maximised by $r = m$ or $r = n - m$. If $r = m$ then

$$\begin{aligned}
h(m) &= f(m, n-m-1, m) \\
&= \tfrac{m}{2}\log(m) - \tfrac{m}{2} \\
&\quad + \tfrac{1}{4}\log(2\pi m) + \tfrac{1}{24m} - 1 + \tfrac{1}{2}\log(2\pi) + \tfrac{1}{12} + (n-m)\log(3) \\
h'(m) &= \tfrac{1}{2}\log(m) + \tfrac{1}{4m} - \tfrac{1}{24m^2} - \log(3)
\end{aligned}$$

One can check that $h'(m) < 0$ if and only if $m < 9$, so $h(m)$ is maximised by either $m = n^{\frac{1}{3}}$ or $m = \frac{n}{2}$. In each case the bound is below $\log(|B_n|)$.

If instead $r = n - m$ then setting $t = \frac{1}{m}$

$$\begin{aligned}
h(t) &= f(n - t^{-1}, t^{-1} - 1, t^{-1}) \\
&= -\tfrac{(n-t^{-1})}{2}\log(t) - \tfrac{n-t^{-1}}{2} - \tfrac{nt-1}{4}\log(\tfrac{t}{2\pi}) + \tfrac{nt^2-t}{24} \\
&\quad + (nt-1)\log(nt-1) - (nt-1) + \tfrac{1}{2}\log(2\pi(nt-1)) \\
&\quad + \tfrac{1}{12(nt-1)} \\
h'(t) &= -\tfrac{n}{2t} - \tfrac{1}{2t^2}\log(t) + \tfrac{1}{4t} - \tfrac{n}{4} - \tfrac{n}{4}\log(\tfrac{t}{2\pi}) + \tfrac{nt}{12} - \tfrac{1}{24} \\
&\quad + n\log(nt-1) + \tfrac{n}{2(nt-1)} - \tfrac{n}{12(nt-1)^2} \\
h''(t) &= \tfrac{n}{2t^2} - \tfrac{1}{2t^3} + \tfrac{1}{t^3}\log(t) - \tfrac{1}{4t^2} - \tfrac{n}{4t} + \tfrac{n}{12} + \tfrac{n^2}{(nt-1)} - \tfrac{n^2}{2(nt-1)^2} + \tfrac{n^2}{6(nt-1)^3} \\
&= m^3(\tfrac{n}{2m} - \tfrac{1}{2} - \log(m) - \tfrac{1}{4m} - \tfrac{n}{4m^2}) + \tfrac{n}{12} + \tfrac{n^2}{(nt-1)} - \tfrac{n^2}{2(nt-1)^2} + \tfrac{n^2}{6(nt-1)^3}
\end{aligned}$$

If $m \leq \frac{n}{2\log(n)}$ we can see that $h''(t) > 0$ and if $m \geq \frac{n}{2\log(n)}$ then $\frac{2}{n-1} \leq t \leq \frac{2\log(n)}{n}$ gives

$$\begin{aligned}
h'(t) \geq\ & -\tfrac{n(n-1)}{4} - \tfrac{(n-1)^2}{8}\log(\tfrac{2}{n-1}) + \tfrac{n}{8\log(n)} - \tfrac{n}{4} - \tfrac{n}{4}\log(\tfrac{\log(n)}{\pi n}) + \tfrac{n}{6(n-1)} - \tfrac{1}{24} \\
& + \tfrac{n}{2(2\log(n)-1)} - \tfrac{n}{12(n\frac{2}{n-1}-1)^2} \\
>\ & 0
\end{aligned}$$

so $h(t)$ is maximised by $m = n^{\frac{1}{3}}$. In which case the bound is below $\log(|B_n|)$.

Case 3.b.ii L_I^Δ Imprimitive

$$\begin{array}{rcl}
\log(|L_I|) & = & \log(|(L_I)_{(\Gamma_I\cup\Delta)}|)+\log(|((L_I)_{(\Delta)})^{\Gamma_I}|)+\log(|L_I^\Delta|)\\
& \leq & f(r,s,m)\\
& = & \frac{n-r-s}{2}\log(n-r-s)-\frac{n-r-s}{2}\log(2)-\frac{n-r-s}{2}\\
& & +\frac{1}{2}\log(\pi(n-r-s))+\frac{1}{6(n-r-s)}+3.5\\
& & +\frac{r}{2}\log(m)-\frac{r}{2}+\frac{r}{4m}\log(2\pi m)+\frac{1}{24m^2}\\
& & +\frac{r}{m}\log(\frac{r}{m})-\frac{r}{m}+\frac{1}{2}\log(2\pi\frac{r}{m})+\frac{m}{12r}\\
& & +\frac{s}{2}\log(\frac{s}{2})-\frac{s}{2}+\log(\pi\frac{s}{2})+\frac{1}{3s}+\log(2)+16\\
\frac{\partial f}{\partial s} & = & -\frac{1}{2}\log(n-r-s)+\frac{1}{2}\log(2)-\frac{1}{2(n-r-s)}+\frac{1}{6(n-r-s)^2}\\
& & +\frac{1}{2}\log(\frac{s}{2})+\frac{1}{s}-\frac{1}{3s^2}\\
\frac{\partial^2 f}{\partial s^2} & = & \frac{1}{2(n-r-s)}-\frac{1}{2(n-r-s)^2}+\frac{1}{3(n-r-s)^3}+\frac{1}{2s}-\frac{1}{s^2}+\frac{2}{3s^3}>0
\end{array}$$

so for fixed r,m $f(r,s,m)$ is maximised by either $s=2m$, $s=n-r-1$ or $s=n-r$. If $s=2m$ then

$$\begin{array}{rcl}
g(r,m) & = & f(r,2m,m)\\
& = & \frac{n-r-2m}{2}\log(n-r-2m)-\frac{n-r-2m}{2}\log(2)-\frac{n-r-2m}{2}\\
& & +\frac{1}{2}\log(\pi(n-r-2m))+\frac{1}{6(n-r-2m)}+3.5\\
& & +\frac{r}{2}\log(m)-\frac{r}{2}+\frac{r}{4m}\log(2\pi m)+\frac{r}{24m^2}\\
& & +\frac{r}{m}\log(\frac{r}{m})-\frac{r}{m}+\frac{1}{2}\log(2\pi\frac{r}{m})+\frac{m}{12r}\\
& & +m\log(m)-m+\log(\pi m)+\frac{1}{6m}+\log(2)+16\\
\frac{\partial g}{\partial r} & = & -\frac{1}{2}\log(n-r-2m)+\frac{1}{2}\log(2)-\frac{1}{2(n-r-2m)}+\frac{1}{6(n-r-2m)^2}\\
& & +\frac{1}{2}\log(m)-\frac{1}{2}+\frac{1}{4m}\log(2\pi m)+\frac{1}{24m^2}+\frac{1}{m}\log(\frac{r}{m})+\frac{1}{2r}-\frac{m}{12r^2}\\
\frac{\partial^2 g}{\partial r^2} & = & \frac{1}{2(n-r-2m)}-\frac{1}{2(n-r-2m)^2}+\frac{1}{3(n-r-2m)^3}+\frac{1}{mr}-\frac{1}{2r^2}+\frac{m}{6r^3}>0
\end{array}$$

so $g(r,m)$ is maximised by $r=m$, $r=n-2m-1$ or $r=n-2m$. If $r=m$ then

$$\begin{array}{rcl}
h(m) & = & f(m,2m,m)\\
& = & \frac{n-3m}{2}\log(n-3m)-\frac{n-3m}{2}\log(2)-\frac{n-3m}{2}\\
& & +\frac{1}{2}\log(\pi(n-3m))+\frac{1}{6(n-3m)}+3.5+\frac{m}{2}\log(m)-\frac{m}{2}\\
& & +\frac{1}{4}\log(2\pi m)+\frac{1}{24m}-1+\frac{1}{2}\log(2\pi)+\frac{1}{12}\\
& & +m\log(m)-m+\log(\pi m)+\frac{1}{6m}+\log(2)+16\\
h'(m) & = & -\frac{3}{2}\log(n-3m)+\frac{3}{2}\log(2)-\frac{3}{2(n-3m)}+\frac{1}{2(n-3m)^2}\\
& & +\frac{1}{2}\log(m)+\frac{1}{4m}-\frac{1}{24m^2}\\
& & +\log(m)+\frac{1}{m}-\frac{1}{6m^2}\\
h''(m) & = & \frac{9}{2(n-3m)}-\frac{9}{2(n-3m)^2}+\frac{3}{(n-3m)^3}+\frac{3}{2m}-\frac{5}{4m^2}+\frac{1}{3m^3}>0
\end{array}$$

so $h(m)$ is maximised by $m=n^{\frac{1}{3}}$, $m=\frac{n-1}{4}$ or $m=\frac{n}{4}$. In each case the bound is below $\log(|H|)$.

If instead $r = n-2m-1$ then

$$\begin{aligned}
h(m) &= f(n-2m-1, 2m, m) \\
&= -\tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 3.5 + \tfrac{n-2m-1}{2}\log(m) \\
&\quad -\tfrac{n-2m-1}{2} + \tfrac{n-2m-1}{4m}\log(2\pi m) + \tfrac{n-2m-1}{24m^2} \\
&\quad +\tfrac{n-2m-1}{m}\log(\tfrac{n-2m-1}{m}) - \tfrac{n-2m-1}{m} + \tfrac{1}{2}\log(2\pi\tfrac{n-2m-1}{m}) + \tfrac{m}{12(n-2m-1)} \\
&\quad +m\log(m) - m + \log(\pi m) + \tfrac{1}{6m} + \log(2) + 16 \\
h'(m) &= \tfrac{n-1}{2m} - \log(m) + \tfrac{n-2m-1}{4m^2} - \tfrac{n-1}{4m^2}\log(2\pi m) - \tfrac{n-1}{12m^3} + \tfrac{1}{12m^2} \\
&\quad -\tfrac{n-1}{m^2}\log(\tfrac{n-2m-1}{m}) - \tfrac{n-1}{2m(n-2m-1)} + \tfrac{n-1}{12(n-2m-1)^2} \\
&\quad +\log(m) + \tfrac{1}{m} - \tfrac{1}{6m^2} \\
h''(m) &= -\tfrac{n-1}{2m^2} - \tfrac{n-1}{2m^3} + \tfrac{1}{2m^2} - \tfrac{n-1}{4m^3} + \tfrac{n-1}{2m^3}\log(2\pi m) + \tfrac{n-1}{4m^4} - \tfrac{1}{6m^3} + \tfrac{(n-1)^2}{m^3(n-2m-1)} \\
&\quad +\tfrac{2(n-1)}{m^3}\log(\tfrac{n-2m-1}{m}) + \tfrac{(n-1)(n-4m-1)}{2m^2(n-2m-1)^2} + \tfrac{n-1}{3(n-2m-1)^3} - \tfrac{1}{m^2} + \tfrac{1}{6m^3}
\end{aligned}$$

Notice that

$$\begin{aligned}
h'(m) + mh''(m) &= \tfrac{1}{2m} - \tfrac{n-1}{2m^2} + \tfrac{n-1}{4m^2}\log(2\pi m) + \tfrac{n-1}{6m^3} - \tfrac{1}{12m^2} + \tfrac{(n-1)^2}{m^3(n-2m-1)} \\
&\quad +\tfrac{n-1}{m^2}\log(\tfrac{n-2m-1}{m}) - \tfrac{n-1}{2m(n-2m-1)} + \tfrac{n-1}{12(n-2m-1)^2} \\
&\quad +\tfrac{(n-1)(n-4m-1)}{2m(n-2m-1)^2} + \tfrac{m(n-1)}{3(n-2m-1)^3} + \tfrac{1}{12m^2} > 0
\end{aligned}$$

so at all times either $h'(m) > 0$ or $h''(m) > 0$ which is only possible if $h(m)$ is maximised by either $m = n^{\frac{1}{3}}$ or $m = \frac{n-1}{3}$. In each case the bound is below $\log(|B_n|)$.

If instead $r = n-2m$ then

$$\begin{aligned}
h(m) &= f(n-2m, 2m, m) \\
&= \tfrac{n-2m}{2}\log(m) - \tfrac{n-2m}{2} + \tfrac{n-2m}{4m}\log(2\pi m) + \tfrac{n-2m}{24m^2} \\
&\quad +\tfrac{n-2m}{m}\log(\tfrac{n-2m}{m}) - \tfrac{n-2m}{m} + \tfrac{1}{2}\log(2\pi\tfrac{n-2m}{m}) + \tfrac{m}{12(n-2m)} \\
&\quad +m\log(m) - m + \log(\pi m) + \tfrac{1}{6m} + \log(2) + 16 \\
h'(m) &= \tfrac{n}{2m} - \log(m) + \tfrac{n-2m}{4m^2} - \tfrac{n}{4m^2}\log(2\pi m) - \tfrac{n}{12m^3} + \tfrac{1}{12m^2} \\
&\quad -\tfrac{n}{m^2}\log(\tfrac{n-2m}{m}) - \tfrac{n}{2m(n-2m)} + \tfrac{n}{12(n-2m)^2} \\
&\quad +\log(m) + \tfrac{1}{m} - \tfrac{1}{6m^2} \\
h''(m) &= -\tfrac{n}{2m^2} - \tfrac{n}{2m^3} + \tfrac{1}{2m^2} - \tfrac{n}{4m^3} + \tfrac{n}{2m^3}\log(2\pi m) + \tfrac{n}{4m^4} - \tfrac{1}{6m^3} + \tfrac{n^2}{m^3(n-2m)} \\
&\quad +\tfrac{2n}{m^3}\log(\tfrac{n-2m}{m}) + \tfrac{n(n-4m)}{2m^2(n-2m)^2} + \tfrac{n}{3(n-2m)^3} - \tfrac{1}{m^2} + \tfrac{1}{6m^3}
\end{aligned}$$

Notice that

$$\begin{aligned}
h'(m) + mh''(m) &= \tfrac{1}{2m} - \tfrac{n}{2m^2} + \tfrac{n}{4m^2}\log(2\pi m) + \tfrac{n}{6m^3} - \tfrac{1}{12m^2} + \tfrac{n^2}{m^3(n-2m)} \\
&\quad +\tfrac{n}{m^2}\log(\tfrac{n-2m}{m}) - \tfrac{n}{2m(n-2m)} + \tfrac{n}{12(n-2m)^2} \\
&\quad +\tfrac{n(n-4m)}{2m(n-2m)^2} + \tfrac{mn}{3(n-2m)^3} + \tfrac{1}{12m^2} > 0
\end{aligned}$$

so at all times either $h'(m) > 0$ or $h''(m) > 0$ which is only possible if $h(m)$ is maximised by either $m = n^{\frac{1}{3}}$ or $m = \frac{n}{3}$. In each case the bound is below $\log(|B_n|)$.

If instead $s = n - r - 1$ then

$$\begin{aligned}
g(r,m) &= f(r, n-r-1, m) \\
&= -\tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 15 + \tfrac{r}{2}\log(m) - \tfrac{r}{2} \\
&\quad + \tfrac{r}{4m}\log(2\pi m) + \tfrac{r}{24m^2} + \tfrac{r}{m}\log(\tfrac{r}{m}) - \tfrac{r}{m} + \tfrac{1}{2}\log(2\pi\tfrac{r}{m}) + \tfrac{m}{12r} \\
&\quad + \tfrac{n-r-1}{2}\log(\tfrac{n-r-1}{2}) - \tfrac{n-r-1}{2} + \log(\pi(n-r-1)) + \tfrac{1}{3(n-r-1)} + \log(2) \\
\tfrac{\partial g}{\partial r} &= \tfrac{1}{2}\log(m) - \tfrac{1}{2} + \tfrac{1}{4m}\log(2\pi m) + \tfrac{1}{24m^2} + \tfrac{1}{m}\log(\tfrac{r}{m}) + \tfrac{1}{2r} \\
&\quad - \tfrac{m}{12r^2} - \tfrac{1}{2}\log(\tfrac{n-r-1}{2}) - \tfrac{1}{n-r-1} + \tfrac{1}{3(n-r-1)^2} \\
\tfrac{\partial^2 g}{\partial r^2} &= \tfrac{1}{rm} - \tfrac{1}{2r^2} + \tfrac{m}{6r^3} + \tfrac{1}{2(n-r-1)} - \tfrac{1}{(n-r-1)^2} + \tfrac{2}{3(n-r-1)^3} > 0
\end{aligned}$$

so $g(r,m)$ is maximised by $r = m$ or $r = n - 2m - 1$. If $r = m$ then

$$\begin{aligned}
h(m) &= f(m, n-m-1, m) \\
&= -\tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 15 + \tfrac{m}{2}\log(m) - \tfrac{m}{2} \\
&\quad + \tfrac{1}{4}\log(2\pi m) + \tfrac{1}{24m} - 1 + \tfrac{1}{2}\log(2\pi) + \tfrac{1}{12} + \tfrac{n-m-1}{2}\log(\tfrac{n-m-1}{2}) \\
&\quad - \tfrac{n-m-1}{2} + \log(\pi(n-m-1)) + \tfrac{1}{3(n-m-1)} + \log(2) \\
h'(m) &= \tfrac{1}{2}\log(m) + \tfrac{1}{4m} - \tfrac{1}{24m^2} - \tfrac{1}{2}\log(\tfrac{n-m-1}{2}) - \tfrac{1}{n-m-1} + \tfrac{1}{3(n-m-1)^2} \\
h''(m) &= \tfrac{1}{2m} - \tfrac{1}{4m^2} + \tfrac{1}{12m^3} + \tfrac{1}{2(n-m-1)} - \tfrac{1}{(n-m-1)^2} + \tfrac{2}{3(n-m-1)^3} > 0
\end{aligned}$$

so $h(m)$ is maximised by $m = n^{\frac{1}{3}}$ or $m = \frac{n-1}{3}$.In each case the bound is below $\log(|B_n|)$.

If instead $r = n - 2m - 1$ then $s = 2m = n - r - 1$ which we have already done.

If instead $s = n - r$ then

$$\begin{aligned}
g(r,m) &= f(r, n-r, m) \\
&= \tfrac{r}{2}\log(m) - \tfrac{r}{2} \\
&\quad + \tfrac{r}{4m}\log(2\pi m) + \tfrac{r}{24m^2} + \tfrac{r}{m}\log(\tfrac{r}{m}) - \tfrac{r}{m} + \tfrac{1}{2}\log(2\pi\tfrac{r}{m}) + \tfrac{m}{12r} \\
&\quad + \tfrac{n-r}{2}\log(\tfrac{n-r}{2}) - \tfrac{n-r}{2} + \log(\pi(n-r)) + \tfrac{1}{3(n-r)} + \log(2) + 16 \\
\tfrac{\partial g}{\partial r} &= \tfrac{1}{2}\log(m) - \tfrac{1}{2} + \tfrac{1}{4m}\log(2\pi m) + \tfrac{1}{24m^2} + \tfrac{1}{m}\log(\tfrac{r}{m}) + \tfrac{1}{2r} \\
&\quad - \tfrac{m}{12r^2} - \tfrac{1}{2}\log(\tfrac{n-r}{2}) - \tfrac{1}{n-r} + \tfrac{1}{3(n-r)^2} \\
\tfrac{\partial^2 g}{\partial r^2} &= \tfrac{1}{rm} - \tfrac{1}{2r^2} + \tfrac{m}{6r^3} + \tfrac{1}{2(n-r)} - \tfrac{1}{(n-r)^2} + \tfrac{2}{3(n-r)^3} > 0
\end{aligned}$$

so $g(r,m)$ is maximised by $r = m$ or $r = n - 2m$. If $r = m$ then

$$\begin{aligned}
h(m) &= f(m, n-m, m) \\
&= -\tfrac{1}{2}\log(2) - \tfrac{1}{2} + \tfrac{1}{2}\log(\pi) + \tfrac{1}{6} + 15 + \tfrac{m}{2}\log(m) - \tfrac{m}{2} \\
&\quad + \tfrac{1}{4}\log(2\pi m) + \tfrac{1}{24m} - 1 + \tfrac{1}{2}\log(2\pi) + \tfrac{1}{12} + \tfrac{n-m}{2}\log(\tfrac{n-m}{2}) \\
&\quad - \tfrac{n-m}{2} + \log(\pi(n-m)) + \tfrac{1}{3(n-m)} + \log(2) \\
h'(m) &= \tfrac{1}{2}\log(m) + \tfrac{1}{4m} - \tfrac{1}{24m^2} - \tfrac{1}{2}\log(\tfrac{n-m}{2}) - \tfrac{1}{n-m} + \tfrac{1}{3(n-m)^2} \\
h''(m) &= \tfrac{1}{2m} - \tfrac{1}{4m^2} + \tfrac{1}{12m^3} + \tfrac{1}{2(n-m)} - \tfrac{1}{(n-m)^2} + \tfrac{2}{3(n-m)^3} > 0
\end{aligned}$$

so $h(m)$ is maximised by $m = n^{\frac{1}{3}}$ or $m = \frac{n-1}{3}$. In each case the bound is below $\log(|B_n|)$.

If instead $r = n - 2m$ then $s = 2m = n - r$ which we have already done.

This completes the proof. $\square$

Altogether we have proved the main theorem which we restate more precisely:

Theorem 3.1.31
Fix $n \geq 28$ and set $k = \frac{n}{2}$ if n is even, $k = \frac{n-1}{2}$ if n is odd.

Define $H = \langle t_1 t_{k+1}, t_2 t_{k+2}, \ldots, t_k t_{2k} \rangle$.

If $4|k$ then setting $x = [1, k+1][2, k+2] \cdots [k, 2k]$ we have that $\langle H, x\rangle$ is a largest core-free subgroup of $2 \cdot A_n$. Otherwise H is a largest core-free subgroup of $2 \cdot A_n$.

3.2 Classical Groups

Minimal non-trivial, but not necessarily faithful, permutation representations of classical groups are well studied, for example in [7] and [20].

3.2.1 $\mathrm{SL}_n(q)$

In this section we extend the arguments in [7, 20] to compute $\mu(\mathrm{SL}_n(q))$. We state the result here for convenience (note that H_i will be defined immediately after).

For this section fix $H = \mathrm{SL}_n(q)$, $v_1, \ldots, v_n$ the standard basis of $\mathbb{F}_q^n$ and $K < H$ the setwise stabiliser of $\langle v_1 \rangle$ in H. Also let $p_1, \ldots, p_{k_0}$ be the primes dividing $|Z(H)|$ and $p_1, \ldots, p_{k_1}$ be the primes dividing $q-1$. For each i fix e_i such that $q - 1 = p_i^{e_i} t_i$ with $p_i \nmid t_i$, d_i such that $|Z(H)| = p_i^{d_i} s_i$ with $p_i \nmid s_i$ and $\lambda_i \in \mathbb{F}_q^*$ of order $p_i^{e_i}$.

Theorem 3.2.1
The following table classifies $\mu(\mathrm{SL}_n(q))$.

(n,q)	$\mu(\mathrm{SL}_n(q))$	*Representation*
$(2,2)$	3	$\{C_2\}$
$(2,3)$	8	$\{C_3\}$
$(2,5)$	24	$\{C_5\}$
$(2,9)$	80	$\{C_3 \times C_3\}$
$(4,2)$	8	A_6
(n,q) *not above,* $\lvert Z(\mathrm{SL}_n(q))\rvert = 1$	$\frac{q^n-1}{q-1}$	*Stabiliser of point in action on* $\mathrm{PG}(n-1,q)$
(n,q) *not above,* $\lvert Z(\mathrm{SL}_n(q))\rvert > 1$	$\frac{q^n-1}{q-1}\sum_{i\in[k_0]} p_i^{e_i}$	$\{H_i \mid i \in [k_0]\}$

We constuct H_i as follows:

$$T = \left\{ \begin{pmatrix} 1 & \mathbf{0} \\ x & I_{n-1} \end{pmatrix} | x \in \mathbb{F}_q^{n-1} \right\} \quad , \quad S = \left\{ \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & M \end{pmatrix} | \det(M) = 1 \right\}$$

$$D_i = \left\{ \begin{pmatrix} a & 0 & \mathbf{0} \\ 0 & a^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I_{n-2} \end{pmatrix} | a \in \langle \lambda_j | j \neq i \rangle \right\} \quad , \quad H_i = D_i S T$$

Notice that $S \leq N_H(T)$ so $ST \leq H$ and $D_i \leq N_H(ST)$ so $H_i \leq H$.

For $i \in [k_0]$ we define M_i as follows. If $d_i = e_i$ then let M_i be a generator of a p_i-Sylow subgroup of $Z(H)$. If $d_i < e_i$ then $p_i^{d_i} | n$ so $(p_i, n-1) = 1$ and therefore there is some $y_i \in \langle \lambda_i \rangle$ with $y_i^{n-1} = \lambda_i^{-1}$. In this case we define

$$M_i = \begin{pmatrix} \lambda_i & \mathbf{0} \\ \mathbf{0} & yI_{n-1} \end{pmatrix}$$

Lemma 3.2.2
For each $i \in [k_0]$ the following hold:

- $p_i \nmid |H_i \cap Z(H)|$.
- $[H : H_i] = \frac{q^n-1}{q-1} p_i^{e_i}$.
- *We have that $M_i \in K$ has order $p_i^{e_i}$ and $M_i^{p_i^{e_i-d_i}} \in Z(H)$. The subgroup generated by these M_i is cylic.*

Proof: Recalling that we take actions on the right this means every element of K has the form

$$\begin{pmatrix} a & \mathbf{0} \\ x & B \end{pmatrix}$$

where $a \in F_q^\times$, $x^T \in \mathbb{F}_q^{n-1}$ and $B \in \mathrm{GL}(n-1,q)$ with $\det(B) = a^{-1}$.

If $M \in H_i \cap Z(H)$ then M is diagonal and the first entry of M is determined by its image in D_i. By construction D_i has no element of order p_i so $H_i \cap Z(H)$ has no element of order p_i hence $p_i \nmid |H_i \cap Z(H)|$.

We compute degree as follows:

$$|T| = q^{n-1}$$

$$|S| = |\mathrm{SL}(n-1,q)| = \frac{\prod_{j=0}^{n-2} q^{n-1} - q^j}{q-1}$$

$$|D_i| = \frac{q-1}{p_i^{e_i}}$$

$$\begin{aligned} [H : H_i] &= \tfrac{\prod_{j=0}^{n-1} q^n - q^j}{q-1} \Big/ \left(q^{n-1} \tfrac{\prod_{j=0}^{n-2} q^{n-1} - q^j}{q-1} \tfrac{q-1}{p_i^{e_i}} \right) \\ &= \tfrac{q^n - 1}{q-1} p_i^{e_i} \end{aligned}$$

We have $\det(M_i) = \lambda_i y^{n-1} = 1$ so $M_i \in K$. Clearly the subgroup generated by such M_i is isomorphic to $\prod_{i=1}^{k_0} C_{p_i^{e_i}}$ so is cyclic. Moreover writing $y = \lambda_i^m$ so $\lambda_i^{-1} = \lambda_i^{m(n-1)}$ and therefore $\lambda_i^m = \lambda_i^{mn+1}$ we have

$$y^{p_i^{e_i - d_i}} = \lambda_i^{mp_i^{e_i - d_i}} = \lambda_i^{mnp_i^{e_i - d_i} + p_i^{e_i - d_i}}$$

Since $p_i^{d_i} | n$ and λ_i has order p^{e_i} this gives $y^{p_i^{e_i - d_i}} = \lambda_i^{p_i^{e_i - d_i}}$ and therefore

$$M_i^{p_i^{e_i - d_i}} = \lambda_i^{p_i^{e_i - d_i}} I_n \in Z(H)$$

as required. □

Corollary 3.2.3
$\{H_1, \ldots, H_{k_0}\}$ *defines a faithful representation of* H.

Proof: As $p_i \nmid |H_i \cap Z(H)|$ for each prime $p_i \mid |Z(H)|$ we have $\cap_{i=1}^{k_0} H_i \cap Z(H) = 1$ so $\cap_{i=1}^{k_0} H_i$ is core-free. □

We will show that $\{H_1, \ldots, H_{k_0}\}$ defines a minimal representation of H.

Lemma 3.2.4

Suppose $L < H$ fixes a subspace V of $\mathbb{F}_q^n$ of dimension d with $2 \leq d \leq n-2$ then $[H : L] > \sum_{i=1}^{k_0}[H : H_i]$.

Proof: Let L_d be the set of subspaces of dimension d. Note that $n \geq 4$ by assumption. As H acts transtively on L_d we have

$$\begin{aligned}[H : L] \geq [H : H_V] &= |L_d| \\ &= \frac{\prod_{i=1}^{n}(q^i-1)}{\prod_{i=1}^{d}(q^i-1)\prod_{i=1}^{n-d}(q^i-1)} \\ &\geq \frac{\prod_{i=1}^{n}(q^i-1)}{\prod_{i=1}^{2}(q^i-1)\prod_{i=1}^{n-2}(q^i-1)} \\ &= \frac{q^n-1}{q-1}\frac{q^{n-1}-1}{q^2-1} \\ &\geq \frac{q^n-1}{q-1}(q+1) \\ &> \frac{q^n-1}{q-1}\sum_{i=1}^{k_1} p_i^{e_i} \\ &\geq \sum_{i=1}^{k_0}[H : H_i]\end{aligned}$$

□

Lemma 3.2.5

Suppose $L < H$ fixes a subspace of $\mathbb{F}_q^n$ of dimension 1. Fix $I \subseteq [k_0]$ such that $i \in I$ implies $p_i \nmid |L \cap Z(H)|$. Then $[H : L] \geq \sum_{i \in I}[H : H_i]$ with equality if and only if $I = \{i\}$ for some i and L is conjugate to H_i.

Proof: Reordering if necessary, assume $I = \{1, \ldots, k_2\}$ for some k_2. Taking the appropriate conjugate of L we may assume $L \leq K$.

If $1 \neq M_i^r \in L$ for some r and some $i \in I$ then $1 \neq M_i^{p_i^{e_i-1}} \in L \cap Z(H)$ contradicting $p_i \nmid |L \cap Z(H)|$. Hence $\langle M_1, \ldots, M_{k_2}\rangle$ is a cyclic subgroup of K intersecting L trivially. This implies $[K : L] \geq \prod_{i=1}^{k_2} p_i^{e_i}$. Therefore

$$\begin{aligned}[H : L] &= [H : K][K : L] \\ &\geq \frac{q^n-1}{q-1}\prod_{i=1}^{k_2} p_i^{e_i} \\ &\geq \sum_{i \in I}[H : H_i]\end{aligned}$$

with equality if and only if $i = 1$ and therefore $L = H_i$. □

The following is an adaptation of a proof in [7]. We start with the case $n = 2$ - here $Z(H)$ is either trivial or order 2 so a minimal representation is transitive. In this case subgroups of $\mathrm{PSL}(n, q)$ are well known - the classification of these subgroups was first given by Dickson and can be found, for example, in [15].

Theorem 3.2.6
The subgroups of $\mathrm{PSL}(2,q)$ *with* $q = p^f$ *consists entirely of groups isomorphic to each of the following.*

1. *Elementary abelian p-group.*
2. *Cyclic of order* z *with* $z \mid \frac{q\pm1}{k}$ *where* $k = (q-1, 2)$.
3. *Dihedral group of order* $2z$ *with* z *as in (2).*
4. A_4 *for* $p > 2$ *and* $f \equiv 0$ (2).
5. S_4 *for* $q^2 - 1 \equiv 0$ (16).
6. A_5 *for* $p = 5$ *or* $q^2 - 1 \equiv 0$ (5).
7. *Semidirect product of an abelian group of order* p^m *with a cyclic group of order* t *such that* $m \leq f$, $t \mid p^m - 1$ *and* $t \mid q - 1$. *Subgroups of this form fix a one-dimensional subspace of* $\mathbb{F}_q^2$.
8. $\mathrm{PSL}(2, p^m)$ *with* $m|f$.
9. $\mathrm{PGL}(2, p^m)$ *with* $2m \mid f$.

Lemma 3.2.7
The following table classifies $\mu(H)$ *in the case* $n = 2$.

(n,q)	$\mu(H)$	*Point Stabiliser*
$(2,2)$	3	C_2
$(2,3)$	8	C_3
$(2,5)$	24	C_5
$(2,9)$	80	$C_3 \times C_3$
$(2,q)$, $q \notin \{2,3,5,9\}$	$2^{\nu_2(q-1)}(q+1)$	H_1 *as in Lemma 3.2.2 for* q *odd* *Point stabiliser in action on* $\mathrm{PG}(1,q)$ *for* q *even.*

Proof: Suppose $L \leq H$ is core-free. Then it is isomorphic to its image in $\mathrm{PSL}(n,q)$ so we consider the possible structures of L given in Theorem 3.2.6.

Case $q = 2$**:** $H \cong S_3$ so $\mu(H) = 3$.

Case $q = 3$**:** $H \cong Q_8 \rtimes C_3$ so if $2|L$ then $Z(H) \leq L$. Hence if L is core-free then $|L| \in \{1,3\}$. Maximal such L satisfies $L \cong C_3$ hence the result.

Case $q \in \{5, 9\}$**:** $\mathrm{SL}(2,5) \cong 2 \cdot A_5$ and $\mathrm{SL}(2,9) \cong 2 \cdot A_6$ so the minimal degrees of these are computed in Section 3.1.

Case $2 \mid q$**:** In this case $Z(H) = 1$ so $H = \mathrm{PSL}(n,q)$. The result is therefore given in the Table in Section 1.3.1.

Hereafter we assume q is odd and $q \notin \{3, 5, 9\}$. It is quite straightforward then to check that the only element of H of order 2 is $-I_n$. In particular $|L|$ must be odd. Each case number below refers to the structure of L as given in Theorem 3.2.6 - as $|L|$ is odd we rule out cases 4, 5, 6, 8 and 9 immediately. In each case we show that $[H : L] \geq 2^{\nu_2(q-1)}(q+1)$. We also see that the bound is attained in case (7). Note that $|H| = q(q-1)(q+1)$.

Case (1): $|L| \leq q$ so $[H : L] \geq (q+1)(q-1) \geq 2^{\nu_2(q-1)}(q+1)$.

Case (2): $|L| \leq \frac{q+1}{2}$ so $[H : L] \geq 2q(q-1) > 2^{\nu_2(q-1)}(q+1)$.

Case (3):

In this case $|L|$ divides $q+1$ or $q-1$. As $|L|$ is odd, $|L| \neq q+1$ so $|L| \leq q(q-1)$ which gives $[H : L] \geq q(q+1) > 2^{\nu_2(q-1)}(q+1)$.

Case (7):

In this case L fixes a one-dimensional subspace of F_q^2 so by Lemma 3.2.5 $|L| \leq |H_1|$ as required. □

Proposition 3.2.8

Fix $n \geq 3$. *If* $L_0 < \mathrm{PSL}(n,q)$ *is flag-transitive then* $(n,q) \in \{(3,2),(4,2)\}$.

Proof: This is a direct corollary of Theorem A in [24]. □

For the rest of this section we suppose $n \geq 3$ and $L < H$ is core-free and does not fix any proper non-trivial subspace of $\mathbb{F}_q^n$.

Lemma 3.2.9

If L *is flag-transitive then* $q = 2$ *so* $\mu(H) = \mu(\mathrm{PSL}(n,q))$.

Proof: If L is flag-transitive then it has flag-transitive image in $\mathrm{PSL}(n,q)$. By Proposition 3.2.8, the only values of (n,q) with $n \geq 3$ such that $\mathrm{PSL}(n,q)$ has a proper flag-transitive subgroup satisfy $q = 2$. In this case the center of H is trivial. □

Before the next technical Lemma, we need to study root subgroups as defined for example in [21] (we rewrite the definition here for convenience).

Definition 3.2.1
Let $\tau \in \mathrm{GL}_n(q)$ and $W \subseteq \mathbb{F}_q^n$. We denote

$$[\tau, W] = \langle \tau w - w | w \in W \rangle$$

Let $0 \neq x \in \mathbb{F}_q^n$ and let $P \subset \mathbb{F}_q^n$ be a hyperplane in $\mathbb{F}_q^n$. We say τ is a transvection with center $\langle x \rangle$ and axis P if $[\tau, \mathbb{F}_q^n] = \langle x \rangle$ and $[\tau, P] = 0$.

The root subgroup *associated with $(\langle x \rangle, P)$ is*

$$\langle \tau \in \mathrm{GL}_n(q) | [T, \mathbb{F}_q^n] = \langle x \rangle, [\tau, P] = 0 \rangle$$

The above definition is dense and we keep it that way to be consistent with [21] which we will need later. However the only root subgroups we will need to care about are those with $x = v_j$ and $P = \langle v_i | i \neq k \rangle$ for some $k \geq j$ where we recall $v_1, \dots, v_n$ is the standard basis. In this case if $[\tau, P] = 0$ then the only non-zero row of $\tau - I_n$ is the k^{th} column and if $[T, \mathbb{F}_q^n] = v_j$ then the k^{th} row of $\tau - I_n$ must be a multiple of v_j. This means the root subgroup associated with $(\langle x \rangle, P)$ consists of those $\tau \in \mathrm{GL}_n(q)$ with 1 on the diagonal, some λ in position (k, j) and 0 everywhere else.

Lemma 3.2.10
Assume $q \neq 2$ and $(n, q) \neq (3, 7)$. Fix $I \subseteq [k_0]$ such that $i \in I$ implies $p \nmid |L \cap Z(H)|$. Then $[H : L] > \sum_{i \in I} [H : H_i]$ or both L is transitive on the points of $\mathrm{PG}(n-1, q)$ and L contains a root subgroup.

Proof:
Note that if $(n, q) \in \{(3, 3), (3, 5), (3, 9), (3, 11)\}$ then $k_0 = 0$ and the result vacuously holds so assume $(n, q) \notin \{(3, 3), (3, 5), (3, 9), (3, 11)\}$. Assume that $[H : L] \leq \sum_{i \in I} [H : H_i]$.

Define

$$K_0 = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathrm{SL}_{n-1}(q) \end{pmatrix}$$

Suppose for all $g \in H$ we have $L \cap K_0^g = K_0^g$ so for all $g \in H$ $L^g \cap K_0 = K_0$. Then immediately L contains a root subgroup. For any two points $x, y \in \mathbb{F}_q^n$ with $\langle x \rangle \neq \langle y \rangle$ take $g \in H$ such that $xg = v_2$ and $yg = v_3$. In particular if

$$l = \begin{pmatrix} -1 & 0 & 0 & \mathbf{0} \\ 0 & 0 & 1 & \mathbf{0} \\ 0 & 1 & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I_{n-3} \end{pmatrix}$$

then $l \in L^g$ and $xgl = yg$ so $l^{g^{-1}} \in L$ and $xl^{g^{-1}} = y$. Hence L acts transitively on the points of $\mathrm{PG}(n-1,q)$. So suppose that $L \cap K_0^g \neq K_0^g$ for some $g \in H$. Replacing L with $L^{g^{-1}}$ we may assume $L \cap K_0 \neq K_0$.

We have $[K_0 : K_0 \cap L] \geq \mu(K_0) = \mu(\mathrm{PSL}_{n-1}(q)) = \frac{q^{n-1}-1}{q-1}$ so

$$|L \cap K_0| \leq (q-1)\prod_{r=1}^{n-2}(q^{n-1}-q^r)$$

We now study $L \cap K$. Notice that any element of K takes the form

$$\begin{pmatrix} \lambda & \mathbf{0} \\ x & \Lambda U \end{pmatrix} = \begin{pmatrix} \lambda & \mathbf{0} \\ \mathbf{0} & \Lambda \end{pmatrix}\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & U \end{pmatrix}\begin{pmatrix} 1 & \mathbf{0} \\ (\Lambda U)^{-1}x & I_{n-1} \end{pmatrix}$$

for some $\lambda \in \mathbb{F}_q^\times$, $x \in \mathbb{F}_q^{n-1}$, $U \in \mathrm{SL}_{n-1}(q)$, $\Lambda \in \mathrm{GL}_{n-1}(q)$ such that $\det(\Lambda) = \lambda^{-1}$. Note that for any Λ' with $\det(\Lambda') = \lambda^{-1}$ we may replace Λ with Λ' by replacing U with $(\Lambda')^{-1}\Lambda U$.

In particular, if $M_0 = \prod_{i\in I} M_i$ and $\alpha \in \mathbb{F}_q^\times$ has order $\frac{q-1}{\prod_{i\in I} p_i^{e_i}}$ then

$$K = \langle M_0\rangle \left\langle \begin{pmatrix} \alpha & 0 & \mathbf{0} \\ 0 & \alpha^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I_{n-2} \end{pmatrix} \right\rangle K_0 T \cong (C_{q-1} \times \mathrm{SL}_{n-1}(q)) \ltimes C_q^{n-1}$$

where we recall

$$T = \left\{ \begin{pmatrix} 1 & \mathbf{0} \\ x & I_{n-1} \end{pmatrix} | x \in \mathbb{F}_q^{n-1} \right\}$$

If $l \in L \cap M_0^r T$ for some r with $M_0^r \neq I_n$ then it is easy to check that $l^q \in \langle M_0\rangle \setminus \{I_n\}$ which contradicts $p \nmid |L \cap (Z(H))|$. Hence the projection $\tilde{K}$ of $L \cap K$ onto $C_{q-1} \times \mathrm{SL}_{n-1}(q)$ intersects $\langle M_0\rangle$ trivially.

Suppose $\tilde{K} \cap \mathrm{SL}_{n-1}(q) = \mathrm{SL}_{n-1}(q)$. As $L \cap K_0$ is isomorphic to its projection onto $\mathrm{SL}_{n-1}(q)$ and this image is normal in $\tilde{K} \cap \mathrm{SL}_{n-1}(q)$ and $L \cap K_0 \neq K_0$, we have $|L \cap K_0| \leq |Z(\mathrm{SL}_{n-1}(q))| \leq q-1$. This gives

$$|L \cap K| \leq \frac{q-1}{\prod_{i\in I} p_i^{e_i}}(q-1)|L \cap T|$$

Suppose instead that $\tilde{K} \cap \mathrm{SL}_{n-1}(q) \neq \mathrm{SL}_{n-1}(q)$. Then

$$|\tilde{K} \cap \mathrm{SL}_{n-1}(q)| \leq \frac{|\mathrm{SL}_{n-1}(q)|}{\mu(\mathrm{SL}_{n-1}(q))} = \prod_{r=1}^{n-2}(q^{n-1}-q^r)$$

In either case we obtain

$$|L \cap K| \leq \frac{q-1}{\prod_{i\in I} p_i^{e_i}} \prod_{r=1}^{n-2}(q^{n-1}-q^r)|L \cap T|$$

Suppose $L \cap T = T$. Immediately L contains a root subgroup. Recalling that $v_1, \dots v_n$ is the standard basis of $\mathbb{F}_q^n$ we have that for any $w \in \langle v_2, \dots v_n \rangle \setminus \{0\}$ we may choose $x \in \langle v_2, \dots v_n \rangle$ with $x \cdot w \neq 0$. Then

$$w \begin{pmatrix} 1 & \mathbf{0} \\ x & I_{n-1} \end{pmatrix} = w + (x \cdot w) v_1$$

In particular, for any $w \in v_1 L$, L is transitive on the lines of $\langle v_1, w \rangle$.

Define $t_x = \begin{pmatrix} 1 & \mathbf{0} \\ x & I_{n-1} \end{pmatrix} \in L$.

As L does not fix a proper subspace of $\mathbb{F}_q^n$ we have some $l_2, \dots, l_n \in L$ such that $v_1, v_1 l_2, \dots, v_1 l_n$ form a basis of $\mathbb{F}_q^n$. After a change of basis we may assume $v_1 l_i = v_i$ for each i.

We prove by induction that L acts transitively on the lines of $\langle v_1, \dots, v_k \rangle$. The case $k = 2$ is shown above so assume $k \geq 3$. Fix $0 \neq w = \mu_1 v_1 + \dots + \mu_k v_k$. If $\mu_k = 0$ then there exists $l \in L$ with $\langle v_1 \rangle l = \langle w \rangle$ by inductive hypothesis. If $w \in \langle v_k \rangle$ then $\langle w \rangle = \langle v_1 \rangle l_k$ by construction. So assume $\mu_k \neq 0$ and $w \notin \langle v_k \rangle$. Using the appropriate x we have $w l_k^{-1} t_x = w l_k^{-1} - \mu_k v_1$ so $w t_x^{l_k} = w - \mu_k v_k$. By inductive hypothesis there exists $l \in L$ with $\langle v_1 \rangle l = \langle w - \mu_k v_k \rangle$ so $\langle v_1 \rangle l t_x^{l_k} = \langle w \rangle$. This completes the proof in the case $L \cap T = T$.

We may therefore assume $L \cap T \neq T$ so $|L \cap T| \leq q^{n-2}$. This gives

$$|L \cap K| \leq \frac{(q-1)q^{n-2}}{\prod_{i \in I} p_i^{e_i}} \prod_{r=1}^{n-2} (q^{n-1} - q^r)$$

As noted above, since L does not fix any proper subspace of $\mathbb{F}_q^n$, every orbit of L in $\mathrm{PG}(n-1, q)$ has length at least n. Hence if L is intransitive on the points of $\mathrm{PG}(n-1, q)$ then $[L : L \cap K] \leq \frac{q^n - 1}{q-1} - n$ so

$$\begin{aligned} [H : L] = \tfrac{|H|}{[L:L\cap K]|L \cap K|} \quad & \geq \frac{\left(\prod_{r=0}^{n-1}(q^n - q^r)\right)/(q-1)}{\left(\frac{q^n-1}{q-1} - n\right)\frac{(q-1)q^{n-2}}{\prod_{i\in I} p_i^{e_i}} \prod_{r=1}^{n-2}(q^{n-1}-q^r)} \\ & = \frac{\prod_{i \in I} p_i^{e_i} (q^n - 1)(q^n - q)}{(q-1)(q^n - 1 - nq + n)} \\ & > \frac{\prod_{i \in I} p_i^{e_i} (q^n - 1)}{(q-1)} \geq \sum_{i \in I} [H : H_i] \end{aligned}$$

contrary to assumption. This completes the proof that L acts transitively on the points of $\mathrm{PG}(n-1, q)$. $\square$

Lemma 3.2.11
Assume $q \neq 2$ and $(n, q) \neq (3, 7)$. Fix $I \subseteq [k_0]$ such that $i \in I$ implies that $p_i \nmid |L \cap Z(H)|$ then $[H : L] > \sum_{i \in I}[H : H_i]$.

Proof: Suppose $[H : L] \leq \sum_{i \in I}[H : H_i]$. Then by Lemma 3.2.10 L is transitive on the points of $\mathrm{PG}(n-1, q)$ and contains a root subgroup. It is shown in [21] that the only transitive groups containing a root subgroup are H and $\mathrm{Sp}_n(Q)$ (for even n). As $L \neq H$ we must have n even and $L = \mathrm{Sp}_q(n)$. In this case

$$\begin{aligned}[H : L] &= \frac{q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1)}{(q-1)q^{\frac{n^2}{4}} \prod_{i=1}^{\frac{n}{2}}(q^{2i}-1)} \\ &= q^{\frac{n(n-2)}{4}} \frac{\prod_{i=1}^{\frac{n}{2}}(q^{2i-1}-1)}{(q-1)} \\ &\geq q(q^n - q) \\ &> \sum_{i=1}^{k_0}[H : H_i]\end{aligned}$$

□

Proof of Theorem: See Lemma 3.2.7 for the case $n = 2$. For $(n, q) = (4, 2)$ or $k_0 = 0$ we have $H = \mathrm{PSL}_n(q)$ so the result is given in section 1.3.1. For $(n, q) = (3, 7)$ we have $|Z(H)| = 3$ so, by Proposition 3.0.2, $\mu(H) \geq 3\frac{q^n-1}{q-1}$ and the result holds. So suppose $n > 2$, $k_0 \neq 0$ and $(n, q) \notin \{(4, 2), (3, 7)\}$.

Let $R = \{L_1, \ldots, L_t\}$ define a minimal representation of H and suppose no conjugate of H_i in H appears in R for some $i \in [k_0]$ - relabelling if necessary assume $i = 1$. If $p_1 \mid |L_i \cap Z(H)|$ for each i then R would not be faithful, so relabelling if necessary we may assume $p_1 \nmid |L_1 \cap Z(H)|$.

If L_1 fixes a subspace of $\mathbb{F}_q^n$ of dimsension $2 \leq d \leq n-2$ then by Lemma 3.2.4 R has degree at least $[H : L_1] > \sum_{i \in [k_0]}[H : H_i]$ contradicting the assumption R is minimal. So we may assume L fixes a subspace of dimension 1 or L_1 fixes no proper subspace of $\mathbb{F}_q^n$.

Fix $I \subseteq [k_0]$ such that for $i \in [k_0]$ we have $i \in I$ if and only if $p_i \nmid |L_1 \cap Z(H)|$. Relabelling if necessary we may assume $I = \{1, \ldots, s\}$. By Lemmas 3.2.4 and 3.2.5 give $[H : L_1] > \sum_{i \in I}[H : H_i]$. Let $R' = \{H_1, \ldots, H_s, L_2, \ldots, L_t\}$.

Suppose $p_j \mid |Z(H) \cap (\cap_{i=1}^{s} H_i) \cap (\cap_{i=2}^{t} L_i)|$ for some $j \in [k_0]$. Then $p_j \mid |Z(H) \cap H_i|$ for $i \in I$. This means $j \notin I$ so $p_j \mid |L_1 \cap Z(H)|$. But also $p_j \mid |L_i \cap Z(H)|$ for $i > 1$ so $p_j \mid |Z(H) \cap (\cap_{i=1}^{t} L_i)|$ contradicting the fact R is faithful. Hence $Z(H) \cap (\cap_{i=1}^{s} H_i) \cap (\cap_{i=2}^{t} L_i) = 1$ so R' is faithful. Since the degree of R' is strictly less than that of R this contradicts the assumption R is minimal.

This shows that some conjugaet of H_i in H appears in R for all i. Therefore the degree of R is at least $\sum_{i \in [k_0]}[H : H_i] = \frac{q^n-1}{q-1} \sum_{i \in [k_0]} p_i^{e_i}$ completing the proof. □

3.3 Sporadic Groups

We list in this section the minimal degrees of the Schur covers of some of the sporadic simple groups. Many of the sporadic simple groups have trivial Schur multiplier so the Schur cover of such a group S is S and $\mu(S)$ can be found in the table in section 1.3.1. The table below gives $\mu(G)$ for the Schur cover G of each sporadic simple group S with non-trivial Schur multiplier, except in the case $S = B$.

We will see that the case $S = B$ is omitted because the maximal subgroups of B are not, as far as the author is aware, available in MAGMA. This is also the case for Co_1 and Fi'_{24}, but representations of $2 \cdot Co_1$ and $3 \cdot Fi'_{24}$ of degrees 196560 and 920808 respectively are given in [6].

S	Schur Multiplier	$\mu(G)$	Representation
M_{12}	C_2	24	$\{M_{11}\}$
M_{22}	C_{12}	5622	$\{3 \cdot A_6, ((C_4 : C_8) : A_5) : C_2\}$
J_2	C_2	200	$\{U_3(3)\}$
J_3	C_3	18468	$\{\mathrm{PSL}_2(16) : 2\}$
Co_1	C_2	196560	$\{Co_2\}$
Fi_{22}	C_6	213488	$\{C_3 \times O_7(3), (C_2 \times O_8^+(2)) : 6\}$
Fi'_{24}	C_3	920808	$\{Fi_{23}\}$
HS	C_2	704	$\{U_3(5)\}$
McL	C_3	66825	$\{2 \cdot \mathrm{PSL}_3(4)\}$
Ru	C_2	16240	$\{^2F_4(2)\}$
Suz	C_6	70866	$\{C_3 \times U_5(2), 2 \cdot G_2(4)\}$
$O'N$	C_3	368280	$\{\mathrm{PSL}_3(7) : 2\}$
B	C_2		

The method used to compute the above representations is a relatively naive algorithm which we describe here. For the rest of this section we take S to be a sporadic simple group with non-trivial Schur multiplier and G to be the Schur cover of S.

By Proposition 1.2.3 a minimal representation of G has at most 2 orbits. If G has simple socle C_p then a minimal representation of G is $\{H_p\}$ where H_p is a core-free subgroup of G. If G has socle C_{pq} where p and q are distinct primes then a minimal representation of G is either $\{H_{pq}\}$ where H_{pq} is a core-free subgroup of G or $\{H_p, H_q\}$ where $H_p \cap \mathrm{Soc}(G) \cong C_p$ and $H_q \cap \mathrm{Soc}(G) \cong C_q$.

Fix $x \in \{p, q, pq\}$ ($x = p$ if G has simple socle). We find the largest of each of these H_x then if G has non-simple socle we check which representation is minimal.

The idea is to check all subgroups of G by starting with the set $L = \{G\}$. Eventually we want the largest subgroup M of G in L to be the largest H_x. While the largest group M in L does not satisfy $M \cap \mathrm{Soc}(G) \cong C_x$ we replace L with

$$L \mapsto (L \cup \{N \leq M | N \,\mathrm{is\,maximal\,in}\, M\}) \setminus \{M\}$$

If we did not terminate this process, we would consider every subgroup of G in decreasing size order, so this terminates with M being the largest possible H_x as required.

For efficiency we can ignore conjugate subgroups in L. Example code which implements this can be found in appendix A in the function `MSAS`. We also provide code that runs through the simple sporadic groups S for which we can compute $\mu(G)$ giving the degrees and defining subgroups of the minimal representations. The files loaded in the code define the Schur covers as G and are available from the online ATLAS database[6].

Appendix A

Example Code

A.1 The Two Cover of The Alternating Group

In this section we include example MAGMA functions implementing the algorithm desibed in Section 3.1.1

```
// Function to build core-free primitives
buildPCFs := function( n )

  if n le 20 then
    //return all core-free primitive groups
    CFs  := [];
    Sn   := Sym( n );
    Prims := PrimitiveGroups( n );

    for G in Prims do
      if IsEven(G) and LooksCoreFree( G ) then
        CFs := CFs cat [[ G`Order , #Normaliser(Sn,G) , n ]];
      end if;
    end for;
```

```
  elif n le 200 then
    //return largest primitive group
    CFs  := [];
    An  := Alt( n );
    Maxes := MaximalSubgroups( An );
    Sort( ~Maxes , func< X,Y | Y`order-X`order >);
    for G in Maxes do
      if IsPrimitive( G`subgroup ) then
        CFs := CFs cat [[ G`order , 2*G`order , n ]];
        break;
      end if;
    end for;
  else
    //return usual bounds
    CFs := [[ 2^n , 2^n , n ]];
  end if;
  return CFs;
end function;


// Brute force function for finding transitive CFs
BruteTCFs := function( n )

  Sn := Sym( n );
  An := Alt( n );
  CFs := [];
  //normalisers of CFs are larger than CFs, so in bounding CFs it suffices to
  //assume normalisers are at least as large as any known CF
  MIN := 0;
  for H in LoadCFs( n , "P" ) do
    if H[1] gt MIN then MIN := H[1]; end if;
  end for;
  Q  := [Sn]; //search for normaliser of CF - top down
```

```
  while #Q ge 1 and #Q[1] ge MIN do

    if IsTransitive( Q[1] ) then

      for H in NormalSubgroups( Q[1] ) do
        if IsTransitive(H`subgroup)  and
           IsEven(H`subgroup)        and
           LooksCoreFree(H`subgroup) then
          CFs := CFs cat [[ H`order , Q[1]`Order , n ]];
          if H`order gt MIN then MIN := H`order; end if;
        end if;
      end for;

      M := Sort( MaximalSubgroups( Q[1] ) , func<X,Y|Y`order-X`order>);
      i := 1;
      j := 2;
      //insert M in Q to maintain ordering on Q
      while i le #M and j le #Q do
        if M[i]`order gt Q[j]`Order then
          Q := Q[1..j-1] cat [M[i]`subgroup] cat Q[j..#Q];
          i +:= 1;
        else
          j +:= 1;
        end if;
      end while;
      if i le #M then
        for k in [i..#M] do
          Q := Q cat [M[k]`subgroup];
        end for;
      end if;

    end if;
    Q := Q[2..#Q];
  end while;
  return CFs;
end function;
```

```
// code to bound order of primitive group of degree n not containing An

prims := [1,1,1,1,20,120,168,1344,1512,1440,7920,95040,5616,2184,20160,
322560, 16320, 4896, 342, 6840, 120960, 887040, 10200960, 244823040 ];

PrimBound := function( n )
  if n le 24 then
    return prims[n];
  else
    return 2^n;
  end if;
end function;

// Function to build core-free transitives

buildTCFs := function ( n )

  if n le 16 then
    // Brute force small cases
    return BruteTCFs( n );
  end if;

  TCFns  := LoadCFs( n , "P" );

  for gam in Divisors(n)[ 2..NumberOfDivisors(n)-1 ] do
```

```
if gam eq 2 then
  if n le 20 then
    TCFns := TCFns cat [[ 2^Floor(n/2-5)*PrimBound(Floor(n/2)),
                          2^Floor(n/2)   *PrimBound(Floor(n/2)),n]];
  else
    TCFns := TCFns cat [[ 2^Floor(n/2-6)*PrimBound(Floor(n/2)),
                          2^Floor(n/2)   *PrimBound(Floor(n/2)),n]];
  end if;
  if n mod 8 eq 0 then
    TCFns := TCFns cat [[   Factorial(Floor(n/2)) ,
                          2*Factorial(Floor(n/2)) , n ]];
  end if;
  if not IsPrime(Floor(n/2)) thenk
    for s in Divisors(Floor(n/2))[2..NumberOfDivisors(Floor(n/2))-1] do
      if s lt n/4 then
        if n le 20 then
TCFns := TCFns cat [[
  2^Floor(n/2-5) * Factorial(s)^Floor(n/(2*s)) * Factorial(Floor(n/(2*s))) ,
  2^Floor(n/2)   * Factorial(s)^Floor(n/(2*s)) * Factorial(Floor(n/(2*s))) ,n]]
        else
TCFns := TCFns cat [[
  2^Floor(n/2-6) * Factorial(s)^Floor(n/(2*s)) * Factorial(Floor(n/(2*s))) ,
  2^Floor(n/2)   * Factorial(s)^Floor(n/(2*s)) * Factorial(Floor(n/(2*s))) ,n]]
          end if;
        elif n gt 20 then
TCFns := TCFns cat [[
  2^Floor(n/2-6) * PrimBound(Floor(n/4))^2 * 2 ,
  2^Floor(n/2)   * PrimBound(Floor(n/4))^2 * 2 ,n]];
TCFns := TCFns cat [[
  2^Floor(n/4+1) * Factorial(Floor(n/4))^2 * 2 ,
  2^Floor(n/2)   * Factorial(s)^Floor(n/(2*s)) * Factorial(Floor(n/(2*s))),n]];
      else
TCFns := TCFns cat [[
  2^Floor(n/2-5) * Factorial(s)^Floor(n/(2*s)) * Factorial(Floor(n/(2*s))) ,
  2^Floor(n/2)   * Factorial(s)^Floor(n/(2*s)) * Factorial(Floor(n/(2*s))) ,n]]
      end if;
    end for;
  end if;
```

```
elif gam eq 3 then
  if n le 24 then
    TCFns := TCFns cat [[
      2^Floor(n/3-4)*3^Floor(n/3)*PrimBound(Floor(n/3)),
      2^Floor(n/3)   *3^Floor(n/3)*PrimBound(Floor(n/3)),
      n                           ]];
  elif n le 30 then
    TCFns := TCFns cat [[
      2^Floor(n/3-5)*3^Floor(n/3)*PrimBound(Floor(n/3)),
      2^Floor(n/3)   *3^Floor(n/3)*PrimBound(Floor(n/3)),
      n                           ]];
  else
    TCFns := TCFns cat [[
      2^Floor(n/3-6)*3^Floor(n/3)*PrimBound(Floor(n/3)),
      2^Floor(n/3)   *3^Floor(n/3)*PrimBound(Floor(n/3)),
      n                           ]];
  end if;
  if not IsPrime(Floor(n/2)) then
    for s in Divisors(Floor(n/2))[2..NumberOfDivisors(Floor(n/2))-1] do
      if n le 24 then
TCFns := TCFns cat [[
  2^Floor(n/3-4)*3^Floor(n/3)*
    Factorial(s)^Floor(n/(3*s))*Factorial(Floor(n/(3*s)))  ,
  6^Floor(n/3) * Factorial(s)^Floor(n/(3*s)) * Factorial(Floor(n/(3*s))),n]];
      elif n le 30 then
TCFns := TCFns cat [[
  2^Floor(n/3-5)*3^Floor(n/3)*
    Factorial(s)^Floor(n/(3*s))*Factorial(Floor(n/(3*s)))  ,
  6^Floor(n/3) * Factorial(s)^Floor(n/(3*s)) * Factorial(Floor(n/(3*s)))  ,n]];
      else
TCFns := TCFns cat [[
  2^Floor(n/3-6)*3^Floor(n/3)*
    Factorial(s)^Floor(n/(3*s))*Factorial(Floor(n/(3*s)))  ,
  6^Floor(n/3) * Factorial(s)^Floor(n/(3*s)) * Factorial(Floor(n/(3*s)))  ,n]];
      end if;
    end for;
  end if;
```

```
elif gam eq 4 then
  if n le 56 then
    //brute force small cases

    Sn := Sym( n );
    An := Alt( n );
    // construct subgroup G = S4^(n/4) of Sn
    G := sub< Sn | Id(Sn) >;
    for i in [1..n/4] do
      G := sub< Sn | G , Sn!(4*i-3,4*i-1) , Sn!(4*i-3,4*i-2,4*i-1,4*i) >;
    end for;
    // NG = S4 wr S(n/4)
    NG := Normaliser( Sn , G );
    G  := G meet An;

    Q := [NG meet An];

    while #Q ge 1 do

      if IsTransitive(Q[1]) and #MinimalBlocks(Q[1])[1] eq 4 then
        if LooksCoreFree(Q[1]) then
          TCFns := TCFns cat [[#Q[1], #Normaliser(Sn,Q[1]), n]];
        else
          for H in MaximalSubgroups( Q[1] ) do
            Q := Q cat [H`subgroup];
          end for;
        end if;
      end if;
      Q := Q[2..#Q];

    end while;

  else
    TCFns := TCFns cat [[
      Floor(Factorial(gam)^(Floor(n/gam))*Factorial(Floor(n/gam))/(2^6)),
      Factorial(gam)^(Floor(n/gam))*Factorial(Floor(n/gam)) ,
      n ]];
  end if;
```

```
  else // gam gt 4
    if n le 40 and n/gam eq 2 then //brute force difficult small cases
      Sn := Sym( n );
      An := Alt( n );
      G := sub< Sn | Id(Sn) >; // construct G = S(n/2)^2
      for i in [1..n/2-1] do
        G := sub<Sn|G,Sn!(i,i+1),Sn!(Floor(n/2)+i,Floor(n/2)+i+1) >;
      end for;
      NG := Normaliser( Sn , G ); // NG = S(n/2) wr S2
      G  := G meet An;
      Q := [NG meet An];
      while #Q ge 1 do
        if IsTransitive(Q[1]) and #MinimalBlocks(Q[1])[1] eq n/2 then
          if LooksCoreFree(Q[1]) then
            TCFns := TCFns cat [[#Q[1], #Normaliser(Sn,Q[1]), n]];
          else
            for H in MaximalSubgroups( Q[1] ) do
              Q := Q cat [H`subgroup];
            end for;
          end if;
        end if;
        Q := Q[2..#Q];
      end while;
    else
      if IsEven(Floor(n/gam)) and n/gam ne 2 then
        TCFns := TCFns cat [[
          Factorial(gam)^(Floor(n/(2*gam)))*Factorial(Floor(n/gam)),
          Factorial(gam)^(Floor(n/(2*gam)))*Factorial(Floor(n/gam)),
          n                                    ]];
      elif IsEven(Floor(n/gam)) then
        if n mod 8 eq 0 then
          TCFns := TCFns cat [[
            Factorial(gam)     ,
            Factorial(gam)*2   ,
            n                  ]];
        end if;
      end if;
    end if;
  end if;
end for;
```

```
  if not IsPrime( n ) then
    if 10 le n and n le 16 then
      Prims := PrimitiveGroups( n );
      for P in Prims do
        if #P ge Factorial(Floor(n/2)) then
          Norms := Sort(NormalSubgroups(P),func<x,y|y`order-x`order>);
          for N in Norms[1..#Norms-1] do
            if not IsPrimitive( N`subgroup ) then
              TCFns := TCFns cat [[N`order , #P , n ]];
            end if;
          end for;
        end if;
      end for;
    end if;

    for d in Divisors(n)[ 2..NumberOfDivisors(n)-1 ] do
      if d ge 5 then

        if n gt 36 then
TCFns := TCFns cat [[PrimBound(d)^Floor(n/d)*Factorial(Floor(n/d)),
                     PrimBound(d)^Floor(n/d)*Factorial(Floor(n/d)),
                     n ]];

        else
          for e in Divisors(n)[ 2..NumberOfDivisors(d) ] do
            if e ge 5 then

              M := PrimBound(e)^Floor(n/e-1)*
                     Factorial(Floor(d/e))^Floor(n/d)*Factorial(Floor(n/d));
              if e mod 2 eq 1 then M:=Floor(M/2);end if;
              Prims := Sort(PrimitiveGroups( e ),func<x,y|#y-#x>);
```

```
              for P in Prims[3..#Prims] do
                Norms := NormalSubgroups( P );
                for N in Norms do
                  if IsEven(N`subgroup) and
                    IsTransitive(N`subgroup) and
                    LooksCoreFree(N`subgroup) then
                    M:=N`order*#P^Floor(n/e-1)*
                        Factorial(Floor(d/e))^Floor(n/d)*Factorial(Floor(n/d));
                    if e mod 2 eq 1 then M:=Floor(M/2);end if;
                    M:= Min([M,
                          PrimBound(e)^Floor(n/e)*
                            Factorial(Floor(d/e))^Floor(n/d)*
                            Factorial(Floor(n/d))]);
                    TCFns := TCFns cat [[
                      M,
                      PrimBound(e)^Floor(n/e)*
                        Factorial(Floor(d/e))^Floor(n/d)*
                        Factorial(Floor(n/d)) ,
                      n ]];
  end if;end for;end for;end if;end for;end if;end if;end for;end if;
  return TCFns;
end function;


// Brute force functions for finding CFs with fixed orbit lengths
// Length 2
BruteFCFs2 := function( n )
  Sn := Sym( n );
  An := Alt( n );
  CFs := [];

  // Groups with all orbits of length 2 are elementary abelian
  Q  := ElementaryAbelianSubgroups( Sylow( An , 2 ) );
  for H in Q do
    if #Orbits(H`subgroup)[1] eq 2 and LooksCoreFree( H`subgroup ) then
      CFs := CFs cat [[ H`order , #Normaliser(Sn,H`subgroup) , 2 ]];
    end if;
  end for;
  return CFs;
end function;
```

```
//Length 3
BruteFCFs3 := function( n )

  Sn := Sym( n );
  An := Alt( n );
  CFs := [];

  // The Sylow 3-subgroup of a group with orbits all of length 3 is
  // elementary abelian
  Q3 := ElementaryAbelianSubgroups( Sylow( An , 3 ) );

  for H3 in Q3 do
    if #Orbits(H3`subgroup)[1] eq 3 then
      // The Sylow 2-subgroup of a group with orbits all of length 3
      // normalises the Sylow 3-subgroup
      Q2 := ElementaryAbelianSubgroups( Sylow(Normaliser(Sn,H3`subgroup),2) );
      for H2 in Q2 do
        H := sub< Sn | H3`subgroup , H2`subgroup > meet An;
        if LooksCoreFree( H ) then
          CFs := CFs cat [[ #H , #Normaliser(Sn,H) , 2 ]];
        end if;
      end for;
    end if;
  end for;

  return CFs;

end function;
```

```
// Function to build core-frees with fixed orbit length
buildFCFs := function( n )
  FCFns := LoadCFs( n , "T" ) cat [[1,Factorial(n),1]];

  // Orbit length
  for gam in Divisors( n )[ 2..NumberOfDivisors(n)-1 ] do
    if gam eq 2 then
      if n le 14 then
        // brute force small cases
        FCFns := FCFns cat BruteFCFs2( n );
      elif n eq 16 then
        FCFns := FCFns cat [[ 2^(Floor(n/2)-4) ,
                              2^Floor(n/2)*Factorial(Floor(n/2)) ,
                              gam ]];
      elif n le 20 then
          FCFns := FCFns cat [[ 2^(Floor(n/2)-5) ,
                                2^Floor(n/2)*Factorial(Floor(n/2)),
                                gam ]];
      else
        FCFns := FCFns cat [[ 2^(Floor(n/2)-6) ,
                              2^Floor(n/2)*Factorial(Floor(n/2)) ,
                              gam ]];
      end if;
    elif gam eq 3 then
      if n le 15 then
        // brute force small cases
        FCFns := FCFns cat BruteFCFs3( n );
      elif n le 24 then
        FCFns := FCFns cat [[ 2^(Floor(n/3)-4)*3^Floor(n/3) ,
                              2^Floor(n/3)*3^Floor(n/3)*Factorial(Floor(n/3)) ,
                              gam ]];
      elif n le 30 then
        FCFns := FCFns cat [[ 2^(Floor(n/2)-5)*3^Floor(n/3) ,
                              2^Floor(n/3)*3^Floor(n/3)*Factorial(Floor(n/3)) ,
                              gam ]];
      else
        FCFns := FCFns cat [[ 2^(Floor(n/3)-6)*3^Floor(n/3) ,
                              2^Floor(n/3)*3^Floor(n/3)*Factorial(Floor(n/3)) ,
                              gam ]];
      end if;
```

```
    elif gam eq 4 then
      FCFns := FCFns cat [[ Floor(24^Floor(n/gam)/4) ,
                            24^Floor(n/gam)*Factorial(Floor(n/gam)) ,
                            gam ]];

    else
      if not IsPrime(gam) then
        M := Divisors(gam)[NumberOfDivisors(gam)-1];

        //possible groups without min block A_m or A_gam
        PrimCand := PrimBound(gam);
        if NumberOfDivisors(gam) gt 3 then
M2          := Divisors(gam)[NumberOfDivisors(gam)-2];
BigBlockCand   := Factorial(M2)^Floor(gam/M2)*Factorial(Floor(gam/M2));
LittleBlockCand  := Factorial(M)*Factorial(Floor(gam/M))^Floor(M);
        else
          BigBlockCand   := 1;
          LittleBlockCand := 1;
        end if;
        PrimMBlockCand:=PrimBound(M)^Floor(gam/M)*Factorial(Floor(gam/M));

        for G in LoadCFs( gam , "F" ) cat [[1,1,gam]] do
          if G[3] ne 1 then
            if IsEven(Floor(n/gam)) then

FCFns := FCFns cat [[ Floor(Factorial(gam)^Floor(n/(2*gam))/2) ,
                  Factorial(gam)^Floor(n/(2*gam))*Factorial(Floor(n/gam)),
                  gam ]];

              if n/gam gt 2 then
FCFns := FCFns cat [[Factorial(gam)^Floor(n/(2*gam)-2)*G[1]*G[2] ,
Factorial(gam)^Floor(n/(2*gam)-2)*Factorial(Floor(n/gam)-2)*G[2]^2*2,gam]];
DoublePart:=Maximum([Factorial(M)^Floor(gam/M)*Factorial(Floor(gam/M))^2,
                      PrimCand^2, BigBlockCand^2,
                      LittleBlockCand^2, PrimMBlockCand^2 ]);
FCFns := FCFns cat [[Factorial(gam)^Floor(n/(2*gam)-2)*DoublePart ,
Factorial(gam)^Floor(n/(2*gam)-2)*Factorial(Floor(n/gam)-2)*DoublePart*2,
gam ]];
              end if;
```

```
else
  FCFns := FCFns cat [[
     Factorial(gam)^Floor(n/(2*gam))*G[1] ,
     Factorial(gam)^Floor(n/(2*gam))*Factorial(Floor(n/gam)-1)*G[2] ,
    gam ]];
  if IsEven(Floor(gam/M)) then
     SinglePart := Maximum([
         Factorial(M)^Floor(gam/(2*M))*Factorial(Floor(gam/M)) ,
         PrimCand, BigBlockCand, LittleBlockCand, PrimMBlockCand ]);
  else
     SinglePart := Maximum([ PrimCand , BigBlockCand ,
                              LittleBlockCand, PrimMBlockCand ]);
  end if;

FCFns := FCFns cat [[ Factorial(gam)^Floor(n/(2*gam)) ,
     Factorial(gam)^Floor(n/(2*gam))*Factorial(Floor(n/gam)-1)*SinglePart ,
    gam ]];
end if;

if IsEven(Floor(n/M)) then
  FCFns := FCFns cat [[
Factorial(M)^Floor(n/(2*M))*Factorial(Floor(gam/M))^Floor((n-gam)/gam),
Factorial(M)^Floor(n/(2*M))*Factorial(Floor(gam/M))^Floor(n/gam)*
                                              Factorial(Floor(n/gam)),
gam ]];
else
  FCFns := FCFns cat [[
Factorial(M)^Floor((n-gam)/(2*M))*Factorial(Floor(gam/M))^Floor(n/gam-1)*G[1],
Factorial(M)^Floor((n-gam)/(2*M))*Factorial(Floor(gam/M))^Floor(n/gam-1)*
                                       Factorial(Floor(n/gam)-1)*G[2],
gam ]];
   SinglePart := Maximum([ PrimCand , BigBlockCand ,
                                        LittleBlockCand, PrimMBlockCand ]);
  FCFns := FCFns cat [[
Factorial(M)^Floor((n-gam)/(2*M))*Factorial(Floor(gam/M))^Floor(n/gam-1),
Factorial(M)^Floor((n-gam)/(2*M))*Factorial(Floor(gam/M))^Floor(n/gam-1)*
                                  Factorial(Floor(n/gam)-1)*SinglePart,
gam ]];
end if;
```

```
        FCFns := FCFns cat [[ G[1]*G[2]^Floor(n/gam-1) ,
                              G[2]^Floor(n/gam)*Factorial(Floor(n/gam)) ,
                              gam ]];

        MaxCont := Maximum([ PrimCand , BigBlockCand ,
                                   LittleBlockCand , PrimMBlockCand ]);

        FCFns := FCFns cat [[ MaxCont^Floor(n/gam-1) ,
                              MaxCont^Floor(n/gam)*Factorial(Floor(n/gam)) ,
                              gam ]];

      end if;
    end for;

else

    if IsEven(Floor(n/gam)) then
      FCFns := FCFns cat [[ Floor(Factorial(gam)^Floor(n/(2*gam))/2) ,
                  Factorial(gam)^Floor(n/(2*gam))*Factorial(Floor(n/gam)) ,
                  gam ]];

      if n/gam gt 2 then
        FCFns := FCFns cat [[
Factorial(gam)^Floor(n/(2*gam)-2)*PrimBound(gam)^2 ,
Factorial(gam)^Floor(n/(2*gam)-2)*Factorial(Floor(n/gam)-2)*PrimBound(gam)^2,
gam ]];
      end if;

    else

      FCFns := FCFns cat [[
Factorial(gam)^Floor(n/(2*gam)) ,
Factorial(gam)^Floor(n/(2*gam))*Factorial(Floor(n/gam)-1)*PrimBound(gam) ,
gam ]];
    end if;

    FCFns := FCFns cat [[ PrimBound(gam)^Floor(n/gam-1) ,
                          PrimBound(gam)^Floor(n/gam)*Factorial(Floor(n/gam)) ,
                          gam ]];
```

```
        for G in LoadCFs( gam , "F" ) do

          if not IsEven(Floor(n/gam)) then

FCFns := FCFns cat [[ Factorial(gam)^Floor(n/(2*gam))*G[1] ,
Factorial(gam)^Floor(n/(2*gam))*Factorial(Floor(n/gam)-1)*G[2],
gam ]];

          end if;

FCFns := FCFns cat [[ PrimBound(gam)^Floor(n/gam-1)*G[1] ,
PrimBound(gam)^Floor(n/gam-1)*Factorial(Floor(n/gam)-1)*G[2] ,
gam ]];

        end for;

      end if;

    end if;

  end for;

  return FCFns;

end function;
```

```
// Function to build all core-free
buildACFs := function( n )
  TCFs  := LoadCFs( n , "T" );
  FCFs  := LoadCFs( n , "F" );
  ACFns  := FCFs;
  min   := [0 : d in [1..n]];
  for CF in ACFns do
    if CF[1] gt min[CF[3]] then
      d := CF[3];
      while d gt 0 and CF[1] gt min[d] do
        min[d] := CF[1];
        d    -:= 1;
      end while;
    end if;
  end for;

  for gam in [ 1..n-1 ] do
    AnmgCFs := LoadCFs( n-gam , "A" );
    gFCFs  := LoadCFs( gam , "F" );
    for G0 in gFCFs do
      s := G0[3];
      for G1 in AnmgCFs do
        if G1[3] gt s then
          if s gt 1 then
            if G0[2]*G1[2] gt min[s] then

              ACFns := ACFns cat [[
                Minimum([G0[1]*G1[2],G1[1]*G0[2]]),
                G0[2]*G1[2]              ,
                s                ]];

              if ACFns[#ACFns][1] gt min[s] then
                d := s;
                while d gt 0 and ACFns[#ACFns][1] gt min[d] do
                  min[d] := ACFns[#ACFns][1];
                  d    -:= 1;
                end while;
              end if;

            end if;
```

```
            else
              if G0[2]*G1[2] gt min[s] then
                ACFns := ACFns cat [[ G1[1] , G0[2]*G1[2] , s]];

                if ACFns[#ACFns][1] gt min[s] then
                  d := s;
                  while d gt 0 and ACFns[#ACFns][1] gt min[d] do
                    min[d] := ACFns[#ACFns][1];
                    d    -:= 1;
                  end while;
                end if;
              end if;
            end if;
        end if;
      end for;
    end for;
  end for;

  return ACFns;

end function;

// Code to sort a sequence of groups by size removing those G with #G and
// #N(G) smaller than #H and #N(H) for some other H

// Order by size, minimal orbit then normaliser
CFComp := function( G,H )
  return 4*Sign( G[1] - H[1] ) + 2*Sign( G[3] - H[3] ) + Sign(G[2]-H[2] );
end function;

// Order by minimal orbit, then size then normaliser
CFCompInit := function( G,H )
  if #G lt 3 then G; end if;
  return 2*Sign( G[1] - H[1] ) + 4*Sign( G[3] - H[3] ) + Sign(G[2]-H[2] );
end function;
```

```
CFSortReduce := procedure( ~CFs )
  Sort( ~CFs , CFCompInit );

  i := #CFs;
  while i gt 1 do

    if CFs[i-1][3] eq CFs[i][3] and //same minimal orbit size so
                                    //#CFs[i] is at least #CFs[i-1]
      CFs[i-1][2] le CFs[i][2] then //#N(CFs[i]) is at least #N(CFs[i-1])
      CFs := CFs[1..i-2] cat CFs[ i ..#CFs]; //#CFs[i-1] is redundant

    end if;

    i -:=1;
  end while;

  Sort( ~CFs , CFComp );
end procedure;

CFSecondReduce := procedure( ~CFs )

  i := 1;
  while i lt #CFs do
    j := i+1;
    while j le #CFs do
      //#CFs[j] is at least #CFs[i]
      if CFs[i][2] le CFs[j][2] and CFs[i][3] le CFs[j][3] then
        //#N(CFs[j]) is at least #N(CFs[i]) and
        //has larger minimal orbit size so CFs[i] redundant
        CFs := CFs[1..i-1] cat CFs[i+1..#CFs];
        j := i+1;
      else
        j +:= 1;
      end if;
    end while;
    i +:= 1;
  end while;

end procedure;
```

```
// Functions to save and load lists of CFSortReduce

SaveCFs := procedure( CFs , n , level )
  // level should be string "P", "T", "F" or "A"
  // These directories must exist

  System("rm " cat level cat "/" cat IntegerToString(n) cat " 2>/dev/null");
  System("touch " cat level cat "/" cat IntegerToString(n));
  i:=1;
  for G in CFs do
    if i gt 1 then System("echo \"\\n\" >>" cat level cat "/"
                                 cat IntegerToString(n) ); end if;
    System("echo \"" cat IntegerToString(G[1]) cat " " cat
           IntegerToString(G[2]) cat " " cat
           IntegerToString(G[3]) cat "\" >>" cat
           level cat "/" cat IntegerToString(n) );

  end for;

end procedure;

LoadCFs := function( n , level )

  F  := Open( level cat "/" cat IntegerToString(n) , "r" );
  CFs := [];

  while true do
    s := Gets(F);
    if IsEof(s) then break; end if;
    if #StringToIntegerSequence(s) eq 3 then
      CFs := CFs cat [StringToIntegerSequence(s)];
    else
      printf "warning: reading %o/%o : found %o\n" ,
        level , n , s;
    end if;
  end while;

  return CFs;
end function;
```

```
//build TCFs, FCFs then ACFs
runTAFs := procedure( MIN , MAX )

  printf "building TCFs, FCFs, ACFs [ %o : %o ]\n" , MIN , MAX;

  for n in [ MIN..MAX ] do

    //TCFS
    CFs := buildTCFs( n );
    CFSortReduce( ~CFs );
    SaveCFs( CFs , n , "T" );

    //FCFs
    CFs := buildFCFs( n );
    CFSortReduce( ~CFs );
    SaveCFs( CFs , n , "F" );

    //ACFs
    CFs := buildACFs( n );
    CFSortReduce( ~CFs );
    CFSecondReduce( ~CFs );
    SaveCFs( CFs , n , "A" );

    if n le 28 then
      if CFs[#CFs][1] ne known[n] then

        printf "%3o : A : %11o : %o\n" , n , known[n] , CFs[#CFs];

      end if;
    elif n mod 8 eq 0 or n mod 8 eq 1 then
      if CFs[#CFs][1] ne Factorial(Floor(n/2)) then

        printf "%3o : A : %11o \n" , n , 1.0*Factorial(Floor(n/2))/CFs[#CFs][1]

      end if;
```

```
    else
      if CFs[#CFs][1] ne Factorial(Floor(n/2))/2 then

        printf "%3o : A : %11o \n",n,1.0*Factorial(Floor(n/2))/(2*CFs[#CFs][1])

      end if;
    end if;

    if (n+1 - MIN) mod 20 eq 0 then
      printf "%o / %o\n" , n+1-MIN , MAX+1-MIN;
    end if;
  end for;

end procedure;
```

A.2 Sporadic Groups

In this section we include an example MAGMA function implementing the method described in Section 3.3

```
//MSAS standing for Maximal Subgroup Avoiding Subgroup.
//assumes subgroups have order at least bound

MSAS := function( G , S )
  //initial record of largest known subgroup avoiding subgroup
  M := <sub<G|Id(G)>,bound>;

  //queue of subgroups considered
  Q := MaximalSubgroups(G);

  //loop over subgroups by taking successive maximal subgroups
  while #Q ge 1 do
    Sort(~Q,func<x,y|y`order-x`order>);
    H := Q[1];
    if H`order lt M[2] then break; end if;
    i := 1;
    while i le #Q and H`order eq Q[i]`order do
      if IsConjugate(G,H`subgroup, Q[i]`subgroup) then
        Q := Q[1..i-1] cat Q[i+1..#Q];
      else
        i +:= 1;
      end if;
    end while;

    //check H
    if H`order gt M[2] then
      if H`subgroup meet S eq sub<G|Id(G)> then
        M := <H`subgroup , H`order>;
      else
        Q := MaximalSubgroups(H`subgroup) cat Q;
      end if;
    end if;
  end while;

  return M;
end function;
```

```
//MAGMA code to run through calculation of minimal degrees
//of Schur covers of sporadic simple groups.

load "MSAS";

//simple socles

load "2M12.txt";
H := MSAS(G, Center(G));
printf "%o\n %o\n\n" , #G/H[2] , CompositionFactors(H[1]);

load "2J2.txt";
H := MSAS(G, Center(G));
printf "%o\n %o\n\n" , #G/H[2] , CompositionFactors(H[1]);

load "3J3.txt";
H := MSAS(G, Center(G));
printf "%o\n %o\n\n" , #G/H[2] , CompositionFactors(H[1]);

load "2HS.txt";
H := MSAS(G, Center(G));
printf "%o\n %o\n\n" , #G/H[2] , CompositionFactors(H[1]);

load "3McL.txt";
H := MSAS(G, Center(G));
printf "%o\n %o\n\n" , #G/H[2] , CompositionFactors(H[1]);

load "2Ru.txt";
H := MSAS(G, Center(G));
printf "%o\n %o\n\n" , #G/H[2] , CompositionFactors(H[1]);

//requires atlas database
load "3ON.txt";
H := MSAS(G, Center(G));
printf "%o\n %o\n\n" , #G/H[2] , CompositionFactors(H[1]);
```

```
//non-simple socles

load "12M22.txt";
ord := #G;
H12 := MSAS(G,Center(G));
H12[2];
H4 := MSAS(G,Sylow(Center(G),2):bound:=H12[2]);
H4[2];
H3 := MSAS(G,Sylow(Center(G),3):bound:=1/(1/(H12[2]+1/H4[2])));
H3[2];
if ord/H12[2] le ord/H4[2]+ord/H3[2] then
  printf "%o\n %o\n\n", ord/H12[2], CompositionFactors(H12[1]);
else
  printf "%o\n %o\n %o\n\n", ord/H4[2]+ord/H3[2],
     CompositionFactors(H4[1]), CompositionFactors(H3[1]);
end if;

load "6Fi22.txt";
ord := #G;
H6 := MSAS(G,Center(G));
H6[2];
H2 := MSAS(G,Sylow(Center(G),2):bound:=H6[2]);
H2[2];
H3 := MSAS(G,Sylow(Center(G),3):bound:=1/(1/(H6[2]+1/H2[2])));
H3[2];
if ord/H6[2] le ord/H2[2]+ord/H3[2] then
  printf "%o\n %o\n\n", ord/H6[2], CompositionFactors(H6[1]);
else
  printf "%o\n %o\n %o\n\n", ord/H2[2]+ord/H3[2],
     CompositionFactors(H2[1]), CompositionFactors(H3[1]);
end if;
```

```
load "6Suz.txt";
ord := #G;
H6 := MSAS(G,Center(G));
H6[2];
H2 := MSAS(G,Sylow(Center(G),2):bound:=H6[2]);
H2[2];
H3 := MSAS(G,Sylow(Center(G),3):bound:=1/(1/(H6[2]+1/H2[2])));
H3[2];
if ord/H6[2] le ord/H2[2]+ord/H3[2] then
  printf "%o\n %o\n\n" , ord/H6[2] , CompositionFactors(H6[1]);
else
  printf "%o\n %o\n %o\n\n" , ord/H2[2]+ord/H3[2] ,
     CompositionFactors(H2[1]) , CompositionFactors(H3[1]);
end if;
```

Bibliography

[1] John Bamberg and Cheryl E. Praeger. Finite permutation groups with a transitive minimal normal subgroup. *Proc. London Math. Soc. (3)*, 89(1):71–103, 2004.

[2] Oren Becker. The minimal degree of permutation representations of finite groups, 2012. preprint, `https://arxiv.org/abs/1204.1668`.

[3] John J. Cannon, Derek F. Holt, and William R. Unger. The use of permutation representations in structural computations in large finite matrix groups. *J. Symbolic Comput.*, 95:26–38, 2019.

[4] Robert Chamberlain. Minimal exceptional p-groups. *Bulletin of the Australian Mathematical Society*, 98(3):434–438, 2018.

[5] Robert Chamberlain. Subgroups with no abelian composition factors are not distinguished. *Bull. Aust. Math. Soc.*, 101(3):446–452, 2020.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[7] Bruce N. Cooperstein. Minimal degree for a permutation representation of a classical group. *Israel J. Math.*, 30(3):213–235, 1978.

[8] David Easdown and Michael Hendriksen. Minimal permutation representations of semidirect products of groups. *J. Group Theory*, 19(6):1017–1048, 2016.

[9] David Easdown and Cheryl E. Praeger. On minimal faithful permutation representations of finite groups. *Bull. Austral. Math. Soc.*, 38(2):207–220, 1988.

[10] Simon Guest, Joy Morris, Cheryl E. Praeger, and Pablo Spiga. On the maximum orders of elements of finite almost simple groups and primitive permutation groups. *Trans. Amer. Math. Soc.*, 367(11):7665–7694, 2015.

[11] Simon Guest, Joy Morris, Cheryl E. Praeger, and Pablo Spiga. On the maximum orders of elements of finite almost simple groups and primitive permutation groups. *Trans. Amer. Math. Soc.*, 367(11):7665–7694, 2015.

[12] Marshall Hall, Jr. *The theory of groups*. Chelsea Publishing Co., New York, 1976. Reprinting of the 1968 edition.

[13] Derek F. Holt and Jacqueline Walton. Representing the quotient groups of a finite permutation group. *J. Algebra*, 248(1):307–333, 2002.

[14] Qiaochu Yuan (https://math.stackexchange.com/users/232/qiaochu yuan). Maximise $(s!)^{\frac{n}{s}}\frac{n}{s}!$. Mathematics Stack Exchange. `https://math.stackexchange.com/q/2315217` (version: 2017-06-08).

[15] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.

[16] D. L. Johnson. Minimal permutation representations of finite groups. *Amer. J. Math.*, 93:857–866, 1971.

[17] L. G. Kovács and Cheryl E. Praeger. Finite permutation groups with large abelian quotients. *Pacific J. Math.*, 136(2):283–292, 1989.

[18] L. G. Kovács and Cheryl E. Praeger. On minimal faithful permutation representations of finite groups. *Bull. Austral. Math. Soc.*, 62(2):311–317, 2000.

[19] Attila Maróti. On the orders of primitive groups. *J. Algebra*, 258(2):631–640, 2002.

[20] V. D. Mazurov. Minimal permutation representations of finite simple classical groups. Special linear, symplectic and unitary groups. *Algebra i Logika*, 32(3):267–287, 343, 1993.

[21] Jack McLaughlin. Some groups generated by transvections. *Arch. Math. (Basel)*, 18:364–368, 1967.

[22] Peter M. Neumann. Some algorithms for computing with finite permutation groups. In *Proceedings of groups—St. Andrews 1985*, volume 121 of *London Math. Soc. Lecture Note Ser.*, pages 59–92. Cambridge Univ. Press, Cambridge, 1986.

[23] Herbert Robbins. A remark on Stirling's formula. *Amer. Math. Monthly*, 62:26–29, 1955.

[24] Gary M. Seitz. Flag-transitive subgroups of Chevalley groups. *Ann. of Math. (2)*, 97:27–56, 1973.

[25] Charles Wells. Some applications of the wreath product construction. *Amer. Math. Monthly*, 83(5):317–338, 1976.

[26] Helmut Wielandt. *Finite permutation groups*. Translated from the German by R. Bercov. Academic Press, New York-London, 1964.

[27] D. Wright. Degrees of minimal embeddings for some direct products. *Amer. J. Math.*, 97(4):897–903, 1975.