Minimal generation of transitive permutation groups

Tracey, Gareth

Minimal generation of transitive permutation groups

Gareth M. Tracey*

Mathematics Institute, University of Warwick,
Coventry CV4 7AL, United Kingdom

October 30, 2017

Abstract

This paper discusses upper bounds on the minimal number of elements $d(G)$ required to generate a transitive permutation group G, in terms of its degree n, and its order $|G|$. In particular, we reduce a conjecture of L. Pyber on the number of subgroups of the symmetric group $\mathrm{Sym}(n)$. We also prove that our bounds are best possible.

1 Introduction

A well-developed branch of finite group theory studies properties of certain classes of permutation groups as functions of their degree. The purpose of this paper is to study the minimal generation of transitive permutation groups.

For a group G, let $d(G)$ denote the minimal number of elements required to generate G. In [21], [7], [26] and [28], it is shown that $d(G) = O(n/\sqrt{\log n})$ whenever G is a transitive permutation group of degree $n \geq 2$ (here, and throughout this paper, "log" means log to the base 2). A beautifully constructed family of examples due to L. Kovács and M. Newman shows that this bound is 'asymptotically best possible' (see Example 6.10), thereby ending the hope that a bound of $d(G) = O(\log n)$ could be proved.

The constants involved in these theorems, however, were never estimated. We prove:

Theorem 1.1. *Let G be a transitive permutation group of degree $n \geq 2$. Then*

(1) $d(G) \leq \left\lfloor \frac{cn}{\sqrt{\log n}} \right\rfloor$ *,where* $c := 1512660\sqrt{\log(2^{19}15)}/(2^{19}15) = 0.920581\ldots$*, and;*

(2) $d(G) \leq \left\lfloor \frac{c_1 n}{\sqrt{\log n}} \right\rfloor$*, where* $c_1 := \sqrt{3}/2 = 0.866025\ldots$*, unless each of the following conditions hold:*

(i) $n = 2^k v$*, where* $v = 5$ *and* $17 \leq k \leq 26$*, or* $v = 15$ *and* $15 \leq k \leq 35$*, and;*

(ii) G contains no soluble transitive subgroups.

In fact, we prove a slightly stronger version of Theorem 1.1, which is given as Theorem 5.3. The following corollary is immediate.

*Electronic address: G.M.Tracey@warwick.ac.uk

Corollary 1.2. *Let G be a transitive permutation group of degree n, containing a soluble transitive subgroup. Then*

$$d(G) \leq \left\lfloor \frac{c_1 n}{\sqrt{\log n}} \right\rfloor,$$

where $c_1 = \sqrt{3}/2$.

As shown in [21], apart from the choice of constants, the bounds in our results are of the right order. Moreover, the infimum of the set of constants $\overline{c}$ satisfying $d(G) \leq \overline{c}n/\sqrt{\log n}$, for all soluble transitive permutation groups G of degree $n \geq 2$, is the constant c_1 in Theorem 6.2, since $d(G) = 4$ when $n = 8$ and $G \cong D_8 \circ D_8$. We conjecture that the best 'asymptotic' bound, that is, the best possible upper bound when one is permitted to exclude finitely many cases, is

$$d(G) \leq \left\lfloor \frac{\widetilde{c}n}{\sqrt{\log n}} \right\rfloor,$$

where $\widetilde{c}$ is some constant satisfying

$$b/2 \leq \widetilde{c} < b := \sqrt{2/\pi}$$

(see Example 6.10 for more details).

The constant b, and the function $n/\sqrt{\log n}$, enter our work by means of the following combinatorial result. For a partially ordered set P, $w(P)$ denotes the *width* of P, that is $w(P)$ denotes the size of the largest antichain in P.

Theorem 1.3. *Suppose that a partially ordered set P, of cardinality $s \geq 2$, is a cartesian product of the chains P_1, P_2, ..., P_t, where each P_i has cardinality k_i. Let $K := \sum_{i=1}^{t} k_i$. Then*

$$w(P) \leq \left\lfloor \frac{s}{2^K} \binom{K}{\lfloor K/2 \rfloor} \right\rfloor \leq \left\lfloor \frac{bs}{\sqrt{K}} \right\rfloor \leq \left\lfloor \frac{bs}{\sqrt{\log s}} \right\rfloor,$$

where $b = \sqrt{2/\pi}$. Furthermore, if each chain has the same cardinality p, then $w(P) \leq \lfloor bp^t/\sqrt{t(p-1)} \rfloor$.

We remark that an asymptotic version of this bound is proved in [7, Theorem 1.4].

To state the key application of Theorem 1.3, we require two definitions.

Definition 1.4. For a positive integer s with prime factorisation $s = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$, set $\omega(s) := \sum r_i$, $\omega_1(s) := \sum r_i p_i$, $K(s) := \omega_1(s) - \omega(s) = \sum r_i(p_i - 1)$ and

$$\widetilde{\omega}(s) = \frac{s}{2^{K(s)}} \binom{K(s)}{\left\lfloor \frac{K(s)}{2} \right\rfloor}.$$

For a prime p, write s_p for the p-part of s.

Definition 1.5. Let s be a positive integer, and let p be prime. We define s_p to be the p-part of s, $\mathrm{lpp}\,(s) = \max\{s_q : q \text{ prime}\}$, and

$$E(s,p) := \min \left\{ \left\lfloor \frac{bs}{\sqrt{(p-1)\log_p s_p}} \right\rfloor, \frac{s}{\mathrm{lpp}\,(s/s_p)} \right\} \text{ and } E_{sol}(s,p) := \min\{\widetilde{\omega}(s), s_p\}$$

where we take $\left\lfloor bs/\sqrt{(p-1)\log_p s_p} \right\rfloor$ to be ∞ if $s_p = 1$.

The mentioned application can now be given as follows.

Theorem 1.6. *Let G be a finite group, let $\mathbb{F}$ be a field of characteristic $p > 0$, let H be a subgroup of G, and let V be an $\mathbb{F}[H]$-module, of dimension a. Let S be the group induced by G on the set of (right) cosets of H. Define E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise. Let M be a submodule of the induced module $V\uparrow_H^G$. Then $d_G(M) \leq aE'(s,p)$.*

Here, $d_G(M)$ denotes the minimal number of elements required to generate M as a G-module. We actually prove slightly stronger results than Theorem 1.6 - see Theorem 4.13 and Theorem 4.24.

Our next main result is motivated by a conjecture of L. Pyber, which states that: *The number of subgroups* $|\mathrm{Sub}(\mathrm{Sym}(n))|$ *of* $\mathrm{Sym}(n)$ *is precisely* $2^{(\frac{1}{16}+o(1))n^2}$ [35]. For $m \in \mathbb{N}$, let $\mathrm{Sub}_m(\mathrm{Sym}(n))$ denote the set of subgroups H of $\mathrm{Sym}(n)$ with the property that all H-orbits are of length at most m. J.C. Schlage-Puchta (private correspondence) has proven that if the quantity

$$f(n) := \max\{d(G)\log|G|/n^2 : G \leq \mathrm{Sym}(n) \text{ transitive}\}$$

approaches 0 as n tends to ∞, then there exists an absolute constant $\underline{c}$ such that the number of subgroups of $\mathrm{Sym}(n)$ is at most $2^{o(n^2)}\,\mathrm{Sub}_{\underline{c}}(\mathrm{Sym}(n))$. This reduces Pyber's conjecture to counting the number of subgroups that have all orbit lengths bounded above by $\underline{c}$.

Motivated by this, we prove the following.

Theorem 1.7. *There exists an absolute constant C such that*

$$d(G) \leq \left\lfloor \frac{Cn^2}{\log|G|\sqrt{\log n}} \right\rfloor$$

whenever G is a transitive permutation group of degree $n \geq 2$.

In particular, the discussed reduction of Pyber's conjecture follows. We remark that the bound in Theorem 1.7 is 'asymptotically best possible'. See Example 6.10 for more details.

Finally, we also discuss minimally transitive permutation groups. A transitive permutation group G is said to be *minimally transitive* if every proper subgroup of G is intransitive. Since every transitive group contains a minimally transitive subgroup, these groups arise naturally in reduction arguments.

Minimally transitive groups also have applications in Combinatorics (for counting vertex transitive graphs; for example, see [3]), and in the theory of BFC-groups (see [31] and [37]). In this paper, we use them to study minimal generator numbers in modules for permutation groups. Thus, some information on their structure is desirable. Our main result is as follows.

Theorem 1.8. *Let G be a minimally transitive permutation group of degree $n = 2^m 3$. Then one of the following holds:*

(i) G is soluble, or:

(ii) G has a unique nonabelian chief factor, which is a direct product of copies of $L_2(p)$, where p is a Mersenne prime.

A minimally transitive group of prime power degree is a p-group (see Lemma 3.1), so is in particular soluble; the motivation behind Theorem 1.8 is to study how far away from being soluble a minimally

transitive group of degree $n := 2^m 3$ is. It would be interesting to study the same question for minimally transitive groups of degree $n := p^m q$, for arbitrary primes p and q. For an analysis of the case $n = pq$, for distinct primes p and q, see [40], [23] and [13].

For information about minimal generator numbers in minimally transitive groups, see [38].

The layout of the paper is as follows: In Section 2, we discuss preliminary results in Permutation Group Theory and Representation Theory. In Section 3 we discuss minimally transitive groups and prove Theorem 1.8. Section 4 is the critical step of the paper: there, we prove upper bounds on the minimal number of elements $d_G(M)$ required to generate a submodule M of an induced module $V \uparrow_H^G$ for a finite group G, and a subgroup $H \leq G$. These bounds are derived in terms of $\dim V$, $|G : H|$, and some additional data when either the field involved is finite, or when G is insoluble. In particular, we prove Theorem 1.6. We also prove Theorem 1.3 in Section 4. In Section 5, we prove a stronger version of Theorem 5.3, while in Section 6 we prove Theorem 1.7.

Our proofs are theoretical, although we do use MAGMA [5] for computations of generator numbers and composition factors for some groups of small order. In particular, we compute the maximum values of $d(G)$ as G runs over the transitive groups of degree n, for $2 \leq n \leq 32$.

Notation: The following is a table of constants which will be used throughout the paper.

b	$\sqrt{2/\pi} = 0.797885\ldots$
b_1	$\sqrt{2}b = 1.12838\ldots$
c_1	$\sqrt{3}/2 = 0.866025\ldots$
c	$1512660\sqrt{\log(2^{19}15)}/(2^{19}15) = 0.920581\ldots$
c_0	$\log_9 48 + (1/3)\log_9 24 = 2.24399\ldots$
c'	$\ln 2/1.25506 = 0.552282\ldots$

We will adopt the $\mathbb{ATLAS}$ [11] notation for group names, although we will usually write $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ for the symmetric and alternating groups of degree n. Furthermore, these groups, and their subgroups, act naturally on the set $\{1, \ldots, n\}$; we will make no further mention of this.

The centre of a group G will be written as $Z(G)$, the Frattini subgroup as $\Phi(G)$, and the Fitting subgroup as $F(G)$. The letters G, H, K and L will usually be used for groups, while U, V and W will usually be modules. The letter M will usually denote a submodule. Finally, group homomorphisms will be written on the right.

We finish by recording a definition which will be used throughout the paper.

Definition 1.9. Let G be a group.

(a) Write $a(G)$ to denote the composition length of G.

(b) Let $a_{ab}(G)$ and $a_{nonab}(G)$ denote the number of abelian and non-abelian composition factors of G, respectively.

(c) Let $c_{nonab}(G)$ denote the number of non-abelian chief factors of G.

The author is hugely indebted to his supervisor Professor Derek Holt for many useful discussions and suggestions; without them, this paper would not be possible. He would also like to thank both Dr. Tim Burness and the referee for many useful comments and suggestions. Finally, he would also like to thank the Engineering and Physical Sciences Research Council for their financial support.

2 Preliminaries

2.1 Permutation groups

We begin with some notation. Suppose that G is a group acting on a set Ω, via the homomorphism $\theta : G \to \mathrm{Sym}(\Omega)$. When there is no ambiguity, we will abbreviate $\omega^{g\theta}$ to ω^g, for $g \in G$, $\omega \in \Omega$. We will also write

$$G^\Omega := G\theta, \text{ and } \mathrm{Ker}_G(\Omega) := \mathrm{Ker}(\theta)$$

to denote the image and kernel of θ, respectively. The orbit $\omega^{G\theta}$ of $\omega \in \Omega$ under the action of G will be abbreviated to ω^G, while the stabiliser will be written as $\mathrm{Stab}_G(\omega)$. If Ω is finite of cardinality n, we have

$$(\mathrm{Sym}(\Omega), \Omega) \cong (\mathrm{Sym}(n), \{1, \ldots, n\}).$$

Thus, in this case, we will usually write $\mathrm{Sym}\,(\Omega) = \mathrm{Sym}\,(n) = S_n$, and say that a subgroup $G \leq \mathrm{Sym}(\Omega)$ is a *permutation group of degree* n. If, for $1 = 1, 2$, G_i is a group acting on the set Ω_i, we will write $(G_1, \Omega_1) \cong (G, \Omega_2)$ if $(G_1, \Omega_1) \cong (G, \Omega_2)$ are permutation isomorphic.

Let ω_i^G, $i \in I$, denote the orbits in Ω under the action of G (the set I is an index set). The groups $G^{\omega_i^G}$ are called the *transitive constituents* of G on Ω.

Definition 2.1. Let G_i, $i \in I$, be a set of groups. A subgroup G of the direct product $\prod_i G_i$ is called a *subdirect product* of the G_i if $\pi_i|_G : G \to G_i$ is surjective for each projection map $\pi_i : \prod_i G_i \to G_i$.

We note the following easily proved proposition, which will be used frequently.

Proposition 2.2 (**[8], Theorem 1.1**). *Let the group G act on the finite set Ω. Then G^Ω is isomorphic to a subdirect product of its transitive constituents.*

2.2 Wreath products

Let R be a finite group, let S be a permutation group of degree s, and consider the wreath product $R \wr S$, as constructed in [8]. Let B be the base group of $R \wr S$, so that B is isomorphic to the direct product of s copies of R. Thus, for a subgroup L of R, B contains the direct product of s copies of L: we will denote this direct product by B_L (so that $B_1 = 1$ and $B_R = B$).

Now, for each $1 \leq i \leq s$, set

$$R_{(i)} := \{(g_1, \ldots, g_s) \in B : g_j = 1 \text{ for all } j \neq i\} \trianglelefteq B.$$

Then $R_{(i)} \cong R$, and $B = \prod_{1 \leq i \leq s} R_{(i)}$. Furthermore, $N_{R\wr S}(R_{(i)}) \cong R_{(i)} \times (R \wr \mathrm{Stab}_S(i))$. Hence, we may define the projection maps

$$\rho_i : N_{R\wr S}(R_{(\gamma)}) \to R_{(i)}. \tag{2.1}$$

We also define $\pi : R \wr S \to S$ to be the quotient map by B. This allows us to define a special class of subgroups of $R \wr S$.

Definition 2.3. A subgroup G of $R \wr S$ is called *large* if

(a) $G\rho_i = R_{(i)}$ for all i in $1 \leq i \leq s$, and;

(b) $G\pi = S$.

Remark 2.4. Suppose, in addition, that R is a permutation group of degree $r > 1$. If $s > 1$ and G is a large subgroup of $R \wr S$, then G is a transitive, and imprimitive, permutation group of degree rs, with a system of s blocks, each of cardinality r. (G acts on the cartesian product $\{1, \ldots, r\} \times \{1, \ldots, s\}$ in this case.

In fact, it turns out that all imprimitive permutation groups arise as a large subgroup of a certain wreath product.

Theorem 2.5 (**[39], Theorem 3.3**). *Let G be an imprimitive permutation group on a set Ω_1, and let Δ be a block for G. Also, let $\Gamma := \Delta^G$ be the set of G-translates of Δ, and set $\Omega_2 := \Delta \times \Gamma$. Denote by R and S the permutation groups $\mathrm{Stab}_G(\Delta)^\Delta$, and G^{Δ^G}, on Δ and Γ respectively. Then*

(i) $G \cong G^{\Omega_2}$ is isomorphic to a large subgroup of $R \wr S$, and;

(ii) (G, Ω_1) and (G, Ω_2) are permutation isomorphic.

If G is an imprimitive permutation group, and the block Δ as in Theorem 2.5 is assumed to be a minimal block for G, then the group $R = \mathrm{Stab}_G(\Delta)^\Delta$ is primitive. When Ω is finite we can iterate this process, and deduce the following.

Corollary 2.6. *Let G be a transitive permutation group on a finite set Ω. Then there exist primitive permutation groups R_1, R_2, ..., R_t such that G is a subgroup of $R_1 \wr R_2 \wr \ldots \wr R_t$.*

Remark 2.7. The wreath product construction is associative, in the sense that $R \wr (S \wr T) \cong (R \wr S) \wr T$, so the iterated wreath product in Corollary 2.6 is well-defined.

Definition 2.8. The tuple $(R_1, R_2, \ldots, R_t)$, where the R_i are as in Corollary 2.6, is called *a tuple of primitive components* for G on Ω.

We caution the reader that a tuple of primitive components for an imprimitive permutation group G on a set Ω is not necessarily unique - see [8, Page 13] for an example.

We close this subsection with an easy lemma concerning the alternating group $\mathrm{Alt}(d)$.

Lemma 2.9. *Let $D \cong \mathrm{Alt}(d)$ be the alternating group of degree $d \geq 5$, and let p be prime. Then D contains a soluble subgroup E with at most two orbits, such that each orbit has p'-length.*

Proof. Assume first that $p = 2$. Then since n is either odd, or a sum of two odd numbers, we can take $E := \langle x_1 x_2 \rangle$, where x_1 is a cycle of odd length, either $x_2 = 1$ or x_2 is a cycle of odd length, and d is the sum of the orders (i.e. lengths) of x_1 and x_2.

So assume that $p > 2$, and write $d = tp + k$, where $0 \leq k \leq p - 1$. If $k \neq p - 1$, then take E_1 to be a soluble transitive subgroup of $\mathrm{Alt}(tp - 1)$, and take E_2 to be a soluble transitive subgroup of $\mathrm{Alt}(k + 1)$. If $k = p - 1$, then take E_1 to be a soluble transitive subgroup of $\mathrm{Alt}(tp + 1)$, and take E_2 to be a soluble transitive subgroup of $\mathrm{Alt}(k - 1)$ (note that $k - 1 > 0$ since $p > 2$). Finally, taking $E := E_1 \times E_2 \leq D$ give us what we need, and proves the claim. □

2.3 Asymptotic results for permutation groups

We will frequently use a result on composition length, due to Pyber. First, define the constant

$$c_0 := \log_9 48 + (1/3)\log_9 24 = 2.24399\ldots \tag{2.2}$$

The result of Pyber can now be given as follows. It is stated slightly different to how it is stated in [34].

Theorem 2.10 ([34], Theorem 2.10). *Let R be a primitive permutation group of degree $r \geq 2$. Then $a_{ab}(R) \leq (1 + c_0)\log r - (1/3)\log 24$, and $a_{nonab}(R) \leq \log r$.*

We shall also require the following theorem of D. Holt and C. Roney-Dougal on generator numbers in primitive groups.

Theorem 2.11 ([19], Theorem 1.1). *Let H be a subnormal subgroup of a primitive permutation group of degree r. Then $d(H) \leq \lfloor \log r \rfloor$, except that $d(H) = 2$ when $m = 3$ and $H \cong \mathrm{Sym}(3)$.*

We deduce the following easy consequence.

Corollary 2.12. *Let G be an imprimitive permutation group of degree n, and suppose that G has a minimal block Δ of cardinality $r \geq 4$. Let S denote the induced action of G on the set of distinct G-translates of Δ. Then $d(G) \leq s\lfloor \log r \rfloor + d(S)$, where $s := n/r$.*

Proof. Let R be the induced action of the block stabiliser $\mathrm{Stab}_G(\Delta)$ on Δ, and let $K := \mathrm{Ker}_G(\Omega)$ be the kernel of the action of G on the set Ω of distinct G-translates of Δ. Then $K^\Delta \trianglelefteq R$, and hence, by Theorem 2.11, each normal subgroup of K^Δ can be generated by $\lfloor \log r \rfloor$ elements.

Since $K \trianglelefteq G$, we have

$$(K, \Delta) \cong (K, \Delta^g) \tag{2.3}$$

for all $g \in G$. Also, since R is primitive, $K^\Delta \trianglelefteq R$ is either trivial or transitive. If K^Δ is trivial, then K is trivial by 2.3, and hence $d(G) = d(G/K) = d(S)$. So assume that K^Δ is transitive. Then K is an iterated subdirect product of s copies of K^Δ, by Proposition 2.2. Hence, $d(K) \leq s\lfloor \log r \rfloor$ by the previous paragraph. Since $G/K \cong S$, the claim follows. □

2.4 Some results from Representation Theory

We now record two lemmas which will be key in the proof of Proposition 4.9. The first has a stronger version which is stated in [19, Lemma 2.13], but we only require the following.

Lemma 2.13 ([19], Lemma 2.13). *Let $G \leq GL_n(\mathbb{F})$ be finite, let $V = \mathbb{F}^n$ be the natural module, and assume that G acts irreducibly on V. Suppose that*

1. *$V\downarrow_L$ is homogeneous for each normal subgroup L of G; and*
2. *G has no non-trivial abelian quotients.*

Then G is isomorphic to a subgroup of $GL_{n/f}(\mathbb{K})$ for some divisor f of n, and some extension field $\mathbb{K}$ of $\mathbb{F}$ of degree f. Furthermore, if W denotes the natural module for $GL_{n/f}(\mathbb{K})$, then G acts irreducibly on W and

(i) $W\downarrow_L$ is homogeneous for each normal subgroup L of G;

(ii) $Z(G)$ is cyclic; and

(iii) Each abelian characteristic subgroup of G is contained in $Z(GL_{n/f}(\mathbb{K}))$.

Lemma 2.14. *Let $G \leq GL_n(\mathbb{F})$ be finite, let V be the natural module, and assume that V is irreducible. Suppose that $1 \neq E \trianglelefteq L \trianglelefteq G$, and that $V\downarrow_L$ is homogeneous. Suppose that $\mathbb{K} \supseteq \mathbb{F}$ is a splitting field for all subgroups of L, and assume that the resulting extension $\mathbb{K}/\mathbb{F}$ is normal. Then $V^{\mathbb{K}}\downarrow_E$ is a non-trivial completely reducible $\mathbb{K}[E]$-module.*

Proof. Since L is homogeneous, $V\downarrow_L \cong eU$, for some irreducible $\mathbb{F}[L]$-module U and some positive integer e. Since G is faithful on V and $L \neq 1$, L is faithful on U. Moreover, $U^{\mathbb{K}}$ is completely reducible, and each of its irreducible constituents are algebraically conjugate, by [12, Theorem 70.15]. It follows that L is faithful on $V^{\mathbb{K}}\downarrow_L$, and hence $V^{\mathbb{K}}\downarrow_E$ is non-trivial. Also, since $E \trianglelefteq L$, and

$$V^{\mathbb{K}}\downarrow_E \cong V^{\mathbb{K}}\downarrow_L\downarrow_E,$$

it follows from Clifford's Theorem (see [12, Theorem 49.7]) that $V^{\mathbb{K}}\downarrow_E$ is completely reducible. This completes the proof. □

Remark 2.15. Let $\mathbb{K}$ be a splitting field for the finite group G, containing the field $\mathbb{F}$. Then every field $\mathbb{E}$ containing $\mathbb{K}$ is also a splitting field for G (for example, see [20, Corollary 9.8]). Thus, one can always find a splitting field $\mathbb{E}$ for G such that $\mathbb{E}/\mathbb{F}$ is a normal extension (for instance, by taking $\mathbb{E}$ to be the normal closure of $\mathbb{K}/\mathbb{F}$).

2.5 Number Theory: The prime counting function

We close this section with a brief discussion of large prime power divisors of positive integers.

Definition 2.16. For a positive integer s and a prime p, write s_p for the p-part of n. Also, define $\operatorname{lpp} s = \max_{p \text{ prime}} s_p$ to be the the largest prime power divisor of s.

Fix $s \geq 2$, and let $k = \operatorname{lpp} s$. By writing the prime factorization of s as $s = kp_2^{r_2}\dots p_t^{r_t}$, one immediately sees that $s \leq k^{\delta(k)}$, where $\delta(k)$ denotes the number of primes less than or equal to k. Hence, $\log s \leq \delta(k)\log k$. Also, it is proved in [36, Corollary 1] that

$$\delta(k) < 1.25506k/\ln k$$

for $k \geq 2$. Define the constant c' by

$$c' := \ln 2/1.25506 \tag{2.4}$$

We deduce the following.

Lemma 2.17. *Let s be a positive integer. Then*

$$\operatorname{lpp} s \geq (\ln 2/1.25506) \log s = c' \log s.$$

3 Minimally transitive groups of degree $2^m 3$

We begin our work towards the proof of Theorem 5.3 with a discussion of minimally transitive permutation groups. As mentioned in Section 1, we use these groups to study minimal generator numbers in modules for permutation groups. Specifically, if $H \leq G$ are finite groups, V is a G-module, and $\widetilde{G}$ is a subgroup of G acting transitively on the set $H\backslash G$ of right cosets of H in G, then $V \uparrow_H^G \cong V \uparrow^{\widetilde{G}}_{\widetilde{G}\cap H}$, by Mackey's Theorem (see [16, Proposition 6.20]). Thus, when studying induced modules, one may often reduce to the case where G acts minimally transitively on $H\backslash G$.

Note also that the bounds we obtain in Theorem 4.24 and its corollaries are strong enough to prove Theorem 5.3 in most cases. Due to the nature of the bounds however, this is not the case when $|G : H|$ has the form $2^m 3$. Thus, we have to work harder, and try to obtain some information about the structure of the minimally transitive groups of degree $2^m 3$. Recall from Section 1 that our main result is as follows.

Theorem 1.8. *Let G be a minimally transitive permutation group of degree $n = 2^m 3$. Then one of the following holds:*

(i) G is soluble; or

(ii) G has a unique nonabelian chief factor, which is a direct product of copies of $L_2(p)$, where p is a Mersenne prime.

We begin preparations towards the proof of Theorem 1.8 with some easy observations on minimally transitive groups.

Lemma 3.1. *Let G be a transitive subgroup of S_n, let A be a point stabiliser in G, let $1 \neq L$ be a normal subgroup of G, and let $\Omega = \{\Delta_1, \ldots, \Delta_\chi\}$ be the set of L-orbits. Then*

(i) Either L is transitive, or Ω forms a system of blocks for G. In particular, the size of an L-orbit divides n.

(ii) (L, Δ_1) is permutation isomorphic to (L, Δ_j), for all j.

(iii) $|\Omega| = |G : AL|$.

(iv) G is minimally transitive if and only if the only subgroup $X \leq G$ satisfying $AX = G$ is $X = G$.

(v) If G is minimally transitive, then G^Ω is minimally transitively.

(vi) If $n = p^a$ for a prime p and G is minimally transitive, then G is a p-group.

Proof. Parts (i), (ii) and (iii) are clear. Also, a subgroup X of G is transitive if and only if $AX = G$. Hence, Part (iv) follows.

Part (v) is proved in [13, Theorem 2.4]. Finally, Part (vi) follows since a Sylow p-subgroup of a transitive group of degree p^a acts transitively. □

3.1 Subgroups of index 2^m3 in direct products of nonabelian simple groups

In [24, Corollary 6], information is given regarding the prime divisors of indices of subgroups of simple groups. We utilise this work in the following proposition.

Proposition 3.2. *Let T be a nonabelian finite simple group, and suppose that T has a proper subgroup X of index $n = 2^i3^j$, with $0 \leq j \leq 1$. Then one of the following holds:*

(i) $T = M_{12}$ and X is contained in one of the two T-conjugacy classes of copies of M_{11} in M_{12}.

(ii) $T = M_{11}$ or M_{24}, and X is T-conjugate to $L_2(11)$ or M_{23}, respectively.

(iii) $T = A_r$, $r = 2^i3^j$, and either X is T-conjugate to A_{r-1}, or $r = 6$ and X is T-conjugate to $L_2(5)$.

(iv) $T = L_2(p)$ where p is a prime of the form $p = 2^{f_1}3^{f_2} - 1$ with $f_2 \leq 1$, and X is a subgroup of index either 1 or 3 in a T-conjugate of the maximal subgroup $M = C_p \rtimes C_{(p-1)/2} < L_2(p)$.

Proof. For a finite set F, let $\pi(F)$ denote the set of prime divisors of $|F|$. Thus, we have $\pi(X) \subseteq \pi(T)$, since $X \leq T$. We wish to reduce to the case $\pi(X) = \pi(T)$ and then use [24, Corollary 6]. However, we first need to deal with some cases which are not covered by this approach. First, the classification of the maximal subgroups of the simple classical groups of dimension up to 12 implies that T is not $L_2(8)$, $L_3(3)$, $U_3(3)$, $\mathrm{Sp}_4(8)$, $U_4(2)$ or $U_5(2)$ (see [6, Tables 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.10, 8.11, 8.14, 8.20 and 8.21]).

Assume next that $T \cong L_2(p)$, for some prime p of the form $p = 2^{f_1}3^{f_2} - 1$, with $f_2 \geq 0$. Also, let M be a maximal subgroup of T containing X. Then, since $|T : M|$ divides $|T : X| = 2^i3^j$ with $j \leq 1$, we must have $M = C_p \rtimes C_{(p-1)/2}$, and $f_2 \leq 1$ (see [6, Table 8.1]). Set $l := 1$ if $f_2 = 0$, and $l := 3$ if $f_2 = 1$. Since $(p+1)/l$ is the highest power of 2 dividing $|T|$, and $|T : X| = 2^i3^j$ with $j \leq 1$, either $X = M$; or $f_2 = 0$ and $|M : X| = 3$. This is the situation described in (iv).

Next, assume that T is one of the Mathieu groups M_{11} or M_{12}. Using the $\mathbb{ATLAS}$ [11], we find that the only possibilities for X are $T = M_{11}$ and X is T-conjugate to $L_2(11) \leq M_{11}$ (of index 12); or $T = M_{12}$ and X is a member of one of the two T-conjugacy classes of $M_{11} \leq M_{12}$ (of index 12).

Finally, assume that T is not one of the groups considered above, and let Π be the set of primes for T given in the statement of [24, Corollary 6]. Then $\pi(|T : X|) \subseteq \{2, 3\}$, and $q \geq 5$ for each $q \in \Pi$ (the cases where Π contains 2 or 3 have been dealt with in the preceding paragraphs - see [24, Corollary 6]). Thus, we must have $\Pi \subseteq \pi(X)$. Hence [24, Corollary 6] gives $\pi(X) = \pi(T)$ and the possibilities for T and X are as follows (see [24, Table 10.7]).

(1) $T = A_r$, $A_k \trianglelefteq X \leq S_k \times S_{r-k}$, and k is greater than or equal to the largest prime p with $p \leq r$ (in particular, $k \geq 5$, since T is simple). Then $|A_r : A_r \cap (S_k \times S_{r-k})| = \binom{r}{k}$ divides $|T : X| = 2^i3^j$. But a well-known theorem of Sylvester and Schur (see [17]) states that either $\binom{r}{k} = 1$ or $\binom{r}{k}$ has a prime divisor exceeding $\min\{k, r-k\}$. Thus, since $k \geq 5$ we must have $k = r-2$ or $k = r-1$. Since $r \geq 5$, $k = r-1$ is the only option and hence $X = A_{r-1}$, which gives us what we need.

(2) $T = A_6$, $X = L_2(5)$. This, together with (1) above, gives precisely the situation described in (iii).

(3) $T = \mathrm{PSp}_{2m}(q)$ (m, q even) or $\mathrm{P}\,\Omega_{2m+1}(q)$ (m even, q odd), and $\Omega^-_{2m}(q) \trianglelefteq X$. Then $X \leq N_T(\Omega^-_{2m}(q))$, so $|T : N_T(\Omega^-_{2m}(q))|$ divides $|T : X| = 2^i3^j$. But

$|N_T(\Omega^-_{2m}(q)) : \Omega^-_{2m}(q)| = 2$, by [22, Proposition 4.8.6] for $T = \mathrm{PSp}_{2m}(q)$ and [22, Proposition 4.1.6] for $T = \mathrm{P}\,\Omega_{2m+1}(q)$. Hence, $|T : \Omega^-_{2m}(q)|$ divides $2^{i+1}3^j$. Also, for each of the two choices of T we get $|T : \Omega^-_{2m}(q)| = q^m(q^m - 1)$. But $q^m(q^m - 1)$ cannot be of the form 2^f or $2^f 3$, since $m > 1$ and $(m, q) \neq (2, 2)$ (as T is simple). Therefore, we have a contradiction.

(4) $T = \mathrm{P}\,\Omega^+_{2m}(q)$ (m even, q odd) and $\Omega_{2m-1}(q) \trianglelefteq X$. As above, $X \leq N_T(\Omega_{2m-1}(q))$, and we use [22, Proposition 4.1.6 Part (i)] to conclude that $|N_T(\Omega_{2m-1}(q)) : \Omega_{2m-1}(q)| = 2$. It follows that $\frac{1}{2}q^{m-1}(q^m - 1) = |T : \Omega_{2m-1}(q)|$ divides $2^{i+1}3^j$. This again gives a contradiction, since $m \geq 4$.

(5) $T = \mathrm{PSp}_4(q)$ and $\mathrm{PSp}_2(q^2) \trianglelefteq X$. Then $X \leq N_T(\mathrm{PSp}_2(q^2))$, and [22, Proposition 4.3.10] gives $|N_T(\mathrm{PSp}_2(q^2)) : \mathrm{PSp}_2(q^2)| = 2$. It follows that $q^2(q^2 - 1) = |T : \mathrm{PSp}_2(q^2)|$ divides $2^{i+1}3^j$. Again, this is impossible.

(6) In each of the remaining cases (see [22, Table 10.7]), we are given a pair (T, Y), where T is $L_2(8)$, $L_3(3)$, $L_6(2)$, $U_3(3)$, $U_3(5)$, $U_4(3)$, $U_6(2)$, $\mathrm{PSp}_4(7)$, $\mathrm{PSp}_4(8)$, $\mathrm{PSp}_6(2)$, $\mathrm{P}\,\Omega^+_8(2)$, $G_2(3)$, ${}^2F_4(2)'$, M_{24}, HS, McL, Co_2 or Co_3, and Y is a subgroup of T containing X. Apart from when $T = M_{24}$, we find that $|T : Y|$ does not divide $2^i 3^j$, so we get a contradiction in each case. When $T = M_{24}$, the only possibility is when X is T-conjugate to $M_{23} \leq M_{24}$ (of index 24).

This completes the proof. □

Our main tool in proving Theorem 1.8 is the Frattini argument. The result is well-known, but we couldn't find a reference so we include a proof here.

Lemma 3.3. *Let G be a group, and let L be a normal subgroup of G. Suppose that H is a subgroup of L with the property that H and H^α are L-conjugate for each $\alpha \in \mathrm{Aut}(L)$. Then $G = N_G(H)L$.*

Proof. Let $g \in G$. Then conjugation by g induces an automorphism of L, so $H^g = H^l$ for some $l \in L$, by hypothesis. Hence, $gl^{-1} \in N_G(H)$, so $g \in N_G(H)L$, and this completes the proof. □

With the Frattini argument in mind, the next corollary will be crucial.

Lemma 3.4. *Let T be a nonabelian finite simple group, and suppose that T has a proper subgroup X of index $r := 2^i 3^j$, with $0 \leq j \leq 1$. Assume also that if $T \cong L_2(p)$, with p a Mersenne prime, then $j = 0$. Denote by Γ the set of right cosets of X in T. Then there exists a proper subgroup H of T with the following properties:*

(i) H and H^α are conjugate in T for each automorphism $\alpha \in \mathrm{Aut}(T)$; and

(ii) $N_T(H)^\Gamma$ is transitive.

Proof. By Proposition 3.2, the possibilities for the pair (T, X) (up to conjugation in T) are as follows:

1. $(T, X) = (A_r, A_{r-1})$, with $r = 2^i 3^j$ for some $j \leq 1$, or $(T, X) = (A_6, L_2(5))$. Since T is nonabelian simple, $r \geq 6$, so r is even. If r is a power of 2, let H be a Sylow 2-subgroup of T. Then H^Γ itself is transitive, and properties (i) and (ii) are clearly satisfied.

   Otherwise, let $H = \langle (1, 2, 3), (4, 5, 6), \ldots, (r - 1, r - 2, r) \rangle$. Then $N_T(H)^\Gamma$ is transitive. Thus, (ii) is satisfied. Property (i) is also easily seen to be satisfied (this includes the case $r = 6$, when $\mathrm{Out}\,(A_6)$ has order 4).

2. $(T, X) = (M_{11}, L_2(11))$: Let H be a Sylow 3-subgroup of T. Then $N_T(H) \cong M_9 : 2$ (see page 18 of the $\mathbb{ATLAS}$ of finite groups [11]) acts transitively on the cosets of X. Since $\mathrm{Aut}(M_{11}) = \mathrm{Inn}(M_{11})$, (i) and (ii) are satisfied.

3. $T = M_{12}$ and X is T-conjugate to one of the two copies of M_{11} in M_{12}; or $T = M_{24}$ and X is T-conjugate M_{23}: In each case, let H be a subgroup of T generated by a fixed point free element of order 3. When $T = M_{12}$, $N_T(H) \cong A_4 \times S_3$ (see [11, page 18]) is a maximal subgroup of T, and acts transitively on the cosets of X (for each copy of M_{11}). Also, the unique non-identity outer automorphism of M_{12} fixes the set of T-conjugates of H, so both (i) and (ii) are satisfied.

   When $T = M_{24}$, $N_T(H)$ has order 1008, and acts transitively on the cosets of X (using MAGMA [5], for example). Also, $\mathrm{Out}\,(T)$ is trivial. Thus, (i) and (ii) are again satisfied.

4. $T = L_2(p)$, with $p = 2^{f_1}3^{f_2} - 1 \geq 7$, $f_2 \leq 1$ and $X = C_p \rtimes C_{(p-1)/2}$. Then $|T : X| = p+1 = 2^{f_1}3^{f_2}$. Assume first that $p \geq 7$, and let H be a dihedral group of order $p+1$ contained in T. Since T has a unique conjugacy class of maximal subgroups of dihedral groups of order $p+1$, (i) follows. Furthermore, $|T : H|$ and $|T : X|$ are coprime, so (ii) is also satisfied.

   This just leaves the case $p = 5$, but in this case $T = A_5$ and X is T-conjugate to D_{10} so taking $H = A_4$ gives us what we need.

□

Lemma 3.5. *Let $p \geq 7$ be a Mersenne prime, and let $L = T_1 \times T_2 \times \ldots \times T_e$, where each $T_i \cong L_2(p)$. Also, let A be a subgroup of L such that $|L : A| = 2^a 3$, for some a, and $|T_i : T_i \cap A| \in \{p+1, 3(p+1)\}$ for all i, with $|T_i : T_i \cap A| = 3(p+1)$ for at least one i. Then*

(i) $|L : A| = 3(p+1)^e$.

(ii) Let P be a Sylow p-subgroup of L. Then $N_L(P)$ is soluble, and has precisely 2^e orbits on the set Δ of (right) cosets of A in L, with $\binom{e}{k}$ orbits of size $3p^k$, for each k, $0 \leq k \leq e$.

Proof. We first prove Part (i) by induction on e, with the case $e = 1$ being trivial. So assume that $e > 1$, and fix k in the range $1 \leq k \leq e$ with $|T_k : T_k \cap A| = 3(p+1)$. Also, fix $i \neq k$, and set $\hat{T}_i := T_1 \times \ldots \times T_{i-1} \times T_{i+1} \times \ldots \times T_e$ and $\hat{A}_i = A \cap \hat{T}_i$. Then

$$|T_j : T_j \cap \hat{A}_i| = |T_j : T_j \cap \hat{T}_i \cap A| = |T_j : T_j \cap A| \in \{3(p+1), p+1\}$$

for each $j \neq i$. In particular, $|T_k : T_k \cap \hat{A}_i| = 3(p+1)$. Also, $|\hat{T}_i : \hat{A}_i| = |\hat{T}_i A : A|$ divides $|L : A|$, and is divisible by $|T_k : T_k \cap \hat{A}_i| = |T_k \hat{A}_i : \hat{A}_i| = 3(p+1)$, so $|\hat{T}_i : \hat{A}_i| = 2^{b_i}3$, for some $b_i \leq a$. Hence, the inductive hypothesis implies that $|\hat{T}_i : \hat{A}_i| = 3(p+1)^{e-1}$.

Assume that the claim in Part (i) does not hold. Then since $(p+1)^e$ is the highest power of 2 dividing $|L|$, we must have $|L : \hat{T}_i A| = |L : A|/|\hat{T}_i : \hat{A}_i| < p+1$. Hence, if $\rho_i : L \to T_i$ denotes projection onto T_i, then $|T_i : \rho_i(A)| = |\rho_i(L) : \rho_i(\hat{T}_i A)| = |L : \hat{T}_i A| < p+1$. But, as can be readily checked using [6, Tables 8.1 and 8.2], no maximal subgroup of $L_2(p)$ can have index a power of 2 and strictly less than $p+1$. Thus, we must have $\hat{T}_i A = L$, so A projects onto T_i. But then $A \cap T_i$ is a

normal subgroup of T_i, so $A \cap T_i = 1$ or T_i. This contradicts $|T_i : A \cap T_i| \in \{p+1, 3(p+1)\}$, and Part (i) follows.

Finally, we prove (ii). Let $N := N_L(P)$. By Proposition 3.2 Part (iii), each $T_j \cap A$ is contained in a maximal subgroup $M_j := C_p \rtimes C_{(p-1)/2}$ of T_j, and $|T_j : T_j \cap A| \in \{p+1, 3(p+1)\}$. Thus, $T_j \cap A$ has a normal Sylow p-subgroup $P_j \cong C_p$. Let $\widetilde{P} := P_1 \times \ldots \times P_e$, so that $\widetilde{P}$ is a Sylow p-subgroup of L. Since P and $\widetilde{P}$ are conjugate in L, we may assume, for the purposes of proving Part (ii), that $\widetilde{P} = P$. Since $M_j = N_{T_j}(P_j)$ is soluble, $N = M_1 \times \ldots \times M_e$ is soluble. Also, $P \trianglelefteq A$ since P is a characteristic subgroup of $(T_1 \cap A) \times \ldots \times (T_e \cap A) \trianglelefteq A$, so $A \leq N$.

Suppose first that $e = 1$. Then $|L : A| = 3(p+1)$, so A has index 3 in N, since $|L : N| = |L : M_1| = p + 1$. Let $x \in L \backslash N$, and let $\Gamma \subset \Delta$ be the N-orbit corresponding to Ax. Then $|\Gamma| = |N : N \cap A^x| = \frac{|L:N \cap A^x|}{|L:N|}$. Since $|L : N| = p + 1$ is a power of 2 and $|L : N \cap A^x|$ is divisible by $|L : A^x| = 3(p+1)$, it follows that 3 divides $|\Gamma|$. Also, as mentioned above, A^x and N have unique Sylow p-subgroups P^x and P, respectively. Since x does not normalise P, we have $P^x \neq P$, so p, and hence $3p$, divides $|N : N \cap A^x| = |\Gamma|$. Since $|N : A| = 3$ and $|L : A| = 3(p+1)$, it follows that $|\Gamma| = 3p$, which proves the claim in the case $e = 1$.

We now consider the general case. Fix $1 \leq i \leq e$, and $x_i \in T_i \backslash M_i$. Suppose first that $|T_i : T_i \cap A| = 3(p+1)$. From the previous paragraph, we see that M_i has precisely two orbits on the cosets of $T_i \cap A$ in T_i, of size 3 and $3p$, represented by A and Ax_i respectively. Next, assume that $|T_i : T_i \cap A| = p+1$. Then $M_i = T_i \cap A$. Moreover, arguing as in the previous paragraph, p divides $|M_i : M_i \cap A^{x_i}|$, from which it follows that M_i again has two orbits on the cosets of $A \cap T_i$ in T_i, of size 1 and p, represented by A and Ax_i respectively.

Let $B := (T_1 \cap A) \times \ldots \times (T_e \cap A) \trianglelefteq A$. It is clear, from the previous paragraph, that $N = M_1 \times \ldots \times M_e$ has 2^e orbits on the cosets of B in L, represented by $Bt_1t_2 \ldots t_e$, where $t_i \in \{1, x_i\}$, for $1 \leq i \leq e$. Also, the orbit represented by the coset $Bt_1t_2 \ldots t_e$ has cardinality $3^d p^k$, where k is the number of subscripts i with $t_i \neq 1$, and d is the number of subscripts i with

$$|T_i : T_i \cap A| = 3(p+1). \tag{3.1}$$

Since $B \leq A$, N has at most 2^e orbits in Δ. Suppose there exist t_i, $\widetilde{t_i} \in \{1, x_i\}$ for $1 \leq i \leq e$, and $n = n_1n_2 \ldots n_e \in N$ (with $n_i \in M_i$), such that $At_1t_2 \ldots t_e = A(\widetilde{t_1}\widetilde{t_2} \ldots \widetilde{t_e})(n_1n_2 \ldots n_e)$. Then $t_i = a_i\widetilde{t_i}n_i$, where $a_1a_2 \ldots a_e \in A$. Since $A \leq N$, it follows that $t_i = 1$ if and only if $\widetilde{t_i} = 1$. Hence, $t_1t_2 \ldots t_e = \widetilde{t_1}\widetilde{t_2} \ldots \widetilde{t_e}$. Thus, N has precisely 2^e orbits in Δ, represented by $At_1 \ldots t_e$, where $t_i \in \{1, x_i\}$. Since the size of the N-orbit corresponding to $At_1t_2 \ldots t_e$ is

$$|N : N \cap A^{t_1t_2 \ldots t_e}| = \frac{|N : N \cap B^{t_1t_2 \ldots t_e}|}{|N \cap A^{t_1t_2 \ldots t_e} : N \cap B^{t_1t_2 \ldots t_e}|} \geq \frac{|N : N \cap B^{t_1t_2 \ldots t_e}|}{|A^{t_1t_2 \ldots t_e} : B^{t_1t_2 \ldots t_e}|},$$

and $|A^{t_1t_2 \ldots t_e} : B^{t_1t_2 \ldots t_e}| = |A : B| = |N : B|/|N : A| = 3^{d-1}$, it now follows from (4.2.1) that

$$|N : N \cap A^{t_1t_2 \ldots t_e}| = \frac{|N : N \cap B^{t_1t_2 \ldots t_e}|}{3^{d-1}} = 3p^k$$

where k is the number of subscripts i such that $t_i \neq 1$. This proves (ii). □

3.2 The proof of Theorem 1.8

First, we fix some notation which will be retained for the remainder of this section: Let G be a minimally transitive permutation group of degree 2^m3; let A be the stabiliser in G of a point δ; let L be a minimal normal subgroup of G; let Ω be the set of L-orbits; let $K := \mathrm{Ker}(G^\Omega)$ be the kernel of the action of G on Ω; and finally, let Δ be the L-orbit containing δ.

Remark 3.6. G^Ω acts minimally transitively on Ω, by Lemma 3.1 Part (v). Note also that, if $|G : AL|$ is a power of 2, then G^Ω is a 2-group by Lemma 3.1 Part (vi).

We require the following easy proposition.

Proposition 3.7. *There exists a subgroup E of G such that $G = EL$ and $E \cap K$ is soluble.*

Proof. Consider the (set-wise) stabiliser $\mathrm{Stab}_G(\Delta)$ of Δ in G. Since L acts transitively on Δ, we have $LA = \mathrm{Stab}_G(\Delta)$. Let E be a subgroup of G minimal with the property that $EK = G$. Then $E \cap K$ is contained in the Frattini subgroup of E, and hence is soluble. Finally, $G = EK \leq E\,\mathrm{Stab}_G(\Delta) = ELA$, so $G = ELA$. Thus, $EL = G$ by minimal transitivity, as needed. □

Corollary 3.8. *If L is abelian, then the set of nonabelian chief factors of G equals the set of nonabelian chief factors of G^Ω. If L is nonabelian and $|\Omega| = |G : LA|$ is a power of 2, then L is the unique nonabelian chief factor of G.*

Proof. Let E be as in Proposition 3.7, and assume that either L is abelian or L is nonabelian and $|\Omega| = |G : LA|$ is a power of 2. For a finite group X write $\mathrm{NCF}(X)$ for the set of nonabelian chief factors of X. We need to prove that $\mathrm{NCF}(G) = \mathrm{NCF}(G^\Omega)$ if L is abelian, and $\mathrm{NCF}(G) = \{L\}$ otherwise. Note that if $|\Omega|$ is a power of 2 then G^Ω is soluble, by Remark 3.6.

Since E^Ω is transitive, the minimal transitivity of G^Ω implies that $G^\Omega = E^\Omega \cong E/E \cap K$. Since $E \cap K$ is soluble, it follows that $\mathrm{NCF}(G^\Omega) = \mathrm{NCF}(E)$. By hypothesis, either L is abelian, or L is nonabelian and E^Ω, and hence E, is soluble. Since $G = EL$, the claim follows, in either case. □

Proposition 3.9. *Suppose that $L = T_1 \times \ldots \times T_f$, where each T_i is isomorphic to a nonabelian simple group T. Without loss of generality, assume that $\mathrm{Ker}_L(\Delta) = T_{e+1} \times \ldots \times T_f$, so that $L^\Delta = T_1^\Delta \times \ldots \times T_e^\Delta$. Then*

(i) $T \cong L_2(p)$ for some Mersenne prime p,

(ii) $|T_i : T_i \cap A| \in \{p+1, 3(p+1)\}$ for each $1 \leq i \leq e$, and;

(iii) There exists at least one i in the range $1 \leq i \leq e$ such that $|T_i : T_i \cap A| = 3(p+1)$.

Proof. Suppose that the proposition is false, and set $X_i := T_i \cap A$. Note that $|T_i : X_i|$ divides 2^m3 for each i, by Lemma 3.1 Part (i). Hence, Proposition 3.2 implies that one of the following must hold:

(a) $T \ncong L_2(p)$, for any Mersenne prime p. Then by Proposition 3.2, either $T_i \cong M_{12}$ and each X_i is contained in one of the two conjugacy classes of M_{11} in M_{12}; or $(T_i, X_i) = (A_r, A_{r-1})$, $(A_6, L_2(5))$, $(M_{11}, L_2(11))$, (M_{24}, M_{23}), or $(L_2(p), C_p \rtimes C_{\frac{p-1}{2}})$ where p is a prime of the form $p = 2^{f_1}3 - 1$. Here, the group X_i is given up to conjugacy in T_i.

(b) $T \cong L_2(p)$ for some Mersenne prime p. In this case, Proposition 3.2 implies that $|T_i : X_i| = p+1$ for all i. In particular, X_i is T_i-conjugate to the maximal subgroup $M_i := C_p \rtimes C_{\frac{p-1}{2}}$ of T_i. (We remark that it is here where we use the assumption that the proposition is false. Specifically, since $|T_i : X_i|$ divides $2^m 3$ for each i, Proposition 3.2 implies that X_i is T_i-conjugate to either M_i, or an index 3 subgroup of M_i. Hence $|T_i : X_i| \in \{p+1, 3(p+1)\}$ for each i. Thus, Part (iii) of the proposition must fail, forcing $|T_i : X_i|$ to be $p+1$, and hence for X_i to be T_i-conjugate to M_i, for each i.)

Fix $1 \leq i \leq e$, and write $T = T_i$. Note that T^Δ is isomorphic to T. Set $\Gamma := \delta^T \subset \Delta$, and set $X := T \cap A$. Then the pair (T, X) satisfies the hypothesis of Lemma 3.4. Thus, we conclude that T contains a proper subgroup H such that

(i) H and H^α are conjugate in T for each automorphism $\alpha \in \mathrm{Aut}(T)$; and

(ii) $N_T(H)^\Gamma$ is transitive.

Fix a T-orbit Γ' in Δ. We claim that $N_T(H)^{\Gamma'}$ is transitive. By Lemma 3.1 Part (ii), $T^{\Gamma'}$ is permutation isomorphic to T^Γ. Hence, by (ii) above, there exists an automorphism α of T such that $N_T(H)^\alpha = N_T(H^\alpha)$ acts transitively on Γ'. Since H is T-conjugate to H^α, it follows that $N_T(H)$ is T-conjugate to $N_T(H)^\alpha$. Thus, $N_T(H)$ acts transitively on Γ', as claimed.

Since $T_i \cong T_j$ for all i, j, we can choose the subgroup $H_j < T_j$ corresponding to H, and the subgroup $N_j < T_j$ corresponding to $N_T(H)$, for each $1 \leq j \leq f$. Furthermore, each group X_i is determined up to conjugacy in T_i by (a) and (b) above. Hence, by the previous paragraph

$$N_j \text{ acts transitively on each } T_j\text{-orbit in } \Delta \text{ whenever } 1 \leq j \leq e. \tag{3.2}$$

Set $\widetilde{H} = H_1 \times H_2 \times \ldots \times H_f < L$, and $N := N_1 \times N_2 \times \ldots \times N_f$. Now, note that $N \leq N_L(\widetilde{H})$. Thus, $N_1^\Delta \times N_2^\Delta \times \ldots \times N_e^\Delta = N^\Delta \leq N_L(\widetilde{H})^\Delta$.

We will now prove that N^Δ is transitive. Indeed, let $\epsilon \in \Delta$, and let $x \in L$ such that $\delta^x = \epsilon$. Write $x = t_1 t_2 \ldots t_e$, with $t_j \in T_j$. By (ii) above, N_1 acts transitively on δ^{T_1}. Hence, there exists $n_1 \in N_1$ such that $\delta^{t_1} = \delta^{n_1}$. We now inductively define the permutations n_2, …, n_e by choosing $n_j \in N_j$ such that $(\delta^{n_1 \cdots n_{j-1}})^{n_j} = \delta^{n_1 \cdots n_{j-1} t_j}$ (this is possible since N_j acts transitively on $(\delta^{n_1 \ldots n_{j-1}})^{T_j}$, by (4.3.1)). Then

$$\begin{aligned}\epsilon = \delta^{t_1 t_2 \cdots t_e} = (\delta^{t_1})^{t_2 \cdots t_e} = \delta^{n_1 t_2 \cdots t_e} = (\delta^{n_1 t_2})^{t_3 \cdots t_e} \\ = \delta^{n_1 n_2 t_3 \cdots t_e} = (\delta^{n_1 n_2 t_3})^{t_4 \cdots t_e} = \cdots = \delta^{n_1 n_2 \cdots n_e}\end{aligned}$$

Thus

$$N^\Delta \text{ is transitive, as claimed.} \tag{3.3}$$

Finally, let $\alpha \in \mathrm{Aut}\,(L) \cong \mathrm{Aut}\,(T) \wr \mathrm{Sym}(f)$. Then there exists $\tau \in \mathrm{Sym}\,(f)$ and $\alpha_i \in \mathrm{Aut}\,(T)$ such

that

$$\begin{aligned}\widetilde{H}^{\alpha} &= H_{1^\tau}^{\alpha_1} \times H_{2^\tau}^{\alpha_2} \times \ldots \times H_{f^\tau}^{\alpha_f} \\ &= H_1^{\alpha_{1\tau^{-1}}} \times H_2^{\alpha_{2\tau^{-1}}} \times \ldots \times H_f^{\alpha_{f\tau^{-1}}}\end{aligned}$$

By (i) above, there exists, for each $1 \leq i \leq f$, an element $t_i \in T_i$ such that $H_i^{\alpha_{i\tau^{-1}}} = H_i^{t_i}$. Hence

$$\widetilde{H}^{\alpha} = H_1^{t_1} \times H_2^{t_2} \times \ldots \times H_f^{t_f} = \widetilde{H}^{t_1 t_2 \ldots t_f}.$$

Thus, $\widetilde{H}$ and $\widetilde{H}^{\alpha}$ are conjugate in L for all $\alpha \in \mathrm{Aut}\,(L)$. Lemma 3.3 then implies that $G = N_G(\widetilde{H})L$. Thus, $N_G(\widetilde{H})$ acts transitively on the set Ω of L-orbits. But $N_G(\widetilde{H})$ also acts transitively on the fixed L-orbit Δ, by (4.3.2). Hence, $N_G(\widetilde{H})$ is a transitive subgroup of G. By minimal transitivity of G, it follows that $N_G(\widetilde{H}) = G$, so $\widetilde{H}$ is normal in G. But this is a contradiction, since $1 < \widetilde{H} < L$ and L is a minimal normal subgroup of G. The proof is complete. □

Property (iii) of Proposition 3.9 immediately implies the following.

Corollary 3.10. *Suppose that L is isomorphic to a direct product of copies of $L_2(p)$, where p is a Mersenne prime. Then $|\Delta|$ is divisible by* 3.

Finally, we are ready to prove Theorem 1.8.

Proof of Theorem 1.8. Assume that G is a counterexample to the theorem of minimal degree. Note that $|\Omega| = |G : LA|$ divides $|G : A| = 2^m 3$, and is less than $2^m 3$. Furthermore, a minimally transitive group of 2-power degree is soluble by Remark 3.6. Hence, the minimality of G as a counterexample implies that $G^{\Omega} = G/K$ satisfies either (i) or (ii) in the statement of the theorem.

If L is abelian, then Corollary 3.8 implies that the set of nonabelian chief factors of G equals the set of nonabelian chief factors of G^{Ω}. Thus, the result follow from the inductive hypothesis in this case. So we may assume that $L = T_1 \times T_2 \times \ldots \times T_f$, where each T_i is isomorphic to a nonabelian finite simple group T. Furthermore, Proposition 3.9 then implies that $T \cong L_2(p)$, where p is a Mersenne prime. Also, 3 divides $|\Delta|$ by Corollary 3.10. But then $|\Omega| = |G : LA|$ is a power of 2, so L is the unique nonabelian chief factor of G by Corollary 3.8. This contradiction completes the proof. □

We also deduce two corollaries which will be vital in our application of Theorem 4.24 (see Section 4.3.2).

Corollary 3.11. *Assume that G is insoluble, and let $p := 2^a - 1$ be a Mersenne prime such that G has a unique nonabelian chief factor isomorphic to a direct product of f copies of $L_2(p)$. Then there exists a triple of integers (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that*

(i) $m = ea + t$, and;

(ii) For some soluble subgroup N of G, N has 2^{e+t_1} orbits, with $\binom{e}{k}2^{t_1}$ of them of length $3p^k \times 2^{t-t_1}$, for each k, $0 \leq k \leq e$.

Proof. Let E be as in Proposition 3.7, so that $G = EL$, and $E \cap K$ is soluble. We prove the claim by induction on m. Suppose first that L is abelian. Then since $EL = G$ and $E \cap K$ is soluble, $G^\Omega = E^\Omega$ is insoluble. Hence $|\Omega| = 2^{\widetilde{m}}3$ and $|\Delta| = 2^{m-\widetilde{m}}$, for some $\widetilde{m}$ with $1 \leq \widetilde{m} < m$, by Lemma 3.1 Parts (i) and (vi). The inductive hypothesis then implies that there exists a triple $(\widetilde{e}, \widetilde{t_1}, \widetilde{t})$ such that

1. $\widetilde{m} = \widetilde{e}a + \widetilde{t}$, and;
2. For some soluble subgroup $\widetilde{N}$ of E^Ω, $\widetilde{N}$ has $2^{\widetilde{e}+\widetilde{t_1}}$ orbits, with $\binom{\widetilde{e}}{k}2^{\widetilde{t_1}}$ of them of length $3p^k \times 2^{\widetilde{t}-\widetilde{t_1}}$, for each k, $0 \leq k \leq \widetilde{e}$.

Set $e := \widetilde{e}$, $t := m - \widetilde{m} + \widetilde{t}$, and $t_1 := \widetilde{t_1}$, so that $m = ea + t$, which is what we need for (i). Also, let $Y \leq E$ such that $Y^\Omega = \widetilde{N}$, and set $N := LY$. Then N is soluble, since the groups Y^Ω, $Y \cap K$ and L are soluble. Moreover, N acts transitively on each L-orbit, since $L \leq N$. Since each L-orbit has size $2^{m-\widetilde{m}}$, it follows that N has 2^{e+t_1} orbits, with $\binom{e}{k} \times 2^{t_1}$ of them of length $3p^k 2^{\widetilde{t}-\widetilde{t_1}+m-\widetilde{m}} = 3p^k 2^{t-t_1}$. This gives us what we need.

So assume that $L = T_1 \times T_2 \times \ldots \times T_f$, where each $T_i \cong L_2(p)$. By Proposition 3.2 Part (iii), $T_i \cap A$ is contained in the maximal subgroup $M_i \cong C_p \rtimes C_{(p-1)/2}$ of T_i, and $|T_i : T_i \cap A| \in \{p+1, 3(p+1)\}$ for all i. Furthermore, Proposition 3.9 implies that there exists at least one subscript i such that $|T_i : T_i \cap A| = 3(p+1)$. Lemma 3.5 now implies that $|\Delta| = |L : L \cap A| = 3(p+1)^e = 2^{ea}3$, where e is the number of direct factors of L acting non-trivially on Δ. It also follows that $|\Omega| = 2^{m-ea}$.

By relabeling the T_i if necessary, we may write $L^\Delta = T_1^\Delta \times T_2^\Delta \times \ldots \times T_e^\Delta$. Let P be a Sylow p-subgroup of L, and let $N := N_L(P)$. By Lemma 3.5 Part (ii), N is soluble, and $N_L(P)^\Delta = N_{L^\Delta}(P^\Delta)$ has 2^e orbits on Δ, with $\binom{e}{k}$ of size $3p^k$, for each $0 \leq k \leq e$. Since the action of L on each L-orbit is permutation isomorphic to the action of L on Δ, it follows that $N := N_L(P)$ has 2^e orbits on each L-orbit, with $\binom{e}{k}$ of size $3p^k$, for each $0 \leq k \leq e$. Also, N acts trivially on the set Ω of L-orbits, so N has 2^{e+m-ea} orbits in total, with $2^{m-ea}\binom{e}{k}$ of them of size $3p^k$, for each $0 \leq k \leq e$. Setting $t := m - ea$ and $t_1 := t$ now gives us what we need, and completes the proof. □

Corollary 3.12. *Let S be a transitive permutation group of degree $s := 2^m 3$, and assume that S contains no soluble transitive subgroups. Then there exists a Mersenne prime $p := 2^a - 1$ and a triple of integers (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that*

(i) $m = ea + t$, and;

(ii) For some soluble subgroup N of S, N has 2^{e+t_1} orbits, with $\binom{e}{k}2^{t_1}$ of them of length $3p^k \times 2^{t-t_1}$, for each k, $0 \leq k \leq e$.

Proof. Let G be a minimally transitive subgroup of S. Then G is insoluble, so Corollary 3.11 applies, and the result follows. □

4 Generating submodules of induced modules for finite groups

The purpose of this paper is to study upper bounds for the function d on the class of finite transitive permutation groups. As can be seen from Section 1, this essentially amounts to deriving upper bounds on $d(G)$ for subgroups G of wreath products $R \wr S$. Our main strategy for doing this will be to reduce

modulo the base group B of $R \wr S$ and use induction to bound $d(G/G \cap B)$. In this way, all that remains is to investigate the contribution of $G \cap B$ to $d(G)$: The purpose of this section is to carry out such an investigation.

As we will show in Lemma 5.8, the group $G \cap B$ is built, as a normal subgroup of G, from submodules of induced modules for G, and nonabelian chief factors of G. Thus, the main aim of the section will be to derive upper bounds for generator numbers in submodules of induced modules. The strategy to do this will be to first view soluble groups as certain partially ordered sets: We prove some properties of these partially ordered sets in Section 4.1. Our main results are Theorem 4.13 and Theorem 4.24, which are proved in Sections 4.3.1 and 4.3.2 respectively. We remark that Theorem 4.13 improves [7, Theorem 1.5], while Theorem 4.24 improves [28, Lemma 4].

4.1 Partially ordered sets

Let $P = (P, \preccurlyeq)$ be a finite partially ordered set, and let $w(P)$ denote the *width* of P. That is, $w(P)$ is the maximum cardinality of an antichain in P. Suppose now that, with respect to $\preccurlyeq$, P is a cartesian product of chains, and write $P = P_1 \times P_2 \times \ldots \times P_t$, where each P_i is a chain of cardinality k_i. Then P is poset-isomorphic to the set of divisors of the positive integer $m = p_1^{k_1-1} p_2^{k_2-1} \ldots p_t^{k_t-1}$, where p_1, p_2, …, p_t are distinct primes. We make this identification without further comment.

Next, recall that each divisor d of m can be written uniquely in the form $d = p_1^{r_1} p_2^{r_2} \ldots p_t^{r_t}$, where $0 \leq r_i \leq k_i - 1$, for each i, $1 \leq i \leq t$. In this case, the *rank* of d is defined as $r(d) = \sum_{i=1}^{t} r_i$. For $0 \leq k \leq K := \sum_{i=1}^{t}(k_i - 1)$, let R_k denote the set of elements of P of rank k; clearly R_k is an antichain in P. In fact, it is proved in [14] that $w(P) = \max |R_k|$. This maximal rank set occurs at $k = \lfloor K/2 \rfloor$, and hence, by [2, Theorem 2], we have

$$w(P) \leq \left\lfloor \frac{s}{2^K} \binom{K}{\lfloor K/2 \rfloor} \right\rfloor$$

where $s := |P| = \prod_{i=1}^{t} k_i$ (note that equality holds when t is even and each k_i is 2, so this upper bound is best possible). Stated more concisely, we have

Lemma 4.1. *Suppose that a partially ordered set P, of cardinality $s \geq 2$, is a cartesian product of the chains P_1, P_2, …, P_t, where each P_i has cardinality k_i. Then*

$$w(P) \leq \left\lfloor \frac{s}{2^K} \binom{K}{\lfloor K/2 \rfloor} \right\rfloor,$$

where $K := \sum_{i=1}^{t}(k_i - 1)$.

We now define a constant b,

$$b := \sqrt{\frac{2}{\pi}}.$$

Proposition 4.2. *Let K be a positive integer. Then*

$$\binom{K}{\lfloor K/2 \rfloor} \leq \frac{b 2^K}{\sqrt{K}}. \tag{4.1}$$

Proof. [1] First consider the case where $K = 2t$ ($t \in \mathbb{N}$), and note that

$$2t\left[\binom{2t}{t}\frac{1}{4^t}\right]^2 = \frac{1}{2}\left(\frac{3}{2}\frac{3}{4}\right)\left(\frac{5}{4}\frac{5}{6}\right)\cdots\left(\frac{2t-1}{2t-2}\frac{2t-1}{2t}\right) = \frac{1}{2}\prod_{j=2}^{t}\left(1+\frac{1}{4j(j-1)}\right)$$

By Wallis' Formula, the expression in the middle converges to $2/\pi$. Hence, since the expression on the right is increasing, we have $2t\left[\binom{2t}{t}\frac{1}{4^t}\right]^2 \leq 2/\pi$, that is, $\binom{2t}{t} \leq b4^t/\sqrt{2t}$, as claimed. If K is odd, we have $\binom{K}{\lfloor K/2\rfloor} = \frac{1}{2}\binom{K+1}{\lfloor (K+1)/2\rfloor}$, and the bound in (4.2) follows from the even case above. □

Proof of Theorem 1.3. By Lemma 4.1 and Proposition 4.2, we have

$$w(P) \leq \frac{s}{2^K}\binom{K}{\lfloor K/2\rfloor} \leq \frac{s}{2^K}\left(\frac{b2^K}{\sqrt{K}}\right) = \frac{bs}{\sqrt{K}}$$

If each $k_i = p$, then $K = t(p-1)$, and the second part of the claim follows. Since $K = \sum_{i=1}^{t}(k_i - 1) \geq \sum_{i=1}^{t}\log k_i = \log s$, the first part also follows, and the proof is complete. □

4.2 Preliminary results on induced modules for finite groups

4.2.1 Composition factors in induced modules

Let $\mathbb{F}$ be a field, let G be a finite group, and let V be a module for G over $\mathbb{F}$. Let

$$0 = N_0 < N_1 < \ldots < N_a = V$$

be a G-composition series for V, and say that a factor N_i/N_{i-1} is *complemented* if there exists a submodule S_i of V containing N_{i-1} such that $V/N_{i-1} = N_i/N_{i-1} \oplus S_i/N_{i-1}$. Also, for an irreducible $\mathbb{F}[G]$-module W, write $t_W(V)$ for the number of complemented composition factors of V isomorphic to W.

Now, fix an irreducible $\mathbb{F}[G]$-module W with $t_W(V) \geq 1$. Then there exists a submodule M of V with the property that V/M is G-isomorphic to W: Define $R_W(V)$ to be the intersection of all such M. In particular, $R_W(V)$ contains the radical $\mathrm{Rad}(V)$ of V.

Lemma 4.3. $V/R_W(V) \cong W^{\oplus t_W(V)}$.

Proof. Let $t := t_W(V)$, and write $R := R_W(V) = M_1 \cap M_2 \cap \ldots \cap M_e$, where V/M_i is isomorphic to W. Then

$$V/R \leq (V/M_1) \oplus (V/M_2) \oplus \ldots \oplus (V/M_e)$$

and hence V/R is a direct sum of k copies of W, where $k \leq e$. Since $t_W(V) = t_W(V/R)$, we have $t = k$, and this completes the proof. □

Lemma 4.4. *Suppose that $V = U\uparrow_H^G$, for a subgroup H of G and an H-module U, and suppose that W is a 1-dimensional $\mathbb{F}[G]$-module. Then $t_W(V) \leq \dim U$.*

[1] The idea for this bound arose from a discussion at the url
http://math.stackexchange.com/questions/58560/elementary-central-binomial-coefficient-estimates.

Proof. Let $R = R_W(V)$ and $t = t_W(V)$. Writing bars to denote reduction modulo R, we have

$$\overline{V} = \overline{N_1} \oplus \overline{N_2} \oplus \ldots \oplus \overline{N_t}$$

where each $\overline{N_i}$ is isomorphic to W. In particular, if we write

$$V/\operatorname{Rad}(V) = \sum_{X \text{ an irreducible } \mathbb{F}[G]\text{-module}} X^{f_X(V)},$$

then we have $t \leq f_W(V)$. Moreover, since $\dim W = 1$, we have

$$f_W(V) = \dim \operatorname{Hom}_{\mathbb{F}[G]}(V, W) = \dim \operatorname{Hom}_{\mathbb{F}[H]}(U, W\downarrow_H) = f_{W\downarrow_H}(U) \leq \dim U$$

where the second equality above follows from Frobenius Reciprosity (see [4, Proposition 3.3.1]). This completes the proof. □

We will need an easy consequence of Lemma 4.4. To state it, we first require two definitions and a remark.

Definition 4.5. Let G be a non-trivial finite group, and $\mathbb{F}$ a field. A *projective representation* of G of dimension m over $\mathbb{F}$ is a homomorphism $\rho : G \to PGL_m(\mathbb{F})$. Define

$$R_{\mathbb{F}}(G) := \min\{m : G \text{ has a non-trivial representation of dimension } m \text{ over } \mathbb{F}\}; \text{ and}$$
$$\overline{R}_{\mathbb{F}}(G) := \min\{m : G \text{ has a non-trivial projective representation of dimension } m \text{ over } \mathbb{F}\}.$$

Also define

$$\overline{R}(G) := \min\left\{\overline{R}_{\mathbb{F}}(G) : \mathbb{F} \text{ a field}\right\}$$

Definition 4.6. Let G be a finite group, let $\mathbb{F}$ be a field, and let V be an $\mathbb{F}[G]$-module. Define $d_G(V)$ to be the minimal number of elements required to generate V as an $\mathbb{F}[G]$-module.

Remark 4.7. Let G, $\mathbb{F}$ and V be as in Definition 4.6, and let t be the number of complemented G-composition factors of V. We claim that $d_G(V) \leq t$. Note first that t is precisely the number of irreducible constituents of $V/\operatorname{Rad}(V)$. In particular, it follows that $d_G(V/\operatorname{Rad}(V)) \leq t$: let v_1, …, $v_t \in V$ such that $V/\operatorname{Rad}(V)$ is generated, as a G-module, by $\{\operatorname{Rad}(V) + v_1, \ldots, \operatorname{Rad}(V) + v_t\}$. Let M be the G-submodule of V generated by $\{v_1, \ldots, v_t\}$. Then $V = M + \operatorname{Rad}(V)$. Since $\operatorname{Rad}(V)$ is contained in every maximal submodule of V, it follows that $V = M$, and hence $d_G(V) \leq t$, as claimed.

The corollary of Lemma 4.4 can now be stated as follows.

Corollary 4.8. *Let G be a finite group, let H be a subgroup of G, and let U be an H-module, over a field $\mathbb{F}$. Let $V := U\uparrow_H^G$. Then*

$$d_G(V) \leq \frac{\dim U|G:H| - \dim U}{R_{\mathbb{F}}(G)} + \dim U.$$

Proof. Write t for the number of complemented G-composition factors of V which are not isomorphic to the trivial G-module 1_G. By Remark 4.7, we have

$$d_G(V) \leq t_{1_G}(V) + t.$$

Since $\dim V = \dim U|G : H|$, we have

$$t \leq \frac{\dim U|G : H| - \dim U}{R_{\mathbb{F}}(G)}.$$

The result now follows immediately from Lemma 4.4. □

4.2.2 Induced modules for Frattini extensions of nonabelian simple groups

In this subsection, we make some observations on modules for Frattini extensions of nonabelian simple groups. That is, modules for groups G with $G/\Phi(G)$ a non-abelian simple group.

The main result of this section reads as follows.

Proposition 4.9. *Let G be a finite group with a normal subgroup $N \leq \Phi(G)$ such that $G/N \cong T$, where T is a non-abelian finite simple group. Also, let W be a nontrivial irreducible G-module, over an arbitrary field $\mathbb{F}$. Then*

(i) Each proper normal subgroup of G is contained in N. In particular, $N = \Phi(G)$.

(ii) $\mathrm{Ker}_G(W)$, the kernel of the action of G on W, is contained in N.

(iii) $n := \dim W \geq \overline{R}(T)$.

Proof. Part (i) follows since $N \leq \Phi(G)$ and G/N is simple. Part (ii) now follows from Part (i) since W is non-trivial.

We will now prove (iii). By (ii), we may assume that G is faithful on W. In particular, we may view G as a subgroup of $GL_n(\mathbb{F})$. Let L be a normal subgroup of G, and assume that $W\downarrow_L$ is non-homogeneous. If K is the kernel of the action of G on the homogeneous components of $W\downarrow_L$, then K is a proper normal subgroup of G, so $K \leq N$ by Part (i). Thus, $HN < G$ for some stabiliser H of a homogeneous component. Hence, $|G : H| \geq |G : HN| = |G/N : HN/N| \geq \overline{R}_{\mathbb{F}}(T)$, since any proper subgroup E of T gives rise to a nontrivial permutation representation for T of dimension $|T : E|$ over $\mathbb{F}$ (a non-trivial projective representation of dimension $|T : E|$ is then achieved by reducing modulo scalars). Thus, the number of homogeneous components is at least $\overline{R}_{\mathbb{F}}(T)$, and the result follows.

So we may assume that $W\downarrow_L$ is homogeneous for each normal subgroup L of G. Hence, by Lemma 2.13, we may assume that $Z(G)$ is cyclic and that each abelian characteristic subgroup of G is contained in $Z(GL_n(\mathbb{F}))$.

Let L be the generalised Fitting subgroup of G, and extend the field $\mathbb{F}$ so that $\mathbb{F}$ is a splitting field for each subgroup of L, and so that the resulting field extension is normal (see Remark 2.15).

We distinguish two cases.

1. L is soluble. In this case, since $L > Z(G)$, $O_r(G)$ must be non-central, for some prime r, and $O_r(G)C_G(O_r(G)) \geq L$. Also, since $O_r(G)$ is non-central, we have $O_r(G)$, $C_G(O_r(G)) \leq N$ by

Part (i). Thus, since $N \leq \Phi(G) \leq L$, it follows that $N = L = O_r(G)C_G(O_r(G))$. Hence, by [29, Lemma 1.7], there exists a positive integer m such that

(1) $O_r(G)$ is a central product of its intersection with $Z := Z(G)$ and an extraspecial group E of order r^{1+2m};

(2) $Z(E)$ coincides with the subgroup of Z of order r (recall that Z is cyclic);

(3) EZ/Z is a completely reducible $\mathbb{F}_r[G]$-module under conjugation; and

(4) $C_{G/Z}(EZ/Z) = O_r(G)C_G(O_r(G))/Z$.

It follows from (4) that $T \cong G/N = G/O_r(G)C_G(O_r(G))$ is a non-trivial completely reducible subgroup of $GL_{2m}(r)$. It then follows that

$$\overline{R}_{\mathbb{F}_r}(T) \leq 2m. \tag{4.2}$$

Next, by Lemma 2.14, $W\downarrow_E$ is completely reducible and its irreducible constituents are non-trivial. Let U be such a constituent. Since $\mathbb{F}$ is a splitting field for E, U is absolutely irreducible. Hence, $\dim U \geq r^m$, by [18, Theorem 5.5]. Thus, by (4.2), we have

$$\overline{R}(T) \leq \overline{R}_{\mathbb{F}_r}(T) \leq 2m \leq r^m \leq \dim U \leq \dim W,$$

which gives us what we need.

2. L is insoluble. By [19, Lemma 2.14], L contains a normal subgroup X of G of the form $X = S_1 \circ \ldots \circ S_t$, where each S_i is isomorphic to a quasisimple group S. But since $N \leq \Phi(G)$, N is nilpotent. Also, G/N is simple, so we must have $G = X$ and G is quasisimple. In particular, $N = Z \leq Z(GL_n(\mathbb{F}))$. Hence, $T \cong G/Z \leq PGL_n(\mathbb{F})$ and $\dim W \geq \overline{R}_{\mathbb{F}}(T) \geq \overline{R}(T)$, as required.

This completes the proof. □

4.3 Induced modules for finite groups

We begin with some terminology.

Definition 4.10. Let M be a group, acted on by another group G. A *G-subgroup* of M is a subgroup of M which is stabilised by G. We say that M is *generated as a G-group* by $X \subset M$, and write $M = \langle X \rangle_G$, if no proper G-subgroup of M contains X. We will write $d_G(M)$ for the cardinality of the smallest subset X of M satisfying $\langle X \rangle_G = M$. Finally, write $M^* := M \backslash \{1\}$.

Note that the definition of $d_G(M)$ is consistent with the notation introduced in Definition 4.6 in the case where M is a G-module.

Definition 4.11. Let G be a group, acting on a set Ω. Write $\chi(G, \Omega)$ for the number of orbits of G on Ω.

The purpose of this section is to derive upper bounds for $d_G(M)$ when M is a submodule of an induced module for G. To this end, we introduce some notation which will be retained for the remainder of the section:

- Let G be a finite group.
- Fix a subgroup H of G of index $s \geq 2$.
- Fix a subgroup H_1 of H of index $d \geq 1$.
- Let U be a module for H_1 of dimension a, over a field $\mathbb{F}$.
- Let $K := \mathrm{core}_G(H)$, and fix a subgroup K' of K.
- Set $V := U\uparrow_{H_1}^H$ and $W := V\uparrow_H^G$ to be the induced modules. Note also that $V\uparrow_H^G \cong U\uparrow_{H_1}^G$.
- Denote the set of right cosets of H in G [respectively H_1 in H] by Ω [resp. Ω_1].
- Define
$$m := m(K') = \min\{\chi(Q^{\Omega_1}, \Omega_1) : Q \leq K' \text{ and } Q^V \text{ is semisimple}\}.$$

We do not exclude the case $d = 1$, that is, $H = H_1$.

4.3.1 Induced modules: The soluble case

This section is essentially an analogue of [7, Section 5]. We first recall the constant b,

$$b := \sqrt{\frac{2}{\pi}}.$$

We also recall, from Section 1, the following definition.

Definition 4.12. For a positive integer s with prime factorisation $s = p_1^{r_1}p_2^{r_2}\dots p_t^{r_t}$, set $\omega(s) := \sum r_i$, $\omega_1(s) := \sum r_i p_i$, $K(s) := \omega_1(s) - \omega(s) = \sum r_i(p_i - 1)$ and

$$\widetilde{\omega}(s) = \frac{s}{2^{K(s)}}\binom{K(s)}{\left\lfloor \frac{K(s)}{2} \right\rfloor}.$$

The main result of this section reads as follows.

Theorem 4.13. *Suppose that G^Ω contains a soluble transitive subgroup, and let M be a submodule of W. Also, denote by $\chi = \chi(K, V^*)$ the number of orbits of K on the non-zero elements of V. Then*

$$d_G(M) \leq \min\left\{\frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi\right\}\widetilde{\omega}(s) \leq \min\left\{\frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi\right\}\left\lfloor \frac{bs}{\sqrt{\log s}} \right\rfloor$$

where $b := \sqrt{2/\pi}$. Furthermore, if $s = p^t$, with p prime, then

$$d_G(M) \leq \min\left\{\frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi\right\}\left\lfloor \frac{bp^t}{\sqrt{t(p-1)}} \right\rfloor.$$

Remark 4.14. If K has infinitely many orbits on the non-zero elements of V, then we assume, in Theorem 4.13, and whenever it is used in the remainder of the paper, that

$$\min\left\{\frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi\right\} = \frac{ad - am}{R_{\mathbb{F}}(K')} + am.$$

We begin our work towards the proof of Theorem 4.13 by first collecting a series of lemmas from [7, Section 5].

Lemma 4.15 ([7], Lemma 5.1). *Suppose that G^Ω contains a soluble transitive subgroup. Then there is a right transversal $\mathcal{T}$ to H in G, with a partial order $\preccurlyeq$ and a full order $\leqslant$, satisfying the following properties:*

(i) Whenever t_1, t_2, $t_3 \in \mathcal{T}$ with $t_1 < t_2 \preccurlyeq t_3$, we have $t_4 < t_3$, where t_4 is the unique element of $\mathcal{T}$ such that $t_1 t_2^{-1} t_3 \in H t_4$.

(ii) With respect to this partial order, $\mathcal{T}$ is a cartesian product of k chains, of length p_1, p_2, …, p_k, where $k = \omega(s)$, and p_1, p_2, …, p_k denote the (not necessarily distinct) prime divisors of s.

Proof. Let F be a subgroup of G such that F^Ω is soluble and transitive. By [7, Lemma 5.1], there exists a right transversal $\mathcal{T}$ for $F \cap H$ in F such that the image $\mathcal{T}^\Omega$ has a partial order $\preccurlyeq'$ and a full order $\leqslant'$ satisfying

(a) Whenever t_1, t_2, $t_3 \in \mathcal{T}$ with ${t_1}^\Omega <' {t_2}^\Omega \preccurlyeq' {t_3}^\Omega$, we have ${t_4}^\Omega <' {t_3}^\Omega$, where t_4 is the unique element of $\mathcal{T}$ such that $(t_1 t_2^{-1} t_3)^\Omega \in (F \cap H)^\Omega {t_4}^\Omega$.

(b) With respect to this partial order, $\mathcal{T}^\Omega$ is a cartesian product of k chains, of length p_1, p_2, …, p_k, where $k = \omega(|F : F \cap H|) = \omega(|G : H|) = \omega(s)$, and p_1, p_2, …, p_k denote the (not necessarily distinct) prime divisors of s.

For t_1, $t_2 \in \mathcal{T}$, say now that $t_1 \preccurlyeq t_2$ if ${t_1}^\Omega \preccurlyeq' {t_2}^\Omega$, and $t_1 \leqslant t_2$ if ${t_1}^\Omega \leqslant' {t_2}^\Omega$. Since F^Ω acts transitively on the set of cosets of H in G, $\mathcal{T}$ is a right transversal for H in G. By definition, (a) and (b) above imply that (i) and (ii) hold for this choice of $\preccurlyeq$ and $\leqslant$. This gives us what we need. □

For the remainder of Section 4.3 assume that G^Ω contains a soluble transitive subgroup, and fix $\mathcal{T}$ to be a right transversal for H in G as exhibited in Lemma 4.15. Then we may write the induced module $W = V \uparrow_H^G$ as $W = \bigoplus_{t \in \mathcal{T}} V \otimes t$, where the action of G is given by

$$(v \otimes t)^{ht'} = v^{h_1} \otimes t_1,$$

where $tht' = h_1 t_1$, h, $h_1 \in H$, t, t', $t_1 \in \mathcal{T}$. Thus, each element w in W may be written as $w = \sum_{t \in \mathcal{T}} v(w,t) \otimes t$, with uniquely determined coefficients $v(w,t)$ in V.

Definition 4.16 ([7], Section 5). Let $w \in W$ be non-zero. The *height* of w, written $\tau(w)$, is the largest element of the set $\{t \in \mathcal{T} : v(w,t) \neq 0\}$, with respect to the full order $\leqslant$. Also, we define $\mu(w) := v(w, \tau(w))$. Thus, $\mu(w)$ is non-zero, and $v(w,t) = 0$ whenever $t > \tau(w)$. The element $\mu(w) \otimes \tau(w)$ is called the *leading summand* of w.

Remark 4.17. In the language of Definition 4.16, Lemma 4.15 Part (i) states that if the height of w is t_2, and if $t_2 \preccurlyeq t_3$, then the height of $w^{t_2^{-1} t_3}$ is t_3. Further, the leading summand of $w^{t_2^{-1} t_3}$ is $\mu(w) \otimes t_3$.

The formulation in Remark 4.17 leads to an important technical point.

Proposition 4.18. *Let M be a submodule of W. Then M has a generating set X with the following property: No subset Y of X, whose image $\tau(Y)$ in $\mathcal{T}$ is a chain with respect to the partial order $\preccurlyeq$, can have more than*

$$\min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')}+am, \chi\right\}$$

elements, where $\chi = \chi(K, V^*)$ denotes the number of orbits of K on the nonzero elements of V.

Before proving Proposition 4.18, we need a preliminary lemma.

Lemma 4.19. *A K'-composition series for V contains at most am factors isomorphic to the trivial module.*

Proof. Let $Q \leq K'$ such that Q^V is semisimple and $\chi(Q^{\Omega_1}, \Omega_1) = m$. By Mackey's Theorem,

$$V\downarrow_Q = \left(U\uparrow_{H_1}^H\right)\downarrow_Q \cong \bigoplus_{i=1}^{m} U_{x_i}, \tag{4.3}$$

where $U_{x_i} := (U \otimes x_i)\uparrow_{Q\cap H_1^{x_i}}^Q$, $\dim U_{x_i} = \dim U = a$, for each i, and $\sum_j |Q : Q \cap H_1^{x_i}| = |H : H_1| = d$. Since Q^V is semisimple, the number of Q-composition factors of $U_{x_i} = (U \otimes x_i)\uparrow_{Q\cap H_1^{x_i}}^Q$ isomorphic to the trivial module 1_Q is precisely

$$\dim \mathrm{Hom}_{\mathbb{F}[Q]}((U \otimes x_i)\uparrow_{Q\cap H_1^{x_i}}^Q, 1_Q) = \dim \mathrm{Hom}_{\mathbb{F}[Q\cap H_1^{x_i}]}((U \otimes x_i), 1_{Q\cap H_1^{x_i}}),$$

applying Frobenius Reciprosity. This is at most $\dim(U \otimes x_i) = \dim U = a$. The result now follows immediately from (4.3.1). □

Proof of Proposition 4.18. Set $e := \frac{ad-am}{R_{\mathbb{F}}(K')} + am$, and let X be a finite generating set for M, consisting of non-zero elements. Suppose that $Y := \{w_0, w_1, \ldots, w_e\}$ is a subset of X whose image under τ forms a chain in $\mathcal{T}$: Say $\tau(w_0) \preccurlyeq \tau(w_1) \preccurlyeq \ldots \preccurlyeq \tau(w_e)$.

Consider now the vectors $\mu(w_0)$, $\mu(w_1)$, …, $\mu(w_e)$: For $1 \leq i \leq e+1$ let W_i denote the K'-module generated by $\mu(w_0)$, …, $\mu(w_{i-1})$, and consider the series of K'-modules

$$0 =: W_0 \leq W_1 \leq \ldots \leq W_{e+1} \tag{4.4}$$

Suppose that $W_i < W_{i+1}$ for all i. Then the series (4.4) can be extended to give a K'-composition series for V. Thus, Lemma 4.19 implies that at most am of the factors W_{i+1}/W_i are trivial. Furthermore, the rest have dimension at least $R_{\mathbb{F}}(K')$. It follows that $\dim W_{e+1} = \sum_{i=1}^{e+1} \dim W_i/W_{i-1} \geq am + (e + 1 - am)R_{\mathbb{F}}(K') > ad$, which is a contradiction, since $\dim V = ad$.

Thus, we must have $\mu(w_i) \in W_i$ for some i. In this case,

$$\mu(w_i) = \sum_{j=0}^{i-1} \sum_{k\in K'} \lambda_{j,k}\mu(w_j)^k,$$

for some scalars $\lambda_{j,k}$. Moreover, the element

$$x := \sum_{j=0}^{i-1} \sum_{k\in K'} \lambda_{j,k} w_j^{k^{\tau(w_j)}\tau(w_j)^{-1}\tau(w_i)}$$

of M has the same leading summand as w_i, by Lemma 4.15 Part (i) (see also Remark 4.17). Hence, either $x = w_i$ and w_i may be removed from X, or w_i may be replaced in X by the element $w_i - x$, which has height strictly preceding w_i in the full order $\leqslant$. In this way, the resulting (modified) set X still generates M. This procedure can only be carried out a finite number of times, and when it can no longer be repeated, the (modified) generating set can have no more than e elements.

If $\chi \geq e$, then we are done, so assume that $\chi < e$. Let v and w be elements of X whose images $\tau(v)$ and $\tau(w)$ are comparable (with respect to $\preccurlyeq$) in $\mathcal{T}$: Say $\tau(v) \preccurlyeq \tau(w)$. Suppose that $\mu(w)$ and $\mu(v)$ lie in the same K-orbit of V, and let $g \in K$ such that $\mu(w)^g = \mu(v)$. Since K is normal in G, the leading summand of w^g is $\mu(v) \otimes \tau(w)$. Thus, by replacing w with w^g, we may assume that $\mu(v) = \mu(w)$. Then, using Lemma 4.15 Part (i) again, we see that $v^{\tau(v)^{-1}\tau(w)}$ has the same leading summand as w. Write $v^{\tau(v)^{-1}\tau(w)} = x + \mu(v) \otimes \tau(w)$, and $w = y + \mu(v) \otimes \tau(w)$, for x, $y \in V$, and let $u = y - x$. Then, we see that, as in the proof of [7, Lemma 5.2], either $u = 0$, and $w = v^{\tau(v)^{-1}\tau(w)}$ may be omitted from X, or $u \neq 0$, and $w = u + v^{\tau(v)^{-1}\tau(w)}$ may be replaced in X by the element u, which has height strictly preceding $\tau(w)$ in the full order $\leqslant$. This way, the resulting set obtained from X still generates M. The procedure outlined above can only be carried out a finite number of times, and when it can no longer be repeated, the (modified) generating set can contain no more than χ elements. This completes the proof. □

Before proving Theorem 4.13, we note the following easy consequence of Dilworth's Theorem ([15, Theorem 1.1]):

Lemma 4.20. *If a partially ordered set P has no chain of cardinality greater than k, and no antichain of cardinality greater than l, then P cannot have cardinality greater than kl.*

Proof of Theorem 4.13. Let $\mathcal{T}$ be a right transversal for H in G with full and partial orders $\leqslant$ and $\preccurlyeq$, as in Lemma 4.15. Now define a partial order on the elements of W as follows: First, for each $t \in \mathcal{T}$, choose a full order on the elements of W of height t. Now, for w_1 and w_2 in W, say that $w_1 < w_2$ if $\tau(w_1)$ is less than $\tau(w_2)$ in $(\mathcal{T}, \preccurlyeq)$, or if $\tau(w_1) = \tau(w_2)$ but w_1 precedes w_2 in the full order chosen for elements of height $\tau(w_1)$.

Then $\tau : W \to \mathcal{T}$ is a poset homomorphism which takes incomparable elements to incomparable elements, so no antichain of its domain can have cardinality greater than $\widetilde{\omega}(s)$, by Lemmas 4.1 and 4.15 Part (ii). Let X be a generating set for M with the properties guaranteed by Proposition 4.18. Then no chain in X can have more than $\min\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\}$ elements. Lemma 4.20 then implies that

$$|X| \leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\}\widetilde{\omega}(s) \leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\}\left\lfloor \frac{bs}{\sqrt{\log s}} \right\rfloor,$$

where the second inequality follows from Theorem 1.3. If $s = p^t$ for p prime, then

$$|X| \leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\}\left\lfloor \frac{bp^t}{\sqrt{t(p-1)}} \right\rfloor,$$

again by Lemma 4.20 and Theorem 1.3. This completes the proof. □

4.3.2 Induced modules for finite groups: The general case

In this section, we prove a weaker form of Theorem 4.13 for general finite groups (i.e. those G for which G^Ω does not necessarily contain a soluble transitive subgroup). We retain the notation introduced at the beginning of Section 4.3.

We begin with a definition. Recall the definitions of $\widetilde{\omega}(s)$, s_p, and $\mathrm{lpp}\,(s)$ from Definitions 1.4 and 1.5.

Definition 4.21. For a prime p, set

$$E(s,p) := \min\left\{\left\lfloor \frac{bs}{\sqrt{(p-1)\log_p s_p}}\right\rfloor, \frac{s}{\mathrm{lpp}\,(s/s_p)}\right\} \text{ and } E_{sol}(s,p) := \min\{\widetilde{\omega}(s), s_p\}$$

where we take $\left\lfloor bs/\sqrt{(p-1)\log_p s_p}\right\rfloor$ to be ∞ if $s_p = 1$.

Proposition 4.22. *Let p be prime. Then $E_{sol}(s,p) \leq E(s,p)$.*

Proof. By Theorem 1.3 we have $\widetilde{\omega}(s) \leq \left\lfloor \frac{bs}{\sqrt{(p-1)\log_p s_p}}\right\rfloor$. Also, it is clear that $s_p \leq \frac{s}{\mathrm{lpp}\,(s/s_p)}$. The result follows. □

Remark 4.23. For any finite group G and any G-module M, $d_G(M)$ is bounded above by $\chi(G, M^*)$.

For the remainder of this section, we will make a further assumption: that the field $\mathbb{F}$ has characteristic $p > 0$. We are now ready to state and prove the main result of this section.

Theorem 4.24. *For a prime $q \neq p$, let P_q be a Sylow q-subgroup of G. Also, let P' be a maximal p'-subgroup of G. Let M be a submodule of the induced module $W = V\uparrow_H^G$.*

(i) If G is soluble, then

$$d_G(M) \leq \min\left\{\frac{ad - a\chi(P'\cap K, \Omega_1)}{R_{\mathbb{F}}(P'\cap K)} + a\chi(P'\cap K, \Omega_1), \chi(P'\cap K, V^*)\right\} s_p.$$

(ii) Let N be a subgroup of G such that N^Ω is soluble, and let s_i, $1 \leq i \leq t$, be the sizes of the orbits of N on Ω. Then

(a) We have

$$d_G(M) \leq \min\left\{\frac{ad - a\chi(N\cap P'\cap K, \Omega_1)}{R_{\mathbb{F}}(N\cap P'\cap K)} + a\chi(N\cap P'\cap K, \Omega_1), \chi(N\cap P'\cap K, V^*)\right\} \times \sum_{i=1}^{t} \widetilde{\omega}(s_i).$$

(b) If N is soluble, and P'_N is a p-complement in N, then

$$d_G(M) \leq \min\left\{\frac{ad - a\chi(P'_N\cap K, \Omega_1)}{R_{\mathbb{F}}(P'_N\cap K)} + a\chi(P'_N\cap K, \Omega_1), \chi(P'_N\cap K, V^*)\right\} \times \sum_{i=1}^{t} E_{sol}(s_i, p).$$

(iii) $d_G(M) \leq \min\left\{\frac{ad-a\chi(P_q\cap K,\Omega_1)}{R_{\mathbb{F}}(P_q\cap K)} + a\chi(P_q\cap K,\Omega_1), \chi(P_q\cap K, V^*)\right\} s/s_q$.

(iv) Assume that $s_p > 1$. *Then*

$$d_G(M) \leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi(K,V^*)\right\}\left\lfloor \frac{bs}{\sqrt{\log s_p}}\right\rfloor.$$

Proof. The proof is based on the idea of Lucchini et al. used in the proof of [28, Lemma 4]. Let Q be a subgroup of G, and choose a full set $\{x_1, x_2, \ldots, x_t\}$ of representatives for the (H,Q)-double cosets in G. Also, for $1 \leq i \leq t$, put $s_i := |Q : Q\cap H^{x_i}|$ (note that, by H^{x_i}, we mean, as usual, the conjugate subgroup $x_i^{-1}Hx_i$). By Mackey's Theorem we have

$$W\downarrow_Q = (V\uparrow_H^G)\downarrow_Q = \bigoplus_{i=1}^{t} V_{x_i} \tag{4.5}$$

where $V_{x_i} \cong (V\otimes x_i)\uparrow_{Q\cap H^{x_i}}^{Q}$. Comparing dimensions of the left and right hand side of (4.5) above, we get

$$ads = \dim W = \sum_{i=1}^{t} ad|Q : Q\cap H^{x_i}| = ad\sum_{i=1}^{t} s_i$$

so that $\sum_{i=1}^{t} s_i = s$. Clearly, the s_i represent the sizes of the orbits of Q on the right cosets of H in G.

Next, for $1 \leq i \leq t$, set $V_i := V_{x_1} \oplus V_{x_2} \oplus \ldots \oplus V_{x_i}$. Then, we have a chain $0 = V_0 \leq V_1 \leq \ldots \leq V_t = W$ of Q-submodules of W. This allows us to define the chain of Q-modules $0 = M_0 \leq M_1 \leq \ldots \leq M_t = M$, where $M_i := M \cap V_i$. Furthermore, in this case, the quotient M_i/M_{i-1} is (isomorphic to) a Q-submodule of V_{x_i}. Hence

$$d_G(M) \leq d_Q(M) \leq \sum_{i=1}^{t} d_Q(M_i/M_{i-1}). \tag{4.6}$$

Note that $V\otimes x_i$ is isomorphic to an induced module $(U\otimes x_i)\uparrow_{H_1^{x_i}}^{H^{x_i}}$. Hence, Mackey's Theorem implies that $(V\otimes x_i)\downarrow_{Q\cap K}$ is isomorphic to a direct sum

$$(V\otimes x_i)\downarrow_{Q\cap K} \cong \bigoplus_j U_{x_{i,j}}, \tag{4.7}$$

where $U_{x_{i,j}} \cong (U\otimes x_{i,j})\uparrow_{Q\cap K\cap H_1^{x_{i,j}}}^{Q\cap K}$ is an induced module for $Q\cap K$, and $\sum_j |Q\cap K : Q\cap K\cap {H_1}^{x_{i,j}}| = |H^{x_i} : H_1^{x_i}| = d$.

Suppose that $(|Q|, p) = 1$. Then each V_{x_i} is a semisimple $\mathbb{F}[Q]$-module, so

$$\begin{aligned}
d_Q(M_i/M_{i-1}) &\leq d_Q(V_{x_i}) \\
&\leq d_{Q\cap H^{x_i}}(V \otimes x_i) \\
&\leq d_{Q\cap K}(V \otimes x_i) \\
&\leq \sum_j d_{Q\cap K}(U_{x_{i,j}}) \\
&\leq \sum_j \min\left\{ \frac{a|Q\cap K : Q\cap K\cap H_1^{x_{i,j}}| - a}{R_{\mathbb{F}}(Q\cap K)} + a, \chi(Q\cap K, \right. \\
&\left. [U_{x_{i,j}}]^*) \right\} \\
&\leq \min\left\{ \sum_j \frac{a|Q\cap K : Q\cap K\cap H_1^{x_{i,j}}| - a}{R_{\mathbb{F}}(Q\cap K)} + a, \sum_j \chi(Q\cap K, \right. \\
&\left. [U_{x_{i,j}})]^*) \right\} \\
&= \min\left\{ \frac{ad - a\chi(Q\cap K, \Omega_1)}{R_{\mathbb{F}}(Q\cap K)} + a\chi(Q\cap K, \Omega_1), \chi(Q\cap K, V^*) \right\}
\end{aligned}$$

The fourth inequality above follows from (4.7), while the fifth follows from Corollary 4.8 and Remark 4.23. Thus

$$d_G(M) \leq \min\left\{ \frac{ad - a\chi(Q\cap K, \Omega_1)}{R_{\mathbb{F}}(Q\cap K)} + a\chi(Q\cap K, \Omega_1), \chi(Q\cap K, V^*) \right\} t \tag{4.8}$$

by (4.6).

Write $s_p := p^\beta$ and $s_q := q^\alpha$. Also, write $s = p^\beta q^\alpha k$ and $|H| = p^\delta q^\gamma l$, where $|H|_p = p^\delta$, $|H|_q = q^\gamma$. We are now ready to prove the theorem.

(i) Suppose that G is soluble, and take $Q := P'$ to be a p-complement in G. Then $|Q| = q^{\alpha+\gamma}kl$. Hence, $s_i = |Q : Q \cap H^{x_i}| \geq q^\alpha k = s/s_p$. Part (i) now follows from (4.8), since $s = \sum_{i=1}^t s_i \geq ts/s_p$.

(ii) Take $Q := N$. By Theorem 4.13, we have

$$\begin{aligned}
d_Q(M_i/M_{i-1}) \leq \min\left\{ \frac{ad - a\chi(Q\cap P'\cap K, \Omega_1)}{R_{\mathbb{F}}(Q\cap P'\cap K)} + a\chi(Q\cap P'\cap K, \Omega_1), \right. \\
\left. \chi(Q\cap P'\cap K, V^*) \right\} \widetilde{\omega}(s_i).
\end{aligned}$$

Part (a) of (ii) now follows from (4.6). Next, assume that N is soluble, with a p-complement P'_N. Then

$$\begin{aligned}
d_Q(M_i/M_{i-1}) \leq \min\left\{ \frac{ad - a\chi(Q\cap P'\cap K, \Omega_1)}{R_{\mathbb{F}}(Q\cap P'\cap K)} + a\chi(Q\cap P'\cap K, \Omega_1), \right. \\
\left. \chi(Q\cap P'\cap K, V^*) \right\} (s_i)_p
\end{aligned}$$

by Part (i). Also, $P'_N = N \cap P'$ for some maximal p'-subgroup P' of G, so Part (b) follows from (4.6) by combining the above with Part (ii)(a).

(iii) In the general case, take $Q := P_q$. Then $|Q| = q^{\alpha+\gamma}$, so $s_i = |Q : Q \cap H^{x_i}| \geq q^\alpha$. Also, $s = \sum_{i=1}^t s_i \geq tq^\alpha = ts_q$. Part (iii) then follows from (4.8).

(iv) Here, we have $\beta > 0$ since $s_p > 0$. Let P be a Sylow p-subgroup of G, and set $Q = KP$. Then $s_i = |Q : Q \cap H^{x_i}| = |QH^{x_i}|/|H^{x_i}| \geq |PH^{x_i}|/|H^{x_i}| = |P : P \cap H^{x_i}| \geq p^\beta$, for each i. Since $K \leq \mathrm{core}_Q(Q \cap H^{x_i})$, we have $\chi(\mathrm{core}_Q\,(Q \cap H^{x_i}), (V \otimes x_i)^*) \leq \chi(K, V^*) =: \chi$ for each i. Then (4.6) and Theorem 4.13 give

$$\begin{aligned} d_G(M) &\leq \sum_{i=1}^t \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\} \left\lfloor \frac{bs_i}{\sqrt{\log s_i}} \right\rfloor \\ &\leq \sum_{i=1}^t \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\} \left\lfloor \frac{bs_i}{\sqrt{\beta}} \right\rfloor \\ &\leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\} \left\lfloor \sum_{i=1}^t \frac{bs_i}{\sqrt{\beta}} \right\rfloor \\ &= \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\} \left\lfloor \frac{bs}{\sqrt{\beta}} \right\rfloor \end{aligned}$$

This proves (iv).

□

Since $\frac{ad-f}{e} + f \leq ad$ for positive integers e and f, the following corollary is immediate.

Corollary 4.25. *Let M be a submodule of W. Also, let q, P_q and P' be as in Theorem 4.24. Then*

(i) If G is soluble, then $d_G(M) \leq \min\{ad, \chi(P' \cap K, V^*)\}\, s_p$.

(ii) Let N be a subgroup of G such that N^Ω is soluble, and let s_i, $1 \leq i \leq t$, be the sizes of the orbits of N on Ω. Then

(a) We have $d_G(M) \leq \min\{ad, \chi(N \cap P' \cap K, V^*)\} \sum_{i=1}^t \widetilde{\omega}(s_i)$.

(b) If N is soluble, and P'_N is a p-complement in N, then

$$d_G(M) \leq \min\left\{ad, \chi(P'_N \cap K, V^*)\right\} \sum_{i=1}^t E_{sol}(s_i, p).$$

(iii) $d_G(M) \leq \min\{ad, \chi(P_q \cap K, V^*)\}\, s/s_q$.

(iv) $d_G(M) \leq \min\{ad, \chi(K, V^*)\} \left\lfloor \frac{bs}{\sqrt{\log s_p}} \right\rfloor$.

We also record the following, which is an immediate consequence of Corollary 4.25. Note that Theorem 1.6

Corollary 4.26. *Define E' to be E_{sol} if G^Ω contains a soluble transitive subgroup, and $E' := E$ otherwise. Let M be a submodule of W. Then $d_G(M) \leq adE'(s, p)$.*

Note that Theorem 1.6 follows from Corollary 4.26. Using the definition of $E(s,p)$, and Lemma 2.17, we also deduce the following.

Corollary 4.27. *Let M be a submodule of W, and fix $0 < \alpha < 1$.*

(i) If $s_p \geq s^\alpha$, then $d_G(M) \leq adE(s,p) \leq ad \left\lfloor \frac{bs\sqrt{\frac{1}{\alpha}}}{\sqrt{\log s}} \right\rfloor$;

(ii) If $s_p \leq s^\alpha$, then $d_G(M) \leq adE(s,p) \leq ad \left\lfloor \frac{\frac{1}{1-\alpha}s}{c' \log s} \right\rfloor$;

(iii) We have

$$d_G(M) \leq adE(s,p) \leq \begin{cases} \left\lfloor \frac{2ads}{c' \log s} \right\rfloor, & \text{if } 2 \leq s \leq 1260, \\ \left\lfloor \frac{adbs\sqrt{2}}{\sqrt{\log s}} \right\rfloor, & \text{if } s \geq 1261. \end{cases}$$

Proof. Part (i) follows immediately from the definition of $E(s,p)$, while Part (ii) follows from the definition and Lemma 2.17. Finally, set $\alpha := 1/2$. Then

$$\frac{2ads}{c' \log s} \leq \frac{adbs\sqrt{2}}{\sqrt{\log s}}$$

for $s \geq 1261$, so Part (iii) also follows. □

The following is also immediate, from Part (ii) of Theorem 4.24.

Corollary 4.28. *Let M be a submodule of W. If G contains a soluble subgroup N, acting transitively on Ω, then*

$$d_G(M) \leq \min \left\{ \frac{ad - a\chi(P'_N \cap K, \Omega_1)}{R_{\mathbb{F}}(P'_N \cap K)} + a\chi(P'_N \cap K, \Omega_1), \chi(P'_N \cap K, V^*) \right\} \times E(s,p)$$

where P'_N is a p-complement in N.

4.4 An application to induced modules for bottom heavy groups

The proofs of the main results of this paper will usually only require the bounds on $d_G(M)$ from Corollary 4.25. For a specific case of the proof of Theorem 1.7 however, we will need the stronger bounds provided by Theorem 4.24. This case is the 'bottom heavy case', which we will now define. Throughout, we retain the notation introduced at the beginning of Section 4.3. In particular, H is a subgroup of G of index of index $s \geq 2$, H_1 is a subgroup of H of index $d \geq 1$, Ω is the set of right cosets of H in G, Ω_1 is the set of right cosets of H_1 in H, and $K := \mathrm{Ker}_G(\Omega)$. Note that we also continue to assume that the field $\mathbb{F}$ has characteristic $p > 0$.

Definition 4.29. Assume that K^{Ω_1}, viewed as a subgroup of $\mathrm{Sym}\,(d)$, contains $\mathrm{Alt}(d)$. Then we say that the triple (G, H, H_1) is *bottom heavy*.

Before stating the main result of this section, we introduce Vinogradov notation: we will write

$$A \ll B$$

to mean $A = O(B)$. The main result can now be stated as follows.

Proposition 4.30. *Assume that $d \geq 5$ and that (G, H, H_1) is bottom heavy. Let M be a submodule of W. Then*

(i) $d_G(M) \leq 2as$, and;

(ii) If $s_p > 1$, then $d_G(M) \ll \frac{as}{\sqrt{\log s_p}}$.

Before proving Proposition 4.30, we require the following:

Proposition 4.31. *Assume that (G, H, H_1) is bottom heavy and that $d \geq 5$. Choose K' to be a subgroup of K minimal with the property that $K'^{\Omega_1} \cong \mathrm{Alt}(d)$. Then a K'-composition series for $V\downarrow_{K'}$ has at most $2a$ factors isomorphic to the trivial K'-module.*

Proof. By the minimality of K', we have $C := \mathrm{core}_H(H_1) \cap K' \leq \Phi(K')$, and hence C is soluble. Let E be a subgroup of K' containing C such that E/C is soluble and, viewed as a subgroup of $\mathrm{Sym}\,(d)$, has at most two orbits, such that each orbit is of p'-length (such a subgroup exists by Lemma 2.9). Then E is soluble, so we may choose a p-complement F in E. Then $F/F \cap C$ also has at most two orbits (and each F-orbit has p'-length).

Next, consider the F-module $X := V\downarrow_F \cong U\uparrow^H_{H_1}\downarrow_F$. Since $F \leq K'$, it suffices to prove that X has at most $2a$ trivial composition factors. To see this, note that since F has at most two orbits on Ω_1 (i.e. the cosets of H_1 in H), represented by x_1 and x_2, say, Mackey's Theorem yields

$$X \cong X_1 \oplus X_2 \text{ or } X \cong X_1$$

where $X_i \cong (U \otimes x_i)\uparrow^F_{F\cap H_1^{x_i}}$. Now, since F has p'-order, X_i is a semisimple F-module. Hence, the number of trivial factors in an F-composition series for X_i is precisely the number of trivial summands of X_i, which is

$$\dim \mathrm{Hom}_{\mathbb{F}[F]}(X_i, 1_F),$$

where 1_F denotes the trivial F-module. By Frobenius Reciprosity, this is equal to

$$\dim \mathrm{Hom}_{\mathbb{F}[F\cap H_1^{x_i}]}(U\downarrow_{F\cap H_1^{x_i}}, 1_{F\cap H_1^{x_i}}) \leq \dim U = a.$$

The claim follows. □

Proof of Proposition 4.30. Choose K' to be a subgroup of K minimal with the property that $K'^{\Omega_1} \cong \mathrm{Alt}(d)$. Then

$$\mathrm{core}_H(H_1) \cap K' \leq \Phi(K'). \tag{4.9}$$

Hence, since

$$\mathrm{Alt}(d) \cong K'^{\Omega} \cong K'/\mathrm{core}_H(H_1) \cap K',$$

Proposition 4.9 applies: $R_{\mathbb{F}}(K') \geq \overline{R}(\mathrm{Alt}(d))$. Note also that $m \leq 2$ by Lemma 2.9. Since $d \ll \overline{R}(\mathrm{Alt}(d))$ (see [22, Proposition 5.3.7]), Part (ii) now follows from Theorem 4.24 Part (iv).

We now prove (i). It follows from Lemma 2.9 that K' has a subgroup N such that N^{Ω_1} is soluble and has at most 2 orbits. Furthermore, each orbit has p'-length. Also, N is soluble, by (4.9).

We now want to apply Corollary 4.25 Part (ii)(b), with (G, H, H_1, V, Ω) replaced by $(H, H_1, H_1, U, \Omega_1)$ (also, (a, s, d) is replaced by $(a, d, 1)$): let d_i, for $i \leq 2$, denote the lengths of the N^{Ω_1} orbits. Then

$$E_{sol}(d_i, p) \leq (d_i)_p = 1,$$

so $E_{sol}(d_i, p) = 1$. Hence for each H-submodule M' of the induced module $V = U \uparrow_{H_1}^{H}$, we have

$$d_H(M') \leq a \sum_{i=1}^{t} E_{sol}(d_i, p) \leq 2a.$$

Since M is a submodule of

$$U \uparrow_{H_1}^{G} \cong V \uparrow_{H}^{G} \cong \sum_{i=1}^{s} V \otimes t_i$$

where each $V \otimes t_i$ is isomorphic, as an H-module, to V, the result now follows. □

5 Minimal generation of transitive permutation groups

In this section, we restate and prove the first main result of this paper, which is stated as Theorem 1.1 in Section 1. The theorem follows in the primitive case from Theorem 2.11, so this section deals predominantly with the case when $G \leq \mathrm{Sym}(n)$ is imprimitive. In this case, G is a large subgroup of a wreath product $R \wr S$, where R is primitive of degree $r \geq 2$, S is transitive of degree $s \geq 2$, and $n = rs$. Due to the nature of our bounds, the most difficult cases to deal with are when $R = \mathrm{Sym}(2)$ or $R = \mathrm{Sym}(4)$, i.e. when G has a minimal block of cardinality either 2 or 4. (Essentially, this is because Sym(2) and Sym(4) have large composition lengths relative to their degree.) We deal with the Sym(4) case in Corollary 5.11; the idea being that we can use the transitive action of the Sylow 3-subgroup in Sym(4) on the non-identity elements of the Klein 4-group $V \trianglelefteq \mathrm{Sym}(4)$ to reduce the contribution of V to our bounds (this is the primary reason we include the invariant χ in our bounds in Section 4).

However, no such option is available to us when $R \cong \mathrm{Sym}(2)$, since Sym(2) is abelian. If G has another minimal block, of cardinality larger than 2, then we can avoid the problem by using this block instead. However, we cannot do this if all minimal blocks for G have cardinality 2, so assume that this is the case. Then, as we will prove in Section 5.2 below, we have $d(G) \leq E(s, 2) + d(S)$. Now, since we just need to bound $d(S)$, we apply the same methods to the transitive group $S \leq \mathrm{Sym}(s)$.

Apart from finitely many cases, our methods yield the upper bound we want: the only problems occur when we "repeatedly get" blocks of cardinality 2. This is encapsulated in the following non-standard definition.

Definition 5.1. Let G be a transitive permutation group, and let

$$X := (R_1, R_2, \ldots, R_t)$$

be a tuple of primitive components for G, where each R_i has degree $r_i \geq 2$. Define

$$\begin{aligned} \mathrm{bl}_{X,2}(G) &:= \min\{i : r_i \neq 2\} - 1, \text{ and} \\ \mathrm{bl}_2(G) &:= \min\{\mathrm{bl}_{X,2}(G) : X \text{ a tuple of primitive components for } G\}. \end{aligned}$$

We call $\mathrm{bl}_2(G)$ the 2-*block number* of G.

Alternatively, the 2-block number of a transitive permutation group G can be defined inductively as follows: if G is primitive, or if G is imprimitive with a minimal block of cardinality greater than 2, then set $\mathrm{bl}_2(G) := 0$. Otherwise, G is imprimitive and all minimal blocks for G have cardinality 2. Let Δ be such a minimal block, and let $\Gamma := \{\Delta^g : g \in G\}$ be the set of G-translates of Δ. Also, let $K := \mathrm{Ker}_G(\Gamma)$. Then define $\mathrm{bl}_2(G) := 1 + \mathrm{bl}_2(G/K)$.

For example, a transitive 2-group G of degree 2^k will have $\mathrm{bl}_2(G) = k$. In other words, any tuple of primitive components for G will consist entirely of Sym(2)s. This is because for any prime p, any minimal block of any transitive p-group has cardinality p.

Remark 5.2. If $\mathrm{bl}_2(G) \geq 1$, then G has a block of size $2^{\mathrm{bl}_2(G)}$, by Remark 2.4.

We can now restate Theorem 1.1 more precisely as follows.

Theorem 5.3. *Let G be a transitive permutation group of degree $n \geq 2$. Then*

(1) $d(G) \leq \left\lfloor \frac{cn}{\sqrt{\log n}} \right\rfloor$, *where* $c := 1512660\sqrt{\log(2^{19}15)}/(2^{19}15) = 0.920581\ldots$.

(2) $d(G) \leq \left\lfloor \frac{c_1 n}{\sqrt{\log n}} \right\rfloor$, *where* $c_1 := \sqrt{3}/2 = 0.866025\ldots$, *unless each of the following conditions hold:*

- *(i)* $n = 2^k v$, *where* $v = 5$ *and* $17 \leq k \leq 26$, *or* $v = 15$ *and* $15 \leq k \leq 35$;
- *(ii)* G *contains no soluble transitive subgroups; and*
- *(iii)* $\mathrm{bl}_2(G) \geq f$, *where* f *is specified in the middle column of Table A.2 (see Appendix A).*

In these exceptional cases, the bounds for $d(G)$ in Table A.2 hold.

Recall that by "log", we always mean log to the base 2. The following is immediate from Theorem 5.3. Note also that Corollary 1.2 follows immediately from Theorem 5.3.

As can be seen from the proof of Theorem 5.3, and the statement of the theorem itself, the cases when $\mathrm{bl}_2(G)$ is large are the most difficult to deal with using our methods. We believe that the finite number of exceptions given in Theorem 5.3 Part (2) are not exceptions at all, that is, we believe that the bound $d(G) \leq \lfloor c_1 n/\sqrt{\log n} \rfloor$ should hold for all n and all G.

Note also that, as shown in [21], the bounds in our results are of the right order. Moreover, the infimum of the set of constants $\overline{c}$ satisfying $d(G) \leq \overline{c}n/\sqrt{\log n}$, for all soluble transitive permutation groups G of degree $n \geq 2$, is the constant c_1 in Theorem 5.3, since $d(G) = 4$ when $n = 8$ and $G \cong D_8 \circ D_8$. We conjecture that the best "asymptotic" bound, that is, the best possible upper bound when one is permitted to exclude finitely many cases, is $d(G) \leq \lfloor \widetilde{c}n/\sqrt{\log n} \rfloor$, where $\widetilde{c}$ is some constant satisfying $b/2 \leq \widetilde{c} < b = \sqrt{2/\pi}$ (see Example 6.10 for more details).

In Section 5.1 we discuss an application of the results of Section 4 to wreath products. We reserve Section 5.2 for the proof of Theorem 5.3.

5.1 An application of the results in Section 4 to wreath products

We first make the following easy observation.

Proposition 5.4. *Let $A = T_1 \times T_2 \times \ldots \times T_f$, where each T_i is isomorphic to the nonabelian finite simple group T. Suppose that $M \leq A$ is a subdirect product of A, and suppose that $M' \trianglelefteq M$ is also a subdirect product of A. Then $M' = M$.*

Proof. We prove the claim by induction on f, and the case $f = 1$ is trivial, so assume that $f > 1$. Since M is subdirect, each $M \cap T_i$ is normal in T_i. If $M = A$, then since the only normal subgroups of A are the groups $\prod_{i \in Y} T_i$, for $Y \subseteq \{1, \ldots, f\}$, the result is clear. So assume that $M \cap T_i = 1$ for some i. Then $M' \cap T_i = 1$, and $M'T_i/T_i$ and MT_i/T_i are subdirect products of $\prod_{j \neq i} T_j$. It follows, using the inductive hypothesis, that $M'T_i = MT_i$. Hence $M' = M$, since $M \cap T_i = 1$, and the proof is complete. □

We also need the following result of Lucchini and Menegazzo.

Theorem 5.5 (**[25] and [27]**). *Let L be a proper minimal normal subgroup of the finite group G. Then $d(G) \leq d(G/L) + 1$. Furthermore, if L is the unique minimal normal subgroup of G, then $d(G) \leq \max\{2, d(G/L)\}$.*

We will now fix some notation which will be retained for the remainder of the section.

- Let R be a finite group (we do not exclude the case $R = 1$).
- Let S be a transitive permutation group of degree $s \geq 2$.
- Let G be a large subgroup of the wreath product $R \wr S$ (see Definition 2.3).
- Write $B := R_{(1)} \times R_{(2)} \times \ldots \times R_{(s)}$ for the base group of $R \wr S$.
- write $\pi : G \to S$ for the projection homomorphism onto the top group.
- Let $H := N_G(R_{(1)}) = \pi^{-1}(\mathrm{Stab}_S(1))$.
- Let $\Omega := H\backslash G$.
- Let $K := G \cap B = \mathrm{core}_G(H) = \mathrm{Ker}_G(\Omega)$.

Recall that for a subgroup N of R, $B_N \cong N^s$ denotes the direct product of the distinct S-conjugates of N. In particular, if $N \trianglelefteq R$, then $B_N \trianglelefteq R \wr S$. Throughout, we will view R as a subgroup of B by identifying R with $R_{(1)}$. We also note that

- $|G : H| = s$; and
- $S = G^{\Omega}$.

In particular, the notation is consistent with the notation introduced at the beginning of Section 4.3.

Remark 5.6. The results in this section will be obtained by applying the results in Section 4 with $H = H_1$ and $d = 1$ (see the notation introduced at the beginning of Section 4.3).

Remark 5.7. If R is a transitive permutation group, acting on a set Δ, then G is an imprimitive permutation group acting on the set $\Delta \times \{1, 2, \ldots, s\}$, and $H = \mathrm{Stab}_G((\Delta, 1))$. Furthermore $H^\Delta = R$, since G is large (see Remark 2.7).

Our strategy for proving Theorem 5.3 can now be summarised as follows:

Step 1: Show that K is "built" from induced modules for G, and non-abelian G-chief factors.

Step 2: Derive bounds on $d(G)$ in terms of the factors from Step 1 and $d(S)$.

Step 3: Use Theorem 5.5, together with the results from Section 4, to bound the contributions from the factors in Step 1 to the bound from Step 2.

Step 4: Use induction to bound $d(S)$.

We begin with Step 1.

Lemma 5.8. *Suppose that $R > 1$ and that $1 := N_0 \leq N_1 \leq \ldots \leq N_e = R$ is a normal series for R, where each factor is either elementary abelian, or a nonabelian chief factor of R. Consider the corresponding normal series $1 := G \cap B_{N_0} \leq G \cap B_{N_1} \leq \ldots \leq G \cap B_{N_e} = G$ for G. Let $V_i := N_i/N_{i-1}$ and $M_i := G \cap B_{N_i}/G \cap B_{N_{i-1}}$.*

(i) If V_i is elementary abelian, then M_i is a submodule of the induced module $V_i \uparrow_H^G$.

(ii) If V_i is a nonabelian chief factor of R, then M_i is either trivial, or a nonabelian chief factor of G.

Proof. Assume first that V_i is elementary abelian, of order p^a say. Then $B_{N_i}/B_{N_{i-1}}$ is a module for G of dimension $as = a|G : H|$ over the finite field of order p. Furthermore, $B_{N_i}/B_{N_{i-1}}$ is generated, as a G-module, by the H-module V_i. It now follows from [1, Corollary 3, Page 56] that $B_{N_i}/B_{N_{i-1}}$ is isomorphic to the induced module $V_i \uparrow_H^G$. This proves (i).

Next, suppose that V_i is a nonabelian chief factor of R. Write bars to denote reduction modulo $B_{N_{i-1}}$. Then $\overline{G}$ is a large subgroup of the wreath product $\overline{R} \wr S$, and $\overline{N_i}$ is a nonabelian minimal normal subgroup of $\overline{R}$. So we just need to prove that $\overline{G} \cap \overline{B_{N_i}}$ is either trivial or a nonabelian minimal normal subgroup of $\overline{G}$. To this end, consider the projection maps

$$\overline{\rho_j} : N_{\overline{G}}(\overline{R_{(j)}}) \to \overline{R_{(j)}}$$

defined in (2.1.1). Suppose that M is a normal subgroup of $\overline{G}$ contained in $\overline{G} \cap \overline{B_{N_i}}$. Then $M \leq N_{\overline{G}}(\overline{R_{(1)}})$, and hence $\overline{\rho_1}(M)$ is a normal subgroup of $\overline{\rho_1}(N_{\overline{G}}(\overline{R_{(1)}})) = \overline{R_{(1)}}$ contained in the minimal normal subgroup of $\overline{R_{(1)}}$ corresponding to $\overline{N_i}$. If $\overline{\rho_1}(M) = 1$ then $\overline{\rho_j}(M) = 1$ for all j, since $\pi(\overline{G}) = S$ is transitive. Hence, in this case, we have $M = 1$. Otherwise, $\overline{\rho_1}(M) \cong \overline{N_i}$, and M is a subdirect product of s copies of $\overline{N_i}$. In this case, since a minimal normal subgroup of a finite group is a direct product of simple groups, we must have $M = \overline{G} \cap \overline{B_{N_i}}$ by Proposition 5.4. Thus, if $\overline{G} \cap \overline{B_{N_i}}$ is non-trivial, then $\overline{G} \cap \overline{B_{N_i}}$ is a nonabelian minimal normal subgroup of $\overline{G}$, as required. □

For the remainder of this section, suppose that $1 := N_0 \leq N_1 \leq \ldots \leq N_e = R$ is a chief series for R, and let $V_i := N_i/N_{i-1}$ and $M_i := G \cap B_{N_i}/G \cap B_{N_{i-1}}$. If V_i is abelian we will also write $|V_i| = p_i^{a_i}$, for p_i prime.

We now have Step 2.

Corollary 5.9. *We have*

$$d(G) \leq \sum_{V_i \text{ abelian}} d_G(M_i) + c_{nonab}(R) + d(S)$$

Proof. We will prove the corollary by induction on $|R|$. If $|R| = 1$ then the bound is trivial, since $G \cong S$ in that case, so assume that $|R| > 1$, and note that

$$G/M_1 \text{ is a large subgroup of } (R/V_1) \wr S. \tag{5.1}$$

Suppose first that V_1 is abelian. Then M_1 is a G-module, so

$$d(G) \leq d_G(M_1) + d(G/M_1).$$

Since $c_{nonab}(R) = c_{nonab}(R/V_1)$, (5.1) and the inductive hypothesis give the result.

So we may assume that V_1 is nonabelian. Then M_1 is either trivial or a minimal normal subgroup of G, by Lemma 5.8 Part (ii). Hence, $d(G) \leq d(G/M_1) + 1$ by Theorem 5.5. The result now follows, again from (5.1) and the inductive hypothesis. □

Before stating our next corollary, we refer the reader to Definition 4.21 for a reminder of the definitions of the functions E and E_{sol}. The next two corollaries deal with Step 3.

Corollary 5.10. *Define E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise. Then*

(i) $d(G) \leq \sum_{V_i \text{ abelian}} a_i E'(s, p_i) + c_{nonab}(R) + d(S)$.

(ii) Suppose that $|R| = 2$ and $s = 2^m q$, where q is odd, and that S has a tuple of primitive components $X = (R_2, \ldots, R_t)$, where $\mathrm{bl}_{X,2}(S) \geq 1$. Let Γ be a full set of blocks for S of size $2^{\mathrm{bl}_{X,2}(S)}$, and set $\widetilde{S} := S^\Gamma$. Then

$$d(G) \leq \sum_{i=0}^{\mathrm{bl}_{X,2}(S)} E'(2^{m-i}q, 2) + d(\widetilde{S}).$$

(iii) Suppose that $|R| = 2$ and $s = 2^m 3$, and that S contains no soluble transitive subgroups. Then by Corollary 3.12 there exists a Mersenne prime $p_1 = 2^a - 1$ and a triple of integers (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that

(1) $m = ea + t$, and;

(2) There exists a subgroup N of G, such that N^Ω is soluble and has 2^{e+t_1} orbits, with $\binom{e}{k}2^{t_1}$ of them of length $3p_1^k \times 2^{t-t_1}$, for each $0 \leq k \leq e$.

Here, we have

$$d(G) \leq \sum_{k=0}^{e} 2^{t-t_1} \binom{e}{k} E_{sol}(3p_1^k 2^{t_1}, 2) + d(S).$$

Proof. By Corollary 5.9, we have

$$d(G) \leq \sum_{V_i \text{ abelian}} d_G(M_i) + c_{nonab}(R) + d(S).$$

Now, by Corollary 4.26, $d_G(M_i) \leq a_i E'(s, p_i)$. This proves (i).

To prove (iii) first note that, by Corollary 3.12, and as mentioned in the statement of (iii), there exists a Mersenne prime $p_1 := 2^a - 1$, and a triple (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that

(i) $m = ea + t$, and;

(ii) There exists a subgroup N of G, such that N^Ω is soluble and has 2^{e+t_1} orbits, with $\binom{e}{k}2^{t_1}$ of them of length $3p_1^k \times 2^{t-t_1}$, for each $0 \leq k \leq e$.

Note that, since $|R| = 2$, the base group $K \leq R^s$ of G is soluble. Hence, since $N^\Omega \cong N/N \cap K$ is soluble, it follows that N itself is also soluble. Corollary 4.25 Part (ii)(b) (with $ad = 1$) then implies that

$$d_G(M_1) \leq \sum_{k=0}^{e} 2^{t_1} \binom{e}{k} E_{sol}(3p_1^k 2^{t-t_1}, 2)$$

Since $|R| = 2$, we have $d(G) \leq d_G(M_1) + d(S)$, and the result follows.

Finally, we prove Part (ii). We will show that

$$d(S) \leq \sum_{i=1}^{\mathrm{bl}_{X,2}(S)} E(2^{m-i}q, 2) + d(\widetilde{S}) \tag{5.2}$$

by induction on $\mathrm{bl}_{X,2}(S)$. The result will then follow, since $d(G) \leq E'(2^m q, 2) + d(S)$ by Part (i). Now, by hypothesis, S has a tuple of primitive components $X = (R_2, \ldots, R_t)$. Also, $|R_2| = 2$ since $\mathrm{bl}_{X,2}(S) \geq 1$. Hence, by Theorem 2.5, S is a large subgroup of a wreath product $R_2 \wr S_2$, where either $S_2 = 1$, or S_2 is a transitive permutation group of degree $2^{m-1}q$, with a tuple $Y := (R_3, \ldots, R_t)$ of primitive components. If $S_2 = 1$ then the result follows, since $s = 4$ and $\widetilde{S} = 1$ in that case. So assume that $S_2 > 1$. By Part (i), we have

$$d(S) \leq E'(2^{m-1}q, 2) + d(S_2) \tag{5.3}$$

If $\mathrm{bl}_{X,2}(S) = 1$ then $S_2 = \widetilde{S}$ and (5.2) follows from (5.3). So assume that $\mathrm{bl}_{X,2}(S) > 1$. Then $\mathrm{bl}_{Y,2}(S_2) = \mathrm{bl}_{X,2}(S) - 1 \geq 1$. The inductive hypothesis then yields $d(S_2) \leq \sum_{i=1}^{\mathrm{bl}_{Y,2}(S_2)} E(2^{m-1-i}q, 2) + d(\widetilde{S}) = \sum_{i=2}^{\mathrm{bl}_{X,2}(S)} E(2^{m-i}q, 2) + d(\widetilde{S})$. The bound (5.2) now follows immediately from (5.3), which completes the proof. □

The next corollary will be key in our proof of Theorem 5.3 when G is imprimitive with minimal block size 4.

Corollary 5.11. *Assume that $R = S_4$ or $R = A_4$. Define E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise. Then*

$$d(G) \leq E'(s,2) + \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\} + E'(s,3) + d(S).$$

Proof. Let $\Delta := \{1,2,3,4\}$, so that R is transitive on Δ. We have $V_1 \cong 2^2$, $V_2 \cong 3$, and $V_3 \cong 2$ if $R \cong S_4$. Since K^Δ is a normal subgroup of $H^\Delta = R$ (see Remark 5.7), K^Δ is isomorphic to either 2^2, A_4, or S_4. In the first two cases M_3 is trivial, so

$$d(G) \leq d_G(M_1) + d_G(M_2) + d(S) \leq 2E'(s,2) + E'(s,3) + d(S)$$

by Corollaries 5.9 and 4.26. So assume that $K^\Delta \cong S_4$. Then a Sylow 3-subgroup P_3 of K^Δ acts transitively on the non-identity elements of V_1. Thus, $\chi(P_3 \cap K, V_1^*) = 1$, so

$$d_G(M_1) \leq \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\}$$

by Corollary 4.25 Parts (iii) and (iv), with $(p,q) := (2,3)$. The result follows. □

5.2 The proof of Theorem 5.3

In this section, we prove Theorem 5.3. First, we deal with Step 4: the inductive step. As mentioned at the beginning of Section 5, the cases where $\mathrm{bl}_2(G)$ is large are the most difficult to deal with using our methods. In these cases, we have $d(G) \leq E(s,2) + d(S)$ and usually the bounds on $d(S)$ which come from the inductive hypothesis then suffice to prove the theorem. However in some small cases the inductive hypothesis does not suffice, and we have to work harder. These cases, of which there are finitely many, are the subject of Appendix A, and include both the exceptional cases from Theorem 5.3 (Table A.2), and some additional cases which have a large 2-part (Table A.1). The purpose of Lemma 5.12 is to prove that the bounds in Appendix A hold.

Throughout this section, we retain the same notation as introduced immediately following Theorem 5.5, with one additional assumption: that R is a primitive permutation group of degree $r \geq 2$. Hence, G is a transitive permutation group of degree $n := rs$, and Remark 5.7 applies. Also, set E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise.

Recall also that $p_i^{a_i}$ denote the orders of the abelian chief factors of R, for p_i prime.

Lemma 5.12. *Assume that Theorem 5.3 holds for degrees less than n. Then*

(i) The bounds in Table A.1 (see Appendix A) hold, and;

(ii) If n and f are as in Table A.2, and either

(a) G contains a soluble transitive subgroup; or

(b) $\mathrm{bl}_2(G) < f$,

then $d(G) \leq \lfloor c_1 n/\sqrt{\log n}\rfloor$, where $c_1 = \frac{\sqrt{3}}{2}$.

(iii) If n and f are as in Table A.2, and

(a) G contains no soluble transitive subgroup; and

(b) $\mathrm{bl}_2(G) \geq f$,

then, the bounds in Table A.2 (Appendix A) hold.

Proof. We first recall some bounds which will be used throughout the proof. We have

$$d(G) \leq s\lfloor \log r \rfloor + d(S), \text{ if } r \geq 4; \text{ and} \tag{5.4}$$

$$d(G) \leq \sum_i a_i E'(s, p_i) + c_{nonab}(R) + d(S). \tag{5.5}$$

These bounds follow from Corollary 2.12 and Corollary 5.10 Part (i) respectively.

To bound $d(S)$ above, we use the database of transitive groups of degree up to 32 in MAGMA ([10]) if $2 \leq s \leq 32$; otherwise, we use either the previous rows of Tables A.1 and A.2; or the bound $d(S) \leq \lfloor c_1 s/\sqrt{\log s} \rfloor$ (from the hypothesis of the lemma) if s is not in Tables A.1 or A.2.

We will first prove (i) and (ii).

(i) and (ii) The values of n occurring in Table A.1 are $n = 2^m$ for $6 \leq m \leq 11$; $n = 2^{m+1}3$ for $3 \leq m \leq 19$; $n = 2^m 5$ for $3 \leq m \leq 16$; and $n = 2^m 15$ for $2 \leq m \leq 14$. We distinguish a number of cases. Recall that $n = rs$. Throughout, we define $E'' := E_{sol}$ if s is of the form $s = 2^m$, and $E'' := E$ otherwise. (Note that a transitive group of prime power degree always contains a soluble transitive subgroup.)

1. $r > 16$. Then $d(G) \leq s\lfloor \log r \rfloor + d(S)$ by (5.4). Combining this with the bounds on $d(S)$ described above gives the required for each n in Table A.1, and each possible pair (r, s) with $r > 16$ and $n = rs$, except when $(n, r, s) = (3145728, 24, 131072)$. However, each primitive group of degree 24 is either simple, or has a simple normal subgroup of index 2 (using the MAGMA [5] database). Hence, in this case, (5.5), together with the hypothesis of the lemma, gives $d(G) \leq E(s, 2) + 1 + \lfloor c_1 s/\sqrt{\log s} \rfloor = 52895$. This gives us what we need.
2. $r = 2$. We distinguish two sub-cases.
   (a) S contains a soluble transitive subgroup. Then $d(G) \leq E_{sol}(s, 2) + d(S)$ by (5.5), and this, together with the bounds on $d(S)$ described above gives the bounds in Table A.1 in each of the relevant cases.
   (b) S contains no soluble transitive subgroups. Then s is not of the form $s = 2^m$. We distinguish each of the relevant cases.
      i $s = 2^m 3$, for some $3 \leq m \leq 19$. By using the MAGMA database [5], we see that each transitive permutation group of degree 24 contains a soluble transitive subgroup, so we must have $s = 2^m 3 \geq 48$. In particular, $4 \leq m \leq 19$. By Corollary 5.10 Part (iii) there exists a Mersenne prime $p_1 = 2^a - 1$ and a triple of integers (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that $m = ea + t$, and

$$d(G) \leq \sum_{k=0}^{e} 2^{t-t_1} \binom{e}{k} E_{sol}(3p_1^k 2^{t_1}, 2) + d(S). \tag{5.6}$$

Since $4 \leq m \leq 19$, the possibilities for n and the triple (a, e, t) are as follows:

Table 5.1	
n	(a, e, t)
48	$(3,1,1)$
96	$(3,1,2)$, $(5,1,0)$
192	$(3,1,3)$, $(3,2,0)$, $(5,1,1)$
384	$(3,1,4)$, $(3,2,1)$, $(5,1,2)$, $(7,1,0)$
768	$(3,1,5)$, $(3,2,2)$, $(5,1,3)$, $(7,1,1)$
1536	$(3,1,6)$, $(3,2,3)$, $(3,3,0)$, $(5,1,4)$, $(7,1,2)$
3072	$(3,1,7)$, $(3,2,4)$, $(3,3,1)$, $(5,1,5)$, $(7,1,3)$, $(5,2,0)$
6144	$(3,1,8)$, $(3,2,5)$, $(3,3,2)$, $(5,1,6)$, $(7,1,4)$, $(5,2,1)$
12288	$(3,1,9)$, $(3,2,6)$, $(3,3,3)$, $(3,4,0)$, $(5,1,7)$, $(7,1,5)$, $(5,2,2)$

Table 5.1 ctd.	
n	(a, e, t)
24576	$(3,1,10)$, $(3,2,7)$, $(3,3,4)$, $(3,4,1)$, $(5,1,8)$, $(7,1,6)$, $(13,1,0)$, $(5,2,3)$
49152	$(3,1,11)$, $(3,2,8)$, $(3,3,5)$, $(3,4,2)$, $(5,1,9)$, $(7,1,7)$, $(13,1,1)$, $(5,2,4)$, $(7,2,0)$
98304	$(3,1,12)$, $(3,2,9)$, $(3,3,6)$, $(3,4,3)$, $(3,5,0)$, $(5,1,10)$, $(7,1,8)$, $(13,1,2)$, $(5,2,5)$, $(7,2,1)$, $(5,3,0)$
196608	$(3,1,13)$, $(3,2,10)$, $(3,3,7)$, $(3,4,4)$, $(3,5,1)$, $(5,1,11)$, $(7,1,9)$, $(13,1,3)$, $(5,2,6)$, $(7,2,2)$, $(5,3,1)$

Table 5.1 ctd.	
n	(a, e, t)
393216	$(3,1,14)$, $(3,2,11)$, $(3,3,8)$, $(3,4,5)$, $(3,5,2)$, $(5,1,12)$, $(7,1,10)$, $(13,1,4)$, $(17,1,0)$, $(5,2,7)$, $(7,2,3)$, $(5,3,2)$
786432	$(3,1,15)$, $(3,2,12)$, $(3,3,9)$, $(3,4,6)$, $(3,5,3)$, $(3,6,0)$, $(5,1,13)$, $(7,1,11)$, $(13,1,5)$, $(17,1,1)$, $(5,2,8)$, $(7,2,4)$, $(5,3,3)$
1572864	$(3,1,16)$, $(3,2,13)$, $(3,3,10)$, $(3,4,7)$, $(3,5,4)$, $(3,6,1)$, $(5,1,14)$, $(7,1,12)$, $(13,1,6)$, $(17,1,2)$, $(19,1,0)$, $(5,2,9)$, $(7,2,5)$, $(5,3,4)$

Going through each of the relevant values of n in the first column of Table A.1, each triple (a, e, t) in the last column of Table 5.1, and each possible value of $t_1 \leq t$, with $n/2 = 2^{ea+t}3$, the required bound follows from (5.6) each time.

ii $s = 2^m 5$, for some $2 \leq m \leq 15$; or $s = 2^m 15$ for some $1 \leq m \leq 14$. Then the bound $d(G) \leq E(s, 2) + d(S)$, together with the bounds on $d(S)$ described above, give the bounds in Table A.1 in each case.

3. $r = 3$. Here, $d(G) \leq E''(s,3) + E''(s,2) + d(S)$, and the bounds from Table A.1 follow in each case from applying the usual upper bounds on $d(S)$.

4. $r = 4$. Then

$$d(G) \leq E''(s,2) + \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\} + E''(s,3) + d(S) \tag{5.7}$$

by Corollary 5.11. Combining this with the bounds on $d(S)$ described above again gives the bound from the second column of Table A.1 for each of the values of n in the first column, as required.

5. $r = 5$. The possible lists of chief factors of the primitive group R of degree 5 can be obtained from the MAGMA database [5]. In particular, applying (5.5) yields

$$d(G) \leq 2E''(s,2) + E''(s,5) + d(S).$$

Again, combining this with the bounds on $d(S)$ described above yields the required bound from Table A.1 in each case.

6. $r = 6$. Again, we take the possible lists of chief factors of the primitive group R of degree 6 from the MAGMA database [5], and apply (5.5). We get

$$d(G) \leq E''(s,2) + 1 + d(S).$$

Combining this with the bounds on $d(S)$ described above yields the required bound from Table A.1 in each of the relevant cases.

7. $r = 8$. After obtaining the possible chief factors of R from the MAGMA database, we again apply (5.5) and get

$$d(G) \leq 3E''(s,2) + E''(s,3) + E''(s,7) + d(S).$$

Using the above with the bounds on $d(S)$ described previously gives the required bound from Table A.1 in each case.

8. $10 \leq r \leq 16$. In each case, we use the same approach as in the previous case, so to avoid being too repetitive we will just check the $r = 16$ case. Again we can take the possible lists of chief factors of the primitive groups R of degree 16 from the MAGMA database, and apply (5.5). We get

$$d(G) \leq 7E''(s,2) + E''(s,3) + \max\{E''(s,3), E''(s,5)\} + d(S).$$

As before, combining this with the usual bounds for $d(S)$ gives the bounds in Table A.1 in each case.

(iii) We now consider the bounds in Table A.2., i.e. the exceptional cases from Theorem 5.3. Thus, either $n = 2^m 5$ and $17 \leq m \leq 26$, or $n = 2^m 15$ and $15 \leq m \leq 35$. Note that $0 \leq \mathrm{bl}_2(G) \leq m$.

If $\mathrm{bl}_2(G) = 0$ then (5.4) for $r > 16$, and (5.5) for $2 < r \leq 16$, as in our proofs in **(i) and (ii)** above yields the required bounds in each case.

So assume that $\mathrm{bl}_2(G) \geq 1$. Then

$$d(G) \leq \sum_{i=1}^{\mathrm{bl}_2(G)} E(2^{m-i}5, 2) + d(\widetilde{S}) \tag{5.8}$$

where $\widetilde{S}$ is transitive of degree $2^{m-\mathrm{bl}_2(G)}v$, by Corollary 5.10 Part (ii).

Now, fix a transitive permutation group G of degree n where n is one of the values from the first column of Table A.2. Suppose first that $\mathrm{bl}_2(G) \leq f$, where f is the corresponding value to n in the second column of Table A.2. To bound $d(\widetilde{S})$ above, we use the database of transitive permutation groups of degree up to 32 in MAGMA (see [10]) if $2 \leq 2^{m-\mathrm{bl}_2(G)}v \leq 32$; otherwise, we use the previous rows of Tables A.1 and A.2. Combining these bounds for $d(\widetilde{S})$ with (5.8) yields $d(G) \leq \lfloor c_1 n/\sqrt{\log n} \rfloor$ in each case, as required.

If G contains a soluble transitive subgroup, then the bound at (5.8) with E replaced by E_{sol} holds, and yields $d(G) \leq \lfloor c_1 n/\sqrt{\log n} \rfloor$ in each case, as needed.

So we may assume that $\mathrm{bl}_2(G) > f$, and that G contains so soluble transitive subgroups. In particular, the bound at (5.8) again holds. If $\widetilde{S}$ is primitive of degree $2^{m-\mathrm{bl}_2(G)}v$, then the bound $d(\widetilde{S}) \leq \lfloor \log(2^{m-\mathrm{bl}_2(G)}v) \rfloor$ of Theorem 2.11 gives us the required bound in Table A.2 in each case. So assume that $\widetilde{S}$ is imprimitive, with minimal block size $\widetilde{r} > 2$. Also, write $\widetilde{s} := 2^{m-f_G}v/\widetilde{r}$. With (r, s) replaced by $(\widetilde{r}, \widetilde{s})$, we can now apply (5.4) if $\widetilde{r} > 16$, and (5.5) for $2 < r \leq 16$, as in cases (i) and (ii) above. (Note that $d(\widetilde{S})$ is bounded above using the database of transitive permutation groups of degree up to 32 in MAGMA (see [10]) if $2 \leq \widetilde{s} \leq 32$). This gives us the required bound in Table A.2 in each case. (We perform these calculations for each possible value of f_G, and each pair $(\widetilde{r}, \widetilde{s})$ with $\widetilde{r} > 2$ and $2^{m-f_G}v = \widetilde{r}\widetilde{s}$.) This completes the proof.

□

We are now ready to prove Theorem 5.3.

Proof of Theorem 5.3. The proof is by induction on n. Suppose first that G is primitive. The result clearly holds when $n \leq 3$. When $n \geq 4$, we have $\log n \leq c_1 n/\sqrt{\log n}$, so the result follows immediately from Theorem 2.11. This can serve as the initial step.

The inductive step concerns imprimitive G. For this, we now use the notation introduced immediately following Theorem 5.5. Write V_i for the abelian chief factors of R, and write $|V_i| = p_i^{a_i}$. Recall that $a(R)$ denotes the composition length of R. In particular, $a(R) \geq \sum_i a_i + c_{nonab}(R)$. The

inductive hypothesis, together with the bounds obtained in Corollaries 4.27 and 2.12, give

$$d(G) \leq \left\lfloor \frac{2a(R)s}{c' \log s} \right\rfloor + \left\lfloor \frac{c_1 s}{\sqrt{\log s}} \right\rfloor \qquad \text{(if } 2 \leq s \leq 1260\text{)} \tag{5.9}$$

$$d(G) \leq \left\lfloor \frac{a(R)b\sqrt{2}s}{\sqrt{\log s}} \right\rfloor + \left\lfloor \frac{cs}{\sqrt{\log s}} \right\rfloor \qquad \text{(if } s \geq 1261\text{)} \tag{5.10}$$

$$d(G) \leq \left\lfloor \frac{a(R)\frac{2}{c'}s}{\sqrt{\log s}} \right\rfloor + \left\lfloor \frac{cs}{\sqrt{\log s}} \right\rfloor \qquad \text{(for all } s \geq 2\text{)} \tag{5.11}$$

$$d(G) \leq s\lfloor \log r \rfloor + \left\lfloor \frac{cs}{\sqrt{\log s}} \right\rfloor \qquad \text{(for } r \geq 4,\ s \geq 2\text{)} \tag{5.12}$$

respectively. Note that (5.9) and (5.10) follow from Corollaries 4.27 and 5.10 Part (i), and together imply (5.11), while (5.12) follows from Corollary 2.12. Recall that we need to prove that $d(G) \leq c_1 rs/\sqrt{\log rs}$ for all cases apart from those listed in Theorem 5.3 Part (2).

Suppose first that $r \geq 481$. Then (5.11), together with Theorem 2.10, gives

$$d(G) \leq \frac{([(2 + c_0)\log r - (1/3)\log 24]\frac{2}{c'} + c)s}{\sqrt{\log s}}.$$

This is less than $c_1 rs/\sqrt{\log rs}$ for $r \geq 481$ and $s \geq 2$, which gives us what we need.

So we may assume that $2 \leq r \leq 480$. Suppose first that $10 \leq r \leq 480$, and consider the function

$$f(e, z, w) = \frac{(eb\sqrt{2} + c)\sqrt{z + w}}{2^z \sqrt{w}}$$

defined on triples of positive real numbers. Clearly when the pair (e, z) is fixed, f becomes a decreasing function of w. We distinguish two sub-cases:

(a) $s \geq 1261$. For each of the cases $10 \leq r \leq 480$, we compute the maximum value $a_{prim}(r)$ of the composition lengths of the primitive groups of degree r, using MAGMA. Each time, we get $f(a_{prim}(r), \log r, \log s) \leq f(a_{prim}(r), \log r, \log 1261)$
$< c_1$, and the result then follows, in each case, from (5.10).

(b) $2 \leq s \leq 1260$. For each fixed r, $10 \leq r \leq 480$, and each s, $2 \leq s \leq 1260$, we explicitly compute $\min\{\lfloor 2a_{prim}(r)s/(c' \log s)\rfloor, s\lfloor \log r \rfloor\} + \lfloor c_1 s/\sqrt{\log s}\rfloor$. Each time, except when $r = 16$ and $72 \leq s \leq 1260$, this integer is less than or equal to $\lfloor c_1 rs/\sqrt{\log rs}\rfloor$, which, after appealing to the inequalities at (5.9) and (5.12), gives us what we need. If $r = 16$, and $72 \leq s \leq 1260$, we have $d(G) \leq 7E(s, 2) + 2E(s, 3) + \lfloor c_1 s/\sqrt{\log s}\rfloor$, by Corollary 5.10 Part (i), and this gives the required bound in each case (the chief factors of the primitive groups of degree 16 are computed using MAGMA - see Table B.2).

Finally, we deal with the cases $2 \leq r \leq 9$. In considering each of the relevant cases, we take the possible lists of chief factors of R from the MAGMA database. In each case, we bound $d(S)$ above by using the database of transitive permutation groups of degree up to 32 in MAGMA (see [10]) if $2 \leq s \leq 32$, Lemma 5.12 if s is in the left hand column of Table A.1 or Table A.2, or the inductive hypothesis otherwise.

(a) $r = 2$. Corollary 5.10 Part (i) gives $d(G) \leq E(s,2) + d(S)$. Write $s = 2^m q$, where q is odd, and assume first that $s < 10^{66}$. Assume first that $\mathrm{lpp}(q) \geq 19$. Then $d(G) \leq s/19 + d(S)$, and the bounds on $d(S)$ described above, yield $d(G) \leq 2c_1 s/\sqrt{\log 2s}$ for $s < 10^{66}$. So assume further that $\mathrm{lpp}(q) \leq 17$. Then q is of the form $q = 3^{l_3}5^{l_5}7^{l_7}11^{l_{11}}13^{l_{13}}17^{l_{17}}$, where $0 \leq l_3 \leq 2$, and $0 \leq l_i \leq 1$, for $i = 5$, 7, 11, 13 and 17. Fix one such q. Then $0 \leq m \leq m(q) := \lfloor \log(10^{66}/q) \rfloor$, and $d(G) \leq E(2^m q, 2) + d(S)$. Now, by using the upper bounds on $d(S)$ described above, we get $d(G) \leq 2c_1 s/\sqrt{\log 2s}$, for each of the 96 possible values of q, and each $0 \leq m \leq m(q)$. This gives us what we need.

Thus, we may assume that $s \geq 10^{66}$. We distinguish two sub-cases.

(i) $s_2 \geq s^{858/1000}$. Then $E(s,2) \leq bs/\sqrt{\log s_2} \leq bs\sqrt{1000/858}/\sqrt{\log s}$. Hence, $d(G) \leq bs\sqrt{1000/858}/\sqrt{\log s} + c_1 s/\sqrt{\log s}$, and this is less than or equal to $2c_1 s/\sqrt{\log 2s}$ for $s \geq 10^{66}$, as required.

(ii) $s/s_2 \geq s^{142/1000}$. Then, by Lemma 2.17, we have

$$E(s,2) \leq s/(c' \log(s/s_2)) \leq (1000/142)s/c' \log s,$$

and hence $d(G) \leq (1000/142)s/(c' \log s) + c_1 s/\sqrt{\log s}$. Again, this is less than or equal to $2c_1 s/\sqrt{\log 2s}$, for $s \geq 10^{66}$.

(b) $r = 3$. Here, Corollary 5.10 Part (i) gives $d(G) \leq E(s,3) + E(s,2) + d(S)$. Using the bounds for $d(S)$ described above, this gives us what we need whenever $2 \leq s \leq 5577$, and whenever S is one of the exceptional cases listed in Theorem 5.3 Part (2))in these cases, we take the bounds for $d(S)$ from Table A.2). Otherwise, $s \geq 5578$, and we use Corollary 4.27 to distinguish two cases, with $\alpha = 1/3$.

(i) $s_2,\ s_3 \leq s^{1/3}$. Then $d(G) \leq 3s/(c' \log s) + c_1 s/\sqrt{\log s}$, and this is less than or equal to $3c_1 s/\sqrt{\log 3s}$ for $s \geq 3824$.

(ii) $s_2 \geq s^{1/3}$, or $s_3 \geq s^{1/3}$. Then $\mathrm{lpp}(s/s_3) \geq s^{1/3}$ or $\mathrm{lpp}(s/s_2) \geq s^{1/3}$, so $d(G) \leq b\sqrt{3}s/\sqrt{\log s} + s^{2/3} + c_1 s/\sqrt{\log s}$, and this is at most $3c_1 s/\sqrt{\log 3s}$, for $s \geq 5578$.

(c) $r = 4$. Here Corollary 5.11 implies that

$$d(G) \leq E(s,2) + \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\} + E(s,3) + d(S). \tag{5.13}$$

Using the bounds on $d(S)$ described above, this yields the required upper bound whenever S is one of the exceptional cases of Theorem 5.3 Part (2), and whenever $7 \leq s \leq 49435925$. When $2 \leq s \leq 6$, G is transitive of degree $4s$, and the result follows by using Table B.1. So assume that $s \geq 115063$, and that s is not one of those cases listed in Theorem 5.3 Part (2). We distinguish three cases.

(i) $s_2,\ s_3 \leq s^{21/50}$. Then $d(G) \leq (200/29)s/(c' \log s) + c_1 s/\sqrt{\log s}$ by Corollary 4.27 (with $alpha = 21/50$), and this is less than or equal to $4c_1 s/\sqrt{\log 4s}$ for $s \geq 49435925$, as needed.

(ii) $s_2 \geq s^{21/50}$. Then $E(s,2) \leq \sqrt{50/21}bs/\sqrt{\log s}$, and $E(s,3) \leq s/\operatorname{lpp}(s/s_3) \leq s/s_2 \leq s^{29/50}$. Hence, $d(G) \leq 2\sqrt{50/21}bs/\sqrt{\log s} + s^{29/50} + c_1 s/\sqrt{\log s}$ by (5.13). This is at most $4c_1 s/\sqrt{\log 4s}$, for $s \geq 28090868$.

(iii) $s_3 \geq s^{21/50}$. Then $d(G) \leq \sqrt{50/21}bs/\sqrt{\log s} + 2s^{29/50} + c_1 s/\sqrt{\log s}$ using a similar argument to (ii) above. This is less than or equal to $4c_1 s/\sqrt{\log 4s}$, for $s \geq 56$. This completes the proof of the theorem in the case $r = 4$.

(d) $r = 5$. Corollary 5.10 Part (i) gives $d(G) \leq E(s,5) + 2E(s,2) + d(S)$. Again, this gives us what we need for each s in the range $3 \leq s \leq 552$, and each exceptional S. Also, $s = 2$ implies that G is transitive of degree 10, and the result follows from Table B.1. Thus, we may assume that $s \geq 553$. Applying Corollary 4.27, with $\alpha = 2/5$, yields three cases.

(i) $s_2,\ s_5 \leq s^{2/5}$. Then $d(G) \leq 5s/(c' \log s) + c_1 s/\sqrt{\log s}$, which is less than or equal to $5c_1 s/\sqrt{\log 5s}$ for $s \geq 553$, as required.

(ii) $s_2 \geq s^{2/5}$. Then $d(G) \leq 2b\sqrt{5/2}s/\sqrt{\log s} + s^{3/5} + c_1 s/\sqrt{\log s}$, and this is no greater than $5c_1 s/\sqrt{\log 5s}$ when $s \geq 139$.

(iii) $s_5 \geq s^{2/5}$. Then $d(G) \leq b\sqrt{5/2}s/\sqrt{\log s} + 2s^{3/5} + c_1 s/\sqrt{\log s}$, which is less than or equal to $5c_1 s/\sqrt{\log 5s}$ for $s \geq 17$.

(e) $r = 6$. Here, Corollary 5.10 Part (i), together with the inductive hypothesis, gives $d(G) \leq E(s,2)+1+d(S)$. Using the usual bounds on $d(S)$, this is at most $\lfloor 6cs/\sqrt{\log 6s} \rfloor$ for $2 \leq s \leq 1260$, and whenever S is one of the exceptional cases. Otherwise, $s \geq 1261$, and $d(S) \leq c_1 s/\sqrt{\log s}$. Hence, by Corollary 4.27 Part (iii), $d(G) \leq b\sqrt{2}s/\sqrt{\log s} + 1 + c_1 s/\sqrt{\log s}$, which is less than or equal to $6c_1 s/\sqrt{\log 6s}$ for $s \geq 2$. This completes the proof of the theorem in the case $r = 6$.

(f) $r = 7$. Here, $d(G) \leq E(s,2) + E(s,3) + E(s,7) + d(S)$, again using Corollary 5.10 Part (i). Bounding $d(S)$ as described previously, this is at most $\lfloor 7c_1 s/\sqrt{\log 7s} \rfloor$ for each s in the range $2 \leq s \leq 1260$, and each exceptional S. Otherwise, $s \geq 1261$, and by Corollary 4.27 Part (iii) $d(G) \leq 3b\sqrt{2}s/\sqrt{\log s} + c_1 s/\sqrt{\log s}$. This is less than $7c_1 s/\sqrt{\log 7s}$ for $s \geq 7$, and, again, we have what we need.

(g) $r = 8$. Using Corollary 5.10 Part (i), $d(G) \leq 3E(s,2) + E(s,3) + E(s,7) + d(S)$. In each of the cases $2 \leq s \leq 272$, and each exceptional case, this bound, together with the bounds on $d(S)$ described above, give us what we need. Thus, we may assume that $s \geq 273$. Then the inductive hypothesis gives $d(S) \leq c_1 s/\sqrt{\log s}$, and applying Corollary 4.27, with $\alpha = 37/100$, yields three cases.

(i) $\max\{s_2, s_3, s_7\} \leq s^{37/100}$. Then $d(G) \leq (500/63)s/(c' \log s) + c_1 s/\sqrt{\log s}$, which is less than or equal to $8c_1 s/\sqrt{\log 8s}$ for $s \geq 273$, as required.

(ii) $s_2 \geq s^{37/100}$. Then $d(G) \leq 3b\sqrt{100/37}s/\sqrt{\log s} + 2s^{63/100} + c_1 s/\sqrt{\log s}$, and this is no greater than $8c_1 s/\sqrt{\log 8s}$ when $s \geq 98$.

(iii) $\max\{s_3, s_7\} \geq s^{37/100}$. Then $d(G) \leq 2b\sqrt{100/37}s/\sqrt{\log s} + 3s^{63/100} + c_1 s/\sqrt{\log s}$, which is less than or equal to $8c_1 s/\sqrt{\log 8s}$ for $s \geq 27$.

(h) $r = 9$. By Corollary 5.10 Part (i), $d(G) \leq 4E(s,2) + 3E(s,3) + d(S)$. When $3 \leq s \leq 2335$, and when S is one of the exceptional cases, this bound, together with the usual bounds on $d(S)$, give us what we need. If $s = 2$, then G is transitive of degree 18, and the result follows from Table A.1. Otherwise, $s \geq 2336$, and $d(S) \leq c_1 s/\sqrt{\log s}$, using the inductive hypothesis. We now use Corollary 4.27 to distinguish three cases, with $\alpha = 37/100$.

(i) $s_2,\ s_3 \leq s^{37/100}$. Then $d(G) \leq (700/63)s/(c' \log s) + c_1 s/\sqrt{\log s}$, and this is less than or equal to $9c_1 s/\sqrt{\log 9s}$ for $s \geq 2336$, as needed.

(ii) $s_2 \geq s^{37/100}$. Then $d(G) \leq 4b\sqrt{100/37}s/\sqrt{\log s} + 3s^{63/100} + c_1 s/\sqrt{\log s}$, which is no larger than $9cs/\sqrt{\log 9s}$, whenever $s \geq 1197$.

(iii) $s_3 \geq s^{37/100}$. Here, $d(G) \leq 3b\sqrt{100/37}s/\sqrt{\log s} + 4s^{63/100} + c_1 s/\sqrt{\log s}$, and this is less than or equal to $9c_1 s/\sqrt{\log 9s}$ for $s \geq 148$.

This completes the proof of Theorem 5.3. □

6 The proof of Theorem 1.7

In proving Theorem 1.7, we will omit reference to the constant C, and just use the Vinogradov notation defined immediately after Definition 4.29. We will now restate some results from Sections 2, 3 and 4 in this language for the convenience of the reader.

We begin with Theorems 2.10 and 1.1.

Theorem 6.1. *Let R be a primitive permutation group of degree r. Then $a(R) \ll \log r$.*

Theorem 6.2. *Let S be a transitive permutation group of degree $s \geq 2$. Then $d(S) \ll s/\sqrt{\log s}$.*

We also note the following useful consequence of Corollaries 5.9 and 4.27, and Theorem 6.2.

Corollary 6.3. *Let R be a finite group, let S be a transitive permutation group of degree $s \geq 2$, and let G be a large subgroup of the wreath product $R \wr S$. Then*

$$d(G) \ll \frac{a(R)s}{\sqrt{\log s}}.$$

Theorem 2.11 reads as follows in Vinogradov notation.

Theorem 6.4 ([19], Theorem 1.1). *Let H be a subnormal subgroup of a primitive permutation group of degree r. Then $d(H) \ll \log r$.*

Finally, we will need the following theorem of Cameron, Solomon and Turull; note that we only give a simplified version of their result here.

Theorem 6.5 ([9], Theorem 1). *Let G be a permutation group of degree $n \geq 2$. Then $a(G) \ll n$.*

6.1 Orders of transitive permutation groups

We now turn to bounds on the order of a transitive permutation group G, of degree n. First, we fix some notation which will be retained for the remainder of the section. Let G be a transitive permutation group of degree n, and let $(R_1, \ldots, R_t)$ be a tuple of primitive components for G, where each R_i is primitive of degree r_i, and $\prod_i r_i = n$. Furthermore, we will write π_1 for the identity map $G \to G$, and for $i \geq 2$, we will write π_i to denote the projection $\pi_i : G\pi_{i-1} \leq R_{i-1} \wr (R_i \wr R_{i+1} \wr \ldots \wr R_t) \to R_i \wr R_{i+1} \wr \ldots \wr R_t$.

The following is a simplified version of a theorem of C. Praeger and J. Saxl [33] (which was later improved by A. Maróti in [30]).

Theorem 6.6 ([33], Main Theorem). *Let G be a primitive permutation group of degree r, not containing* $\mathrm{Alt}(r)$. *Then* $\log |G| \ll r$.

Since the symmetric and alternating groups are 2-generated, the next corollary follows immediately from Theorems 6.4 and 6.6.

Corollary 6.7. *Let G be a subnormal subgroup of a primitive permutation group of degree r. Then $d(G) \log |G| \ll r \log r$.*

6.2 The proof of Theorem 1.7

Before proceeding to the proof of Theorem 1.7, we require an application of the results in Section 5.1. First, we need a preliminary lemma.

Lemma 6.8. *Let R and S be transitive permutation groups of degree $r \geq 2$ and $s \geq 1$ respectively, let D be a subgroup of* $\mathrm{Sym}(d)$ *containing* $\mathrm{Alt}(d)$, *let P be a large subgroup of the wreath product $D \wr S$, and let G be a large subgroup of $R \wr P$. Also, write U_i for the abelian chief factors of R. Suppose that $d \geq 5$. Then*

(i) There exists a large subgroup Q of the wreath product $R \wr D$, and an embedding $\theta : G \to Q \wr S$, such that $G\theta$ is a large subgroup of $Q \wr S$.

(ii) Let $H := N_Q(R_{(1)})$. Then Q has a normal series

$$1 = N_0 \leq N_1 \leq \ldots < N_t < N_{t+1} \leq N_{t+2} = Q,$$

where for each abelian U_i with $i \leq t$, N_i/N_{i-1} is contained in the Q-module $U_i \uparrow_H^Q$; and for each non-abelian U_i with $i \leq t$, N_i/N_{i-1} is either trivial or a non-abelian chief factor of Q. Also, $N_{t+1}/N_t \cong \mathrm{Alt}(d)$, and $|N_{t+2}/N_{t+1}| \leq 2$.

Proof. Note first that G is an imprimitive permutation group of degree rds, with a block Δ_1 of size r, by Remark 2.4. Now, by Remark 2.7, G is also a subgroup of the wreath product $X := (R \wr D) \wr S$. Hence, G also has a block of size rd, again using Remark 2.4. Let Δ be a block of size rd containing Δ_1. Let $H_1 := \mathrm{Stab}_G(\Delta_1)$ and $H := \mathrm{Stab}_G(\Delta) = N_Q(R_{(1)})$. Then $H_1 \leq H$, and Δ_1 is a block for H^Δ of size r, with block stabiliser H_1^Δ. Let Γ_1 be the set of H-translates of Δ_1, and let Γ be the set of G-translates of Δ. Then G is a large subgroup of $H^\Delta \wr G^\Gamma$, while H^Δ is a large subgroup of

$H_1^{\Delta_1} \wr H^{\Gamma_1}$, by Theorem 2.5. By Definition 2.3, $H_1^{\Delta_1} \cong R$. Thus, to complete the proof of Part (i) we just need to show that $H^{\Gamma_1} \cong D$ and $G^{\Gamma} \cong S$ (we then take $Q = H^{\Delta}$).

First, let $\pi : G \leq R \wr P \to P$ denote projection over the top group. Note that $H\pi \leq P$ is a permutation group of degree ds, stabilising a block of size d. Furthermore, since $\mathrm{Ker}(\pi) = \mathrm{core}_G(H_1) \leq H_1 \leq H$, we have $s = |G : H| = |G\pi : H\pi|$. Thus, $H\pi$ is the full (set-wise) stabiliser of a block for P of size d. It follows that $H^{\Gamma_1} \cong D$, since P is large in $D \wr S$.

Since $\mathrm{Ker}(\pi) = \mathrm{Ker}_G(\Delta_1^G) \leq \mathrm{Ker}_G(\Gamma)$, we have $G^{\Gamma} \cong \pi(G)^{\Gamma} = P^{\Gamma} = S$, as needed. Finally, since Q is a large subgroup of $R \wr D$, and $D \cong \mathrm{Alt}(d)$ or $D \cong \mathrm{Sym}(d)$, Part (ii) follows from Lemma 5.8. □

The mentioned application can now be given as follows.

Proposition 6.9. *Let R be a finite group, let S be a transitive permutation group of degree $s \geq 2$, let D be a subgroup of $\mathrm{Sym}(d)$ containing $\mathrm{Alt}(d)$, let P be a large subgroup of the wreath product $D \wr S$, and let G be a large subgroup of $R \wr P$. Also, let K_1 be the kernel of the action of $P \leq D \wr S$ on a set of blocks of size d, and let A be the induced action of K_1 on a fixed block Δ for P. Assume that $A \neq 1$, that $d \geq 5$, and set $g(d, s) := \max\{1, \frac{d}{\sqrt{\log s}}\}$. Then*

(i) $d(G) \ll a(R)s$; and

(ii) $d(G) \ll \frac{a(R)g(d,s)s}{\sqrt{\log s}}$.

Proof. Let U_i, for $1 \leq i \leq t$ say, denote the chief factors of R. Also, if U_i is abelian, write $|U_i| = p_i^{a_i}$, for p_i prime. By Lemma 6.8 Part (i), G is a large subgroup of $Q \wr S$, where Q is a large subgroup of $R \wr D$. Let $H_1 := N_Q(R_{(1)})$. By Lemma 6.8 Part (ii), Q has a normal series

$$1 = N_0 \leq N_1 \leq \ldots \leq N_t < N_{t+1} \leq N_{t+2} = Q,$$

where each abelian factor N_i/N_{i-1}, for $i \leq t$, is contained in the Q-module $U_i \uparrow_{H_1}^{Q}$, and each nonabelian factor is a chief factor of Q. Also, $N_{t+1}/N_t \cong \mathrm{Alt}(d)$, and $|N_{t+2}/N_{t+1}| \leq 2$. In particular,

$$c_{nonab}(Q) \leq c_{nonab}(R) + 1. \tag{6.1}$$

Denote by B the base group of $Q \wr S$, and consider the corresponding normal series

$$1 = G \cap B_{N_0} \leq G \cap B_{N_1} \leq G \cap B_{N_2} \leq \ldots \leq G \cap B_{N_t} \tag{6.2}$$

$$< G \cap B_{N_{t+1}} \leq G \cap B_{N_{t+2}} = G \cap B \tag{6.3}$$

for $G \cap B$. Let M_i be the abelian factors in (6.2). Then

$$d(G) \ll \sum_{U_i \text{ abelian}} d_G(M_i) + c_{nonab}(R) + \frac{s}{\sqrt{\log s}} \tag{6.4}$$

by Corollary 5.9 and Theorem 6.2. Viewing G as a subgroup of $Q \wr S$, let $H := N_G(Q_{(1)})$. Also, let $\pi : R \wr P \to P$ denote projection over the top group. Since $H\pi \leq P$ stabilises a block of size d, we may assume, without loss of generality, that

$$H\pi = \mathrm{Stab}_P(\Delta)$$

(recall that Δ is a block of size d for $P \leq D \wr S$). Note also that M_i is a submodule of the induced module $U_i \uparrow_{H_1}^{H} \uparrow_{H}^{G} \cong U_i \uparrow_{H_1}^{G}$, by Lemmas 5.8 and 6.1.

Fix i in the range $1 \leq i \leq t$ such that U_i is abelian. Suppose first that $s_{p_i} \leq \sqrt{s}$. Then Corollary 4.27 Part (ii), with $\alpha := 1/2$, gives

$$d_G(M_i) \ll \frac{a_i d s}{\log s} \leq \frac{a_i g(d,s) s}{\sqrt{\log s}} \tag{6.5}$$

Assume next that $s_{p_i} > \sqrt{s}$ for some fixed i. Let $K := \mathrm{core}_G(H)$. Note that $K\pi = K_1 \leq P$, since $H\pi = \mathrm{Stab}_P(\Delta)$ is a block stabiliser. Then

$$1 < A = (K\pi)^{\Delta} \trianglelefteq (H\pi)^{\Delta} = D,$$

so $(K\pi)^{\Delta} \geq \mathrm{Alt}(d)$. Hence, Proposition 4.30 Part (ii) implies that

$$d_G(M_i) \ll \frac{a_i s}{\sqrt{\log s_{p_i}}} \leq \frac{\sqrt{2} a_i s}{\sqrt{\log s}} \ll \frac{a_i g(d,s) s}{\sqrt{\log s}}. \tag{6.6}$$

Thus, (6.4), (6.5) and (6.6) yield:

$$\begin{aligned} d(G) &\ll \sum_{U_i \text{ abelian}} \frac{a_i g(d,s) s}{\sqrt{\log s}} + c_{nonab}(R) + \frac{s}{\sqrt{\log s}} \\ &\ll \frac{a(R) g(d,s) s}{\sqrt{\log s}} + \frac{s}{\sqrt{\log s}} \\ &\ll \frac{a(R) g(d,s) s}{\sqrt{\log s}} + \frac{g(d,s) s}{\sqrt{\log s}} \ll \frac{a(R) g(d,s) s}{\sqrt{\log s}} \end{aligned}$$

and this proves Part (ii).

Finally, 6.4 and Proposition 4.30 Part (i) give

$$\begin{aligned} d(G) &\ll \sum_{U_i \text{ abelian}} a_i s + c_{nonab}(R) + \frac{s}{\sqrt{\log s}} \\ &\ll a(R) s + \frac{s}{\sqrt{\log s}} \ll a(R) s \end{aligned}$$

and this completes the proof. □

We are now ready to prove Theorem 1.7.

Proof of Theorem 1.7. Let $f(G) = d(G) \log |G| \sqrt{\log n}/n^2$. We will prove, by induction on n, that $f(G) \ll 1$. If G is primitive, then $f(G) \ll (\log n)^{3/2}/n$ by Corollary 6.7, and the claim follows.

For the inductive step, assume that G is imprimitive. Fix a tuple $(R_1, R_2, \ldots, R_t)$ of primitive components for G, where each R_i is primitive of degree r_i, say. Also, for $1 \leq i \leq t-1$, let Δ_i be a block of size r_i for $\pi_i(G) \leq R_i \wr \pi_{i+1}(R_i)$, and denote by A_i the induced action of $\mathrm{Ker}_{\pi_i(G)}(\{{\Delta_i}^g : g \in \pi_i(G)\})$ on Δ_i (in particular, note that $A_i \trianglelefteq R_i$). Finally, set $A_t := \pi_t(G)$.

Then

$$|G| \leq \prod_{i=1}^{t} |A_i|^{\frac{n}{r_1 \dots r_i}} \tag{6.7}$$

Next, for $1 \leq i \leq t$, we define the functions f_i as follows

$$f_i(G) := \frac{d(G) n \log |A_i| \sqrt{\log n}}{r_1 r_2 \dots r_i n^2} = \frac{d(G) \log |A_i| \sqrt{\log n}}{r_1 r_2 \dots r_i n} \tag{6.8}$$

The inequality at 6.7 then yields $f(G) \leq \sum_{i=1}^{t} f_i(G)$. We claim that $f_i(G) \ll \frac{(i-1)}{2^{i-1}}$ for $2 \leq i \leq t$, and that $f_1(G) \ll 1$ (the implied constants here are independent on i). The result will then follow. Indeed, in this case, $f(G) \ll \sum_{i=1}^{\infty} \frac{i-1}{2^{i-1}} \ll 1$.

To this end, first fix i in the range $2 \leq i \leq t$. Clearly we may assume that A_i is non-trivial. Let $D = R_i$, $S := \pi_i(G)$, and note that G is a large subgroup of a wreath product $R \wr P$, where R is transitive of degree $r := r_1 r_2 \dots r_{i-1}$, and P is a large subgroup of $D \wr S$. Set $d := r_i$, $s := r_{i+1} \dots r_t$, and $m := \max\{r, d, s\}$. Suppose first that $d \geq 5$ and that D contains the alternating group $\mathrm{Alt}(d)$. (In particular, we are in the "bottom heavy" situation of Proposition 6.9.) Then A_i, being a nontrivial normal subgroup of D, also contains $\mathrm{Alt}(d)$. Note that $|A_i| \leq d^d$. We distinguish two cases. Note throughout that $\log n \leq \log m^3 \ll \log m$.

1. $s \leq 2^{(\log d)^2}$. Then $n = rds \leq m_1^2 2^{(\log m_1)^2}$, where $m_1 := \max\{r, d\}$. Thus, $\log n \leq 2 \log m_1 + (\log m_1)^2 \ll (\log m_1)^2$. Since $a(R) \ll r$ by Theorem 6.5, Proposition 6.9 Part (i) then implies that $d(G) \ll rs$. Hence, from 6.8 we deduce

$$f_i(G) \ll \frac{rsd \log d \log m_1}{r^2 d^2 s} = \frac{\log d \log m_1}{rd} \ll \frac{\log r}{r} \leq \frac{(i-1)}{2^{i-1}}$$

since $r \geq 2^{i-1}$, and this gives us what we need.

2. $s > 2^{(\log d)^2}$. Note that $m \in \{r, s\}$ in this case. Set $g(d, s) := \max\left\{1, \frac{d}{\sqrt{\log s}}\right\}$. Then

$$g(d, s) \log d \leq d \tag{6.9}$$

since $\sqrt{\log s} > \log d$. Now, Theorem 6.5 gives $a(R) \ll r$. Hence, Proposition 6.9 Part (ii) gives $d(G) \ll \frac{r g(d,s) s}{\sqrt{\log s}}$. Hence, since $n \leq m^3$, we have

$$\begin{aligned} f_i(G) &\ll \frac{r g(d,s) s d \log d \sqrt{\log m}}{r^2 d^2 s \sqrt{\log s}} \\ &= \frac{g(d,s) \log d \sqrt{\log m}}{rd\sqrt{\log s}} \\ &\leq \frac{d\sqrt{\log m}}{rd\sqrt{\log s}} && \text{by (6.9)}, \\ &\leq \frac{\sqrt{\log r}}{r} \leq \frac{\sqrt{i-1}}{2^{i-1}} && \text{since } m \in \{r, s\}. \end{aligned}$$

This gives us what we need.

Next, suppose that either $d \leq 4$, or that D does not contain $\mathrm{Alt}(d)$. Then $\log |A_i| \ll d$ by Theorem

6.6. Now, G is a large subgroup of $R \wr P$, where P is transitive of degree ds. Also, $a(R) \ll r$ by Theorem 6.5. Then, by Corollary 6.3 we have

$$d(G) \ll \frac{rds}{\sqrt{\log ds}}.$$

Thus

$$f_i(G) \ll \frac{rdsd\sqrt{\log m}}{r^2d^2s\sqrt{\log ds}} = \frac{\sqrt{\log m}}{r\sqrt{\log ds}} \leq \frac{\sqrt{\log r}}{r} \leq \frac{\sqrt{i-1}}{2^{i-1}}$$

and again this gives us what we need.

Finally, we deal with the case $i = 1$. Here, set $r := r_1$, $s := r_2r_3 \dots r_t$, and $m = \max\{r, s\}$. Then $|A_i| \leq r^r$ and $\log n \ll \log m$. Also, G is a large subgroup of a wreath product $R \wr S$, where R is primitive of degree r, and S is transitive of degree s. Thus, $a(R) \ll \log r$ by Theorem 6.1. Thus, Corollary 6.3 implies that $d(G) \leq s \log r/\sqrt{\log s}$, and hence

$$f_i(G) \ll \frac{(\log r)sr \log r\sqrt{\log m}}{r^2s\sqrt{\log s}} = \frac{(\log r)^2\sqrt{\log m}}{r\sqrt{\log s}} \leq \frac{(\log r)^{5/2}}{r} \ll 1.$$

This completes the proof. □

We conclude with an example which shows that the bounds of Theorems 5.3 and 1.7 are asymptotically best possible.

Example 6.10. Let A be an elementary abelian group of order 2^{2k-1}, and write R for the radical of the group algebra $\mathbb{F}_2[A]$. Consider the 2-group $G := R^{k-1} \rtimes A$.

The largest trivial submodule of $\mathbb{F}_2[A]$ is 1-dimensional, while $\dim(R^{k-1}) > 1$, by [21, 3.2]. Hence, the centraliser $C_A(R^{k-1})$ of R^{k-1} in A is a proper characteristic subgroup of A; since A is characteristically simple, it follows that $C_A(R^{k-1}) = 1$. Thus, $C_G(R^{k-1}) = R^{k-1}$, so $Z := Z(G) = C_{R^{k-1}}(A)$. Again, since the largest trivial submodule of $\mathbb{F}_p[A]$ is 1-dimensional, and Z is nontrivial, it follows that Z has order 2, and hence Z is the unique minimal normal subgroup of G. Let H be a subspace complement to Z in R^{k-1}. Then H has codimension 1 in R^{k-1}, and hence has index 2^{2k} in G. It is also clear that H is core-free in G, so G is a transitive permutation group of degree 2^{2k}.

Next, note that

$$\sqrt{2k}\binom{2k}{k}\frac{1}{4^k} = \left[\frac{1}{2}\left(\frac{3}{2}\frac{3}{4}\right)\left(\frac{5}{4}\frac{5}{6}\right)\cdots\left(\frac{2k-1}{2k-2}\frac{2k-1}{2k}\right)\right]^{1/2} = \left[\frac{1}{2}\prod_{j=2}^{k}\left(1+\frac{1}{4j(j-1)}\right)\right]^{1/2}.$$

As in the proof of Theorem 1.3, the expression in the middle converges to $b = \sqrt{2/\pi}$, by Wallis' formula. Hence, since the expression on the right is increasing, we conclude that for all $\epsilon > 0$, there exists a positive integer k such that $\sqrt{2k}\binom{2k}{k}\frac{1}{4^k} \geq b - \epsilon$, that is, $\binom{2k}{k} \geq (b-\epsilon)4^k/\sqrt{2k}$.

Now, the derived subgroup G' of G is R^k, and $G/G' \cong (R^{k-1}/R^k) \times A$ is elementary abelian of rank $\binom{2k-1}{k-1} + 2k - 1$, again using [21, 3.2]. Thus, for large enough k we have

$$d(G) = \binom{2k-1}{k-1} + 2k - 1 = \frac{1}{2}\binom{2k}{k} + 2k - 1 \geq \frac{(b-\epsilon)2^{2k}}{2\sqrt{2k}} + 2k - 1.$$

Furthermore, $|R^{k-1}| = 2^{\sum_{i=k-1}^{2k-1}\binom{2k-1}{i}} = 2^{2^{2k-1}-2^{k-2}} \sim 2^{n/2}$. Hence, $|G| \sim 2^{n-1}$, which shows that $d(G)\log|G|$ is at least a constant times $n^2/\sqrt{\log n}$.

Appendices

A Upper bounds for $d(G)$ for some transitive groups of small degree

The groups G in the right hand column of Table A.1 below are transitive permutation groups of degree d, where d is as specified in the left hand column. In Table A.2, the groups are transitive permutation groups of degree d which have at least f 2-blocks (see Section 1).

Table A.1	
d	$d(G) \leq$
48	16
64	20
96	31
128	40
192	57
256	75
384	109
512	145
$2^8 3$	203
2^{10}	271
$2^9 3$	392
2^{11}	523
$2^{10} 3$	738

Table A.1 ctd	
d	$d(G) \leq$
$2^{11} 3$	1431
$2^{12} 3$	2718
$2^{13} 3$	5292
$2^{14} 3$	10118
2153	19770
$2^{16} 3$	38002
$2^{17} 3$	74467
$2^{18} 3$	143750
$2^{19} 3$	282317
$2^{20} 3$	546854
$2^3 5$	9
$2^4 5$	18
$2^5 5$	34

Table A.1 ctd	
d	$d(G) \leq$
$2^6 5$	66
$2^7 5$	130
$2^8 5$	258
$2^9 5$	514
$2^{10} 5$	1026
$2^{11} 5$	2050
$2^{12} 5$	4098
$2^{13} 5$	8194
$2^{14} 5$	16386
$2^{15} 5$	32770
$2^{16} 5$	65538
$2^2 15$	15

Table A.1 ctd	
d	$d(G) \leq$
$2^3 15$	27
$2^4 15$	52
$2^5 15$	100
$2^6 15$	196
$2^7 15$	388
$2^8 15$	772
$2^9 15$	1540
$2^{10} 15$	3076
$2^{11} 15$	6148
$2^{12} 15$	12292
$2^{13} 15$	24580
$2^{14} 15$	49156

Table A.2		
d	f	$d(G) \leq$
$2^{17} 5$	5	130900
$2^{18} 5$	4	257722
$2^{19} 5$	4	504220
$2^{20} 5$	4	984067
$2^{21} 5$	4	1919461
$2^{22} 5$	4	3745164
$2^{23} 5$	5	7312620
$2^{24} 5$	5	14290701
$2^{25} 5$	6	27953017
$2^{26} 5$	7	54725580
$2^{15} 15$	6	98308

Table A.2 ctd		
d	f	$d(G) \leq$
$2^{16} 15$	4	196612
$2^{17} 15$	3	392700
$2^{18} 15$	3	773166
$2^{19} 15$	3	1512660
$2^{20} 15$	3	2952202
$2^{21} 15$	3	5758386
$2^{22} 15$	3	11235497
$2^{23} 15$	3	21937865
$2^{24} 15$	3	42872110
$2^{25} 15$	3	83859059

Table A.2 ctd		
d	f	$d(G) \leq$
$2^{26} 15$	4	164176748
$2^{27} 15$	4	321692696
$2^{28} 15$	4	630835627
$2^{29} 15$	4	1237980292
$2^{30} 15$	5	2431149936
$2^{31} 15$	5	4777379825
$2^{32} 15$	5	9393534359
$2^{33} 15$	6	18480443646
$2^{34} 15$	7	36376783048
$2^{35} 15$	8	71639170628

References

[1] Alperin, J.L. *Local Representation Theory.* Cambridge University Press, Cambridge, 1986.

[2] Anderson, I. On primitive sequences. *J. London Math. Soc.* **42** (1967) 137-148.

[3] Babai, L.; Sòs, V.T. Sidon sets in groups and induced subgraphs of Cayley graphs. *Europe. J. Combin.* **6(2)** (1985) 101-114.

[4] Benson, D.J. *Representations and Cohomology: Volume 1, Basic Representation Theory of Finite Groups and Associative Algebras*. Cambridge University Press, Cambridge, 1998.

[5] Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997) 235-265.

[6] Bray, J. N.; Holt, D. F.; Roney-Dougal, C. M. *The maximal subgroups of the low-dimensional finite classical groups*. London Math. Soc., Lecture Note Series 407, Cambridge, 2013.

[7] Bryant, R.M.; Kovács, L.G.; Robinson, G.R. Transitive permutation groups and irreducible linear groups. *Quart J. Math.* **46** (1995) 385-407.

[8] Cameron, P.J. *Permutation Groups*, London Math. Soc. (Student Texts), vol. 45, CUP, Cambridge, 1999.

[9] Cameron, P.J.; Solomon, R.G.; Turull, A. Chains of subgroups in symmetric groups. *J. Algebra* **127** (1989) 340-352.

[10] Cannon, J.J.; Holt, D.F. The transitive permutation groups of degree up to 32. *Experimental Math.* **17** (2008) 307-314.

[11] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A. *An ATLAS of Finite Groups*. Clarendon Press, Oxford, 1985; reprinted with corrections 2003.

[12] Curtis, C.W.; Reiner, I. *Representation Theory of Finite Groups and Associative Algebras: Volume I*, Wiley, New York, 1988.

[13] Dalla Volta, F.; Siemons, J. On Solvable Minimally Transitive Permutation Groups. *Codes, Designs, Cryptography* **44** nn. 1-3 (2007) 143-150.

[14] de Bruijn, N.G.; van Ebbenhorst Tengbergen, Ca.; Kruyswijk, D. On the set of divisors of a number. *Nieuw Arch. Wiskunde* **23** (1951) 191-193.

[15] Dilworth, R.P. A decomposition theorem for partially ordered sets. *Ann. of Math.* **51(2)** (1950) 161-166.

[16] Doerk, K.; Hawkes, T. *Finite Soluble Groups*. de Gruyter, Berlin, 1992.

[17] Erdos, P. A Theorem of Sylvester and Schur. *J. London Math. Soc.* **9** (1934) 282-288.

[18] Gorenstein, D. *Finite Groups*. Harper and Row, New York, 1968.

[19] Holt, D.F.; Roney-Dougal, C.M. Minimal and random generation of permutation and matrix groups. *J. Algebra* **387** (2013) 195-223.

[20] Isaacs, I.M. *Character Theory of Finite Groups*. Dover, New York, 1994.

[21] Kovács, L.G.; Newman, M.F. Generating transitive permutation groups. *Quart. J. Math. Oxford* (2) **39** (1988) 361-372.

[22] Kleidman, P.; Liebeck, M. W. *The subgroup structure of the finite classical groups*. CUP, Cambridge, 1990.

[23] Kopylova, T.I. Solvable minimal transitive groups of permutations of degree pq. (Russian) *VestsīAkad. Navuk BSSR Ser. Fīz.-Mat. Navuk* **(6) 126** (1985) 5460.

[24] Liebeck, M. W.; Praeger, C. E.; Saxl, J. Transitive subgroups of primitive permutation groups. *J. Algebra* **234** (2000) 291-361.

[25] Lucchini, A. Generators and minimal normal subgroups. *Arch. Math* **64** (1995) 273-276.

[26] Lucchini, A. Enumerating transitive finite permutation groups. *Bull. London Math. Soc.* **30** (1998) 569-577.

[27] Lucchini, A.; Menegazzo, F. Generators for finite groups with a unique minimal normal subgroups *Rend. Sem. Math. Univ. Padova* **98** (1997) 173-191.

[28] Lucchini, A.; Menegazzo, F.; Morigi, M. Asymptotic results for transitive permutation groups. *Bull. London. Math. Soc.* **32** (2000) 191-195.

[29] Lucchini, A.; Menegazzo, F.; Morigi, M. On the number of generators and composition length of finite linear groups. *J. Algebra* **243** (2001) 227-247.

[30] Maroti, A. On the orders of primitive groups. *J. Algebra* **258 (2)** (2002) 631-640.

[31] Neumann, P.M.; Vaughan-Lee, M.R. An essay on BFC-groups. *Proc. London. Math. Soc.* **35** (1977), 213237.

[32] Pálfy, P.P. A polynomial bound for the orders of primitive solvable groups. *J. Algebra* **77** (1982) 127-137.

[33] Praeger, C.; Saxl, J. On the order of primitive permutation groups. *Bull. London Math. Soc.* **12** (1980) 303-308.

[34] Pyber, L. Asymptotic results for permutation groups. *Groups and Computation* DIMACS Ser. Discrete Math. Theoret. Computer Sci. **11** (ed. Finkelstein, L. and Kantor, W.M., Amer. Math. Soc., Providence, 1993) 197-219.

[35] Pyber, L. Enumerating finite groups of given order. *Ann. Math.*, **(2) 137** (1993), 203220.

[36] Rosser, J.B.; Schoenfeld, L. Approximate formulas for some functions of prime numbers. *Illinois J. Math.* **6** (1962) 64-97.

[37] Shepperd, J.A.M.; Wiegold, J. Transitive groups and groups with finite derived groups. *Math. Z.* **81** (1963) 279-285.

[38] Tracey, G.M. Generating minimally transitive permutation groups. *J. Algebra* **460** (2016) 380-386.

[39] Suprunenko, D.A. *Matrix Groups.* Translations of Mathematical Monographs, 45. Amer. Math. Soc., Providence, 1976.

[40] Suprunenko, D.A. Solvable minimal transitive permutation groups of degree pq. *Soviet. Math. Dokl.* **27** (1986) 337-340.

[41] Wallis, J. *Arithmetica Infinitorum.* Oxford, England, 1656.