Permutation groups, simple groups, and sieve methods

D.R. Heath-Brown
Mathematical Institute
24-29, St. Giles'
Oxford, OX1 3LB
England

Cheryl E. Praeger
School of Mathematics and Statistics
University of Western Australia
35 Stirling Highway
Crawley WA 6009
Australia

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904
Israel

April 20, 2006

Abstract

We show that the number of integers $n \leq x$ which occur as indices of subgroups of nonabelian finite simple groups, excluding that of A_{n-1} in A_n, is $\sim hx/\log x$, for some given constant h. This might be regarded as a noncommutative analogue of the Prime Number Theorem (which counts indices $n \leq x$ of subgroups of abelian simple groups).

We conclude that for most positive integers n, the only quasiprimitive permutation groups of degree n are S_n and A_n in their natural action. This extends a similar result for primitive permutation groups obtained by Cameron, Neumann and Teague in 1982.

Our proof combines group-theoretic and number-theoretic methods. In particular we use the classification of finite simple groups, and we also apply sieve methods to estimate the size of some interesting sets of primes.

Research partially supported the Australian Research Council for C.E.P. and by the Bi-National Science Foundation United States-Israel Grant 2000-053 for A.S.

2000 *Mathematics Subject Classification: 20B05, 20D06*

1 Introduction

By the Prime Number Theorem there are $O(x/\log x)$ integers $n \leq x$ which are primes, that is, orders of abelian finite simple groups. As a result of the Classification of the nonabelian finite simple groups and their order formulae one concludes easily that $O(x/\log x)$ integers $n \leq x$ occur as orders of finite simple groups.

In 1982 Cameron, Neumann and Teague [CNT] showed that $O(x/\log x)$ integers $n \leq x$ occur as indices $|G : M|$, where G is a finite simple group, M is a maximal subgroup of G, and $(G, M) \neq (A_n, A_{n-1})$ for any $n \geq 5$. It follows from our first theorem that the same conclusion holds if the condition that M is maximal is removed.

The major motivation of Cameron, Neumann and Teague in proving their theorem about simple groups was to study finite permutation groups. They applied their result to prove that the set of degrees n of primitive permutation groups, other than A_n and S_n, has density zero in the natural numbers. Like them, our principal focus is the degree set of certain families of permutation groups. We show in Theorems 1.5 and 1.6 that the sets of degrees n of quasiprimitive permutation groups and of innately transitive permutation groups, other than A_n and S_n, also have density zero.

Our proofs combine various tools from group theory and number theory. We adopt standard number-theoretic notation. In particular $\pi(x)$ denotes the number of primes $\leq x$, ϕ denotes the Euler function, and for real functions f, g we write $f \sim g$ if $f(x)/g(x) \to 1$ as $x \to \infty$.

Define a constant h by

$$h = \sum_{d=1}^{\infty} \frac{1}{d\phi(2d)}.$$

It is easy to prove that $h < \infty$, and computer estimates can be used to show that $h = 1.763085...$ We are grateful to John Bamberg and Devin Kilminster for this computation.

For a subset $N \subseteq \mathbb{N}$ and a real number $x > 1$, set $N(x) = |\{n \in N \mid n \leq x\}|$.

Define

$$\begin{aligned} I &= \{|G : H| \mid G \text{ a finite nonabelian simple group, } H < G, \text{ and} \\ &\quad (G, H) \neq (A_n, A_{n-1})\}. \end{aligned}$$

We can now state our first main result.

Theorem 1.1 *With the above notation we have*

$$I(x) \sim h\frac{x}{\log x}.$$

Theorem 1.1 follows from two more detailed results. In order to state them we need more definitions. For an odd prime p let $S(p)$ denote the set of subgroups H of $\mathrm{PSL}(2,p)$ which are contained in a parabolic subgroup and contain a Sylow p-subgroup. Thus $H \in S(p)$ is a semidirect product of a cyclic group of order p with a cyclic group of order dividing $(p-1)/2$.

Let

$$I_1 \;=\; \{|\mathrm{PSL}(2,p) : H| \mid p \text{ an odd prime}, H \in S(p)\},$$

and

$$\begin{aligned} I_2 \;=\; &\{|G:H| \mid G \text{ a finite nonabelian simple group, } H < G, \text{ and} \\ &(G,H) \neq (A_n, A_{n-1}) \text{ or } (\mathrm{PSL}(2,p), H) \text{ with } H \in S(p)\}. \end{aligned}$$

Theorem 1.2 *With the above notation we have*

$$I_1(x) = h\frac{x}{\log x} + O(\frac{x}{(\log x)^2}).$$

Theorem 1.3 *With the above notation we have*

$$I_2(x) = O(x^{48/49}).$$

Since $I = I_1 \cup I_2$ it follows from Theorems 1.2 and 1.3 that

$$I(x) = h\frac{x}{\log x} + O(\frac{x}{(\log x)^2}).$$

In particular this implies Theorem 1.1.

To compare these results to those of [CNT], define

$$\begin{aligned} J \;=\; &\{|G:M| \mid G \text{ a finite nonabelian simple group, } M < G \text{ maximal,} \\ &\text{and } (G,M) \neq (A_n, A_{n-1})\}, \end{aligned}$$

and

$$\begin{aligned} J_2 \;=\; &\{|G:M| \mid G \text{ a finite nonabelian simple group, } M < G \text{ maximal,} \\ &(G,M) \neq (A_n, A_{n-1}), \text{ and if } G = \mathrm{PSL}(2,p) \text{ with } p \text{ prime} \\ &\text{then } |G:M| \neq p+1\}. \end{aligned}$$

Then it was is shown in [CNT] that

$$J_2(x) = \sqrt{2}x^{1/2} + O(\frac{x^{1/2}}{\log x}) = O(x^{1/2}),$$

and since $J = \{p+1 \mid p \text{ prime }\} \cup J_2$ we have

$$J(x) = \pi(x-1) + O(x^{1/2}) \sim \frac{x}{\log x}.$$

Combining this with Theorem 1.1 we obtain the following.

Corollary 1.4 *With the above notation we have*

$$J(x)/I(x) \to 1/h \text{ as } x \to \infty.$$

Hence, roughly speaking, the probability that an index of a subgroup of some finite simple group (excluding A_{n-1} in A_n) is an index of a maximal subgroup of some finite simple group (excluding A_{n-1} in A_n) is $1/h = 0.567...$

We now turn to applications to finite permutation groups. Recall that a transitive permutation group is said to be *primitive* if it does not preserve a non-trivial partition of the permutation domain. The main result of [CNT] deals with degrees of primitive permutation groups, that is, with the set

$$\mathrm{Deg}_{\mathrm{prim}} = \{n \mid \exists\ G \leq S_n,\ G \text{ primitive}, G \neq A_n, S_n\}.$$

The main result of [CNT] shows that

$$\mathrm{Deg}_{\mathrm{prim}}(x) = 2\pi(x) + (1+\sqrt{2})x^{1/2} + O(\frac{x^{1/2}}{\log x}) \sim 2\frac{x}{\log x}.$$

We extend this result to a larger family of finite permutation groups.

A permutation group G is said to be *quasiprimitive* if all the non-trivial normal subgroups of G are transitive. It is easy to see that primitive groups are quasiprimitive, but the converse does not hold. For example, all simple transitive permutation groups are quasiprimitive, but they are only primitive if a point stabilizer is a maximal subgroup.

Quasiprimitive groups arise in the study of 2-arc transitive graphs (see [Pr]) and other contexts, and it is interesting to find out which properties of primitive groups extend to quasiprimitive groups (see [PrSh]).

Let

$$\mathrm{Deg}_{\mathrm{qp}} = \{n \mid \exists\ G \leq S_n,\ G \text{ quasiprimitive}, G \neq A_n, S_n\}.$$

Recall that the density of a subset $N \subseteq \mathbb{N}$ is defined by $\limsup_{x\to\infty} N(x)/x$. Using Theorem 1.1 and an O'Nan–Scott type theorem for quasiprimitive groups [Pr] we establish the main result of this paper.

Theorem 1.5 *With the above notation we have*

$$\mathrm{Deg}_{\mathrm{qp}}(x) \sim (h+1)\frac{x}{\log x}.$$

In particular $\mathrm{Deg}_{\mathrm{qp}}$ *has density zero.*

We may therefore say that for most integers n, the only quasiprimitive permutation groups of degree n are A_n and S_n. In fact our arguments show that

$$\mathrm{Deg}_{\mathrm{qp}}(x) = (h+1)\frac{x}{\log x} + O(\frac{x}{(\log x)^2}).$$

The proof of Theorem 1.5 applies also to a larger family of transitive permutation groups, namely the family of finite innately transitive groups. A permutation group is said to be *innately transitive* if it has a transitive minimal normal subgroup. Such groups often arise as automorphism groups of arc-transitive graphs and their structure has been studied in [BPr]. In particular, every quasiprimitive group is innately transitive. We include in Section 5, a proof that:

Theorem 1.6

$$\mathrm{Deg}_{\mathrm{it}}(x) = (h+1)\frac{x}{\log x} + O(\frac{x}{(\log x)^2})$$

where

$$\mathrm{Deg}_{\mathrm{it}} = \{n \mid \exists\ G \leq S_n,\ G \textit{ innately transitive}, G \neq A_n, S_n\}.$$

The layout of this paper is as follows. Section 2 is the main number-theoretic section, devoted to the proof of Theorem 1.2. The proof of Theorem 1.3 is carried out in Sections 3 and 4, dealing with alternating groups and Lie type groups respectively. Section 5 is devoted to quasiprimitive groups and the proof of Theorems 1.5 and 1.6.

2 A problem in prime number theory

In this section we prove Theorem 1.2, counting indices $|\mathrm{PSL}(2,p) : H|$ with $H \in S(p)$. Since $|\mathrm{PSL}(2,p) : H| = d(p+1)$ where $d|(p-1)/2$, Theorem 1.2 is equivalent to the following number-theoretic result.

Theorem 2.1 *Define*

$$N(x) = |\{n \in \mathbb{N} :\ n \leq x,\ \exists\, p, d \in \mathbb{N},\ p \textit{ prime},\ n = d(p+1),\ 2d|(p-1)\}|.$$

Then

$$N(x) = h\frac{x}{\log x} + O(\frac{x}{(\log x)^2}),$$

where

$$h = \sum_{d=1}^{\infty} \frac{1}{d\phi(2d)}.$$

One can also write h as a product

$$h = \frac{4}{3}\prod_{p\geq 3} \frac{p^3 - p^2 + 1}{(p-1)(p^2-1)},$$

where p runs over the odd primes. John Bamberg and Devin Kilminster estimated the value of h using computer calculations, showing that

$$1.76308527 < h < 1.76308545.$$

In Remark 2.2 at the end of the section, we make several comments about the size of the error term, and the constant implied by the $O(\ldots)$ notation in Theorem 2.1.

To prove the theorem we begin by writing

$$\pi(x;q,a) = |\{p \le x : p \text{ prime}, \ q|(p-a)\}|$$

and

$$N_0(x) = \sum_{d \le \sqrt{x}} \pi(\frac{x}{d} - 1; 2d, 1).$$

Then by the inclusion-exclusion principle we see that

$$N(x) \le N_0(x) \tag{1}$$

and

$$N(x) \ge N_0(x) - \sum_{d < d' \le \sqrt{x}} N(x;d,d') \tag{2}$$

where

$$\begin{aligned} N(x;d,d') \quad = \quad & |\{n \in \mathbb{N} : n \le x, \exists p, p' \text{ prime}, \ n = d(p+1) = d'(p'+1), \\ & 2d|(p-1), \ 2d'|(p'-1)\}|. \end{aligned}$$

We proceed by estimating $N_0(x)$ asymptotically, and showing that the contribution from the terms $N(x;d,d')$ is negligible.

To handle $N_0(x)$ our main tool is the Siegel-Walfisz Theorem, which states that for any positive integer m there is a constant $c(m) > 0$ such that

$$\pi(N;q,a) = \frac{1}{\phi(q)} \int_2^N \frac{dt}{\log t} + O(N \exp\{-c(m)\sqrt{\log N}\})$$

uniformly for $q \le (\log N)^m$, and for $(a,q) = 1$. In fact the usual references, such as Davenport [D; Chapter 22, (4)], give the corresponding result for the closely related function $\psi(N;q,a)$, but it is an easy exercise to derive the result above from this. We shall take $m = 100$, which will be more than large enough. If $d \le (\log x)^{50}$ then $2d \le (\log(x/d))^{100}$ as soon as $x \ge x_0$, say. Moreover for such d we have

$$\sqrt{\log \frac{x}{d}} \ge \frac{1}{2}\sqrt{\log x}$$

if $x \geq x_1$, say. We also note that

$$\pi(\frac{x}{d} - 1; 2d, 1) = \pi(\frac{x}{d}; 2d, 1) + O(1).$$

Thus if $d \leq (\log x)^{50}$ we have

$$\begin{aligned}
\pi(\frac{x}{d} - 1; 2d, 1) &= \frac{1}{\phi(2d)} \int_2^{x/d} \frac{dt}{\log t} + O(\frac{x}{d} \exp\{-\frac{c(100)}{2}\sqrt{\log x}\}) + O(1) \\
&= \frac{1}{\phi(2d)}\{\frac{x/d}{\log x/d} + O(\frac{x/d}{(\log x/d)^2})\} + O(\frac{x}{(\log x)^{1000}}) \\
&= \frac{1}{\phi(2d)}\{\frac{x}{d\log x} + O(\frac{x\log 2d}{d(\log x)^2})\} + O(\frac{x}{(\log x)^{1000}}) \\
&= \frac{x}{d\phi(2d)\log x}\{1 + O(\frac{\log 2d}{\log x})\}.
\end{aligned}$$

Here we have written $2d$ in the error term merely to cater for the case $d = 1$, and in the second equality above we have used $\int_2^y \frac{dt}{\log t} = \frac{y}{\log y} + O(\frac{y}{(\log y)^2})$ and $\exp\{-\frac{c(100)}{2}\sqrt{\log x}\} = O(\frac{x}{(\log x)^{1000}})$.

To handle the ϕ function we note that for any integer m we have

$$\frac{m}{\phi(m)} \ll \log\log(3m) \ll \log(2m) \tag{3}$$

(recall that $f \ll g$ means $f = O(g)$), whence

$$\sum_{d \leq D} \frac{1}{d\phi(2d)} = \sum_{d=1}^{\infty} \frac{1}{d\phi(2d)} + O(D^{-1}\log D)$$

for $D \geq 2$ and

$$\sum_{d \leq D} \frac{\log(2d)}{d\phi(2d)} \ll 1.$$

It therefore follows that

$$\sum_{d \leq (\log x)^{50}} \pi(\frac{x}{d} - 1; 2d, 1) = \frac{x}{\log x} \sum_{d=1}^{\infty} \frac{1}{d\phi(2d)} + O(\frac{x}{(\log x)^2}).$$

Finally, to handle values $d > (\log x)^{50}$ we use the trivial bound

$$\pi(N; q, 1) \leq \frac{N}{q}$$

which shows that

$$\pi(\frac{x}{d} - 1; 2d, 1) \leq \frac{x}{2d^2}.$$

We deduce from this that the overall contribution to $N_0(x)$ arising from terms $d > (\log x)^{50}$ is $O(x(\log x)^{-50})$. It therefore follows that

$$N_0(x) = \frac{x}{\log x}\sum_{d=1}^{\infty}\frac{1}{d\phi(2d)} + O(\frac{x}{(\log x)^2}) = h\frac{x}{\log x} + O(\frac{x}{(\log x)^2}). \qquad (4)$$

We turn now to the terms $N(x;d,d')$. We begin by considering the contribution from the case $d' \geq x^{1/8}$. Since $d'(p'+1) \leq x$ this implies $p' \leq x^{7/8}$. We now observe that any positive integer $m \leq x$ has $O(x^{1/24})$ divisors. Indeed for any fixed $\varepsilon > 0$ the number of divisors of such an m is $O(x^{\varepsilon})$. Hence each value of $p' \leq x^{7/8}$ corresponds to $O(x^{1/24})$ integers $d' \geq x^{1/8}$ such that $p'(d'+1) \leq x$ and $2d' \,|\, (p'-1)$. Moreover since $d'(p'+1)$ has $O(x^{1/24})$ divisors, and since $d(p+1) = d'(p'+1)$, each pair p', d' determines $O(x^{1/24})$ pairs p, d. It follows that the total contribution to the summation in (2) arising from terms with $d' \geq x^{1/8}$ is

$$\ll x^{7/8}.\, x^{1/24}.\, x^{1/24} = x^{23/24}.$$

This is clearly satisfactory for our theorem.

Henceforth we may assume that $d < d' < x^{1/8}$. Now let $\ell = \text{h.c.f.}(d,d')$, say, and set $d = \ell k, d' = \ell k'$. If $2d \,|\, (p-1)$ and $2d' \,|\, (p'-1)$ we may write $p = 1 + 2\ell k m$ and $p' = 1 + 2\ell k' m'$, so that the condition $n = d(p+1) = d'(p'+1)$ becomes

$$k(1+\ell k m) = k'(1+\ell k' m'). \qquad (5)$$

We plan to show that p and p' take the form

$$p = a + 2\ell k k'^2 s, \quad p' = a' + 2\ell k^2 k' s, \quad s \in \mathbb{N} \cup \{0\} \qquad (6)$$

with appropriate non-negative integers a, a' depending only on k, k' and ℓ. To do this we begin by remarking that kk' is coprime to ℓ. For if q is a prime factor of both k, say, and ℓ, then if we take (5) as a congruence modulo q we deduce that $q \,|\, k'$, which would contradict the coprimality of k and k'. Thus we shall henceforth assume that $\text{h.c.f.}(kk', \ell) = 1$, as well as $\text{h.c.f.}(k,k') = 1$. We now view (5) as a congruence modulo k'^2, whence

$$\ell k^2.m \equiv k' - k \pmod{k'^2}, \qquad (7)$$

and write $m_0 = m_0(\ell, k, k')$ for the smallest non-negative solution to this congruence. It is then apparent that the entire set of solutions in non-negative integers m will be given by $m = m_0 + sk'^2$, with s running over non-negative integers. Thus p takes the form $p = 1+2\ell k m = 1+2\ell k m_0 + 2\ell k k'^2 s$, which is of the shape required for (6) on taking $a = 1 + 2\ell k m_0$. Moreover, since (7) holds with m replaced by m_0 we must have $\ell k^2 m_0 = k' - k + k'^2 m_1$, say. It is clear that m_1 must be non-negative, since

$$k' + k'^2 m_1 \quad = \quad k + \ell k^2 m_0 > 0.$$

We now find that

$$\begin{aligned} p' &= \frac{d}{d'}(p+1)-1 \\ &= \frac{k}{k'}(2+2\ell k m_0+2\ell k k'^2 s)-1 \\ &= \frac{k}{k'}(2+2\frac{k'-k+k'^2 m_1}{k}+2\ell k k'^2 s)-1 \\ &= 1+2k'm_1+2\ell k^2 k' s. \end{aligned}$$

This too is of the shape required for (6) on taking $a' = 1+2k'm_1$. This completes the proof of our assertion (6). We note for later reference that, from our definitions $a = 1+2\ell k m_0$ and $a' = 1+2k'm_1$, where $\ell k^2 m_0 = k'-k+k'^2 m_1$, it follows that

$$ak - a'k' = k' - k. \tag{8}$$

Since $d(p+1) \le x$ we see that $d.2\ell k k'^2 s \le x$, whence $s \le x/(2\ell^2 k^2 k'^2)$. It follows that

$$N(x;d,d') \le \\ |\,\{s \in \mathbb{Z} : 0 \le s \le \frac{x}{2(\ell k k')^2},\ a+2\ell k k'^2 s \text{ and } a'+2\ell k^2 k' s \text{ prime}\}\,|. \tag{9}$$

If either a or a' contains a factor in common with $2\ell k k'$ then we cannot obtain primes except, possibly, for $s = 0$. Thus we shall assume henceforth that h.c.f.$(aa', 2\ell k k') = 1$. To estimate the right-hand side of (9) we shall use a result from sieve methods, namely Theorem 4.1 of Halberstam and Richert [HR]. This result refers to a sequence $\mathcal{A}$ which we shall take to be

$$\mathcal{A} = \{(a+2\ell k k'^2 s)(a'+2\ell k^2 k' s) :\ 0 \le s \le \frac{x}{2(\ell k k')^2}\}.$$

We have also to fix a set of primes $\mathcal{P}$, which we take to be the set of all primes. Then $S(\mathcal{A};\mathcal{P},z)$ denotes the number of elements in the sequence $\mathcal{A}$ all of whose prime factors are at least z, and we will choose the value of z later. Thus if $a+2\ell k k'^2 s$ and $a'+2\ell k^2 k' s$ are both prime, the element $(a+2\ell k k'^2 s)(a'+2\ell k^2 k' s) \in \mathcal{A}$ will be counted by $S(\mathcal{A};\mathcal{P},z)$, providing that $a+2\ell k k'^2 s$ and $a'+2\ell k^2 k' s$ are both at least z. It follows that

$$N(x;d,d') \le S(\mathcal{A};\mathcal{P},z) + z.$$

We shall define an arithmetic function $\omega(c)$ to be the number of solutions s of the congruence $(a+2\ell k k'^2 s)(a'+2\ell k^2 k' s) \equiv 0 \pmod{c}$ in the range $1 \le s \le c$. Then $\omega(c)$ is multiplicative. Moreover, when c is a prime p we have

$$\omega(p) = \begin{cases} 0 & \text{if } p \,|\, 2\ell k k' \\ 1 & \text{if } p \,|\, (ak - a'k'),\ p \nmid 2\ell k k' \\ 2 & \text{otherwise.} \end{cases}$$

Thus the conditions (Ω_1) and $\Omega_2(\kappa)$ required by Halberstam and Richert hold with $\kappa = 2$. Finally we note that the number of elements in $\mathcal{A}$ which are divisible by a given number c takes the form $\omega(c)X/c + R_c$, where

$$X = 1 + \frac{x}{2(\ell k k')^2}, \quad |R_c| \leq \omega(c).$$

We are now ready to apply Halberstam and Richert [HR; Theorem 4.1], which produces

$$S(\mathcal{A}; \mathcal{P}, z) \ll XW(z) + \sum_{c \leq z^2} \mu^2(c) 3^{\nu(c)} \omega(c),$$

where

$$W(z) = \prod_{p<z} (1 - \frac{\omega(p)}{p})$$

$\mu(n)$ is the Möbius function, and $\nu(n)$ is the number of distinct prime factors of n. Since

$$(\ell k k')^2 \leq d^2.\, d'^2 \leq (x^{1/8})^4 = x^{1/2} \tag{10}$$

we see that $1 \ll x/(\ell k k')^2$, whence

$$X \ll \frac{x}{(\ell k k')^2}.$$

To estimate $W(z)$ we set $\Delta = 2\ell k k'(ak - a'k')$. Then by (8), we have

$$\Delta = 2\ell k k'(k' - k). \tag{11}$$

We now have

$$\begin{aligned} W(z) &= \prod_{p<z} (1 - \omega(p)/p) \\ &\leq \prod_{p<z,\, p \nmid \Delta} (1 - 2/p) \\ &\ll \prod_{p|\Delta} (1 - 1/p)^{-2} \prod_{p<z} (1 - 1/p)^2. \end{aligned}$$

Now, by Mertens' Theorem we have $\prod_{p<z}(1 - 1/p) \ll (\log z)^{-1}$. Thus, noting that $\prod_{p|\Delta}(1 - 1/p)^{-1} = \frac{\Delta}{\phi(\Delta)}$, this yields

$$W(z) \ll \frac{\Delta^2}{\phi(\Delta)^2} (\log z)^{-2}.$$

Since $d = \ell k < d' = \ell k'$ it is clear from (11) that $1 \leq \Delta \leq 2d'^3$. Thus (3) produces

$$\frac{\Delta^2}{\phi(\Delta)^2} \ll (\log d')^2$$

and hence

$$W(z) \ll (\frac{\log d'}{\log z})^2.$$

Finally we estimate

$$\sum_{d \leq z^2} \mu^2(d) 3^{\nu(d)} \omega(d).$$

Trivially we have $\omega(d) \leq 2^{\nu(d)}$ and $\nu(d) \leq (\log d)/(\log 2)$, whence

$$3^{\nu(d)} \omega(d) \leq 8^{\nu(d)} \leq d^3.$$

It follows that the sum above is at most z^8. Putting all these estimates together we therefore conclude that

$$S(\mathcal{A}; \mathcal{P}, z) \ll \frac{x}{(\ell k k')^2} (\frac{\log d'}{\log z})^2 + z^8$$

for $1 \leq d < d' < x^{1/8}$, and hence that

$$N(x; d, d') \ll \frac{x}{(\ell k k')^2} (\frac{\log d'}{\log z})^2 + z^8.$$

We now choose $z = x^{1/24}$. The bound (10) then implies

$$\frac{x}{(\ell k k')^2} (\frac{\log d'}{\log z})^2 \gg x^{1/2} \frac{1}{(\log x)^2} \gg x^{1/3},$$

whence we may conclude that

$$N(x; d, d') \ll \frac{x}{(\ell k k')^2} (\frac{\log d'}{\log x})^2.$$

It remains to estimate the contribution of these terms to the sum occurring in (2). That is to say, we have to bound

$$\sum_{d < d' < x^{1/8}} \frac{x}{(\ell k k')^2} (\frac{\log d'}{\log x})^2,$$

with $d = \ell k$, $d' = \ell k'$. We shall ignore the condition h.c.f.$(k, k') = 1$. The above expression is then at most

$$\frac{x}{(\log x)^2} \sum_{k=1}^{\infty} \sum_{k'=1}^{\infty} \sum_{h=1}^{\infty} \frac{(\log \ell k')^2}{(\ell k k')^2}.$$

Since the triple sum is convergent the total is $O(x(\log x)^{-2})$. Theorem 2.1 now follows from this, in view of (1), (2) and (4).

Remark 2.2 We conclude this section with two remarks. Firstly we note that the argument above produces

$$N(x;1,2) \ll \frac{x}{(\log x)^2},$$

for example. We expect that this can be improved to give

$$N(x;1,2) = \kappa \frac{x}{(\log x)^2} + o(\frac{x}{(\log x)^2})$$

with an appropriate constant κ, but it appears that this is at least as hard as the Twin Prime problem. Thus there is presently no hope of improving the error term specified in Theorem 2.1. Secondly we observe that the proof of the Siegel-Walfisz Theorem is 'ineffective'. That is to say, the proof cannot provide an explicit value for the constant implied by the $O(\ldots)$ notation. It follows that the implied constant in Theorem 2.1 is also ineffective. This can probably be avoided by a more delicate argument using a weaker effective version of the Siegel-Walfisz Theorem.

3 Alternating groups

This section, and the section following it, are devoted to the proof of Theorem 1.3.

Here we study the subset of I arising from subgroups of finite alternating groups. We introduce the following notation.

$$\begin{aligned}
\mathrm{I}_{\mathrm{Alt}} &= \{|G:H| \mid G = A_n,\ H < G,\ \text{and } |G:H| > n\} \\
\mathrm{Large}_{\mathrm{Alt}} &= \{|G:H| \mid G = A_n,\ H < G,\ \text{and } |G:H| \geq \frac{\binom{n}{[n/2]}}{2}\} \\
\mathrm{Small}_{\mathrm{Alt}} &= \{|G:H| \mid G = A_n,\ H < G,\ \text{and } n < |G:H| < \frac{\binom{n}{[n/2]}}{2}\}.
\end{aligned}$$

Clearly $\mathrm{I}_{\mathrm{Alt}} = \mathrm{Large}_{\mathrm{Alt}} \cup \mathrm{Small}_{\mathrm{Alt}}$. Our aim in this section is to prove the following.

Theorem 3.1 *With the above notation we have* $\mathrm{I}_{\mathrm{Alt}}(x) \sim (\sqrt{2}+1)x^{1/2}$.

We begin by determining an upper bound for certain values of the integer function $d(m)$, where $d(m)$ denotes the number of divisors of a positive integer m.

Lemma 3.2 *Let k be a positive integer. Then there exists a constant c such that, for all n, $d(n!^k) \leq e^{(c+\log k)n/\log n}$.*

Proof. Let $n! = \prod_{p\le n} p^{a_p}$ be the prime factorization of $n!$. Then $a_p = \sum_{i\ge 1}[n/p^i] \le (n-1)/(p-1)$, and so $ka_p+1 \le k(n-1)/(p-1)+1 \le 2kn/p$. Hence

$$d(n!^k) = \prod_{p\le n}(ka_p+1) \le \prod_{p\le n}(2kn/p) = (2kn)^{\pi(n)}/(\prod_{p\le n} p).$$

Therefore

$$\log d(n!^k) \le \pi(n)\log(2k) + \pi(n)\log n - \theta(n),$$

where $\theta(n) = \sum_{p\le n}\log p$.

We use the standard estimates $\pi(n) \le n/\log n + cn/(\log n)^2$ and $\theta(n) \ge n - cn/\log n$ (see [SS, pp.31-32] for even sharper estimates) to obtain

$$\begin{aligned}\log d(n!^k) &\le (\frac{n}{\log n} + \frac{cn}{(\log n)^2})\log(2k) + (n + \frac{cn}{\log n}) - (n - \frac{cn}{\log n}) \\ &= (2c + \log(2k) + o(1))\,\frac{n}{\log n}.\end{aligned}$$

The result follows. ∎

Note that the bound above is best possible up to the constant c; indeed we have $d(n!) \ge 2^{\pi(n)} \ge e^{c'n/\log n}$. We now apply this result to estimate $\mathrm{Large}_{\mathrm{Alt}}(x)$.

Lemma 3.3 *We have* $\mathrm{Large}_{\mathrm{Alt}}(x) \le x^{c/\log\log x}$ *for some constant* c.

Proof. Let $m \in \mathrm{Large}_{\mathrm{Alt}}$ with $m \le x$. Then there is n and a subgroup $H < A_n$ such that $m = |A_n : H| \ge \binom{n}{[n/2]}/2 \ge 2^{n/3}$. Hence $n \le a\log m \le a\log x$, where $a = 3/\log 2$. Obviously we also have $m \mid n!$. It follows that, given $n \le a\log x$, there are at most $d(n!)$ choices for m, and so applying Lemma 3.2 above we obtain

$$\mathrm{Large}_{\mathrm{Alt}}(x) \le \sum_{5\le n\le a\log x} d(n!) \le \sum_{5\le n\le a\log x} e^{cn/\log n}.$$

This yields

$$\mathrm{Large}_{\mathrm{Alt}}(x) \le a\log x \cdot e^{c'\log x/\log\log x} = a\log x \cdot x^{c'/\log\log x},$$

from which the result follows. ∎

Lemma 3.4 *With the above notation we have* $\mathrm{Small}_{\mathrm{Alt}}(x) \sim (\sqrt{2}+1)x^{1/2}$.

Proof. A_n has subgroups of indices $\binom{n}{2}$ and $2\binom{n}{2}$, and the number of such indices up to x is $(\sqrt{2}+1)x^{1/2} + O(1)$. It remains to show that the contribution of the other indices m is $o(x^{1/2})$.

Let $m \in \mathrm{Small}_{\mathrm{Alt}}$ with $m \leq x$ be such an index. Then there is n and a subgroup $H < A_n$ of index $m < \binom{n}{[n/2]}/2$, satisfying $m \neq n, \binom{n}{2}, 2\binom{n}{2}$. We may assume that $n > 9$. Then by [DM, Theorem 5.2A], there exists $r < n/2$ and a subset Δ of size $n - r$ of the permutation domain Ω, such that

$$\mathrm{Alt}(\Delta) \leq H \leq \mathrm{Sym}(\Delta) \times \mathrm{Sym}(\Omega \setminus \Delta).$$

It follows that $m = \binom{n}{r}d$, where d is a divisor of $r!$. Using the trivial inequality $\binom{n}{r} \geq 2^r$ (for $r < n/2$) we see that $r \leq \log x / \log 2$. We also have $r \geq 3$ by our assumption on m.

Now, given r, there are at most $d(r!)$ choices for d, and at most $O(x^{1/3})$ choices for n satisfying $\binom{n}{r} \leq x$. By Lemma 3.2, $d(r!) \leq e^{cr/\log r}$, and since $r \leq \log x / \log 2$, we have $e^{cr/\log r} \leq x^{c'/\log\log x}$ for some constant c'. It follows that

$$\mathrm{Small}_{\mathrm{Alt}}(x) = (\sqrt{2}+1)x^{1/2} + O(x^{1/3+c'/\log\log x}),$$

and this implies the required conclusion. ∎

Theorem 3.1 now follows from Lemmas 3.3 and 3.4.

4 Groups of Lie type

In this section we study the subset of I arising from subgroups of finite simple groups of Lie type, thereby completing the proof of Theorem 1.3. Since the contributions from finite alternating groups have already been considered we assume that the Lie type simple group is not isomorphic to A_5, A_6 or A_8, that is to say, we study the set

$$\begin{aligned} \mathrm{I}_{\mathrm{Lie}} &= \{|G:H| \mid G \text{ a Lie type simple group, } H < G, \text{ and } G \ncong \\ &\quad A_5, A_6, A_8\}. \end{aligned}$$

Let J_2 be as in the Introduction, and define

$$I_3 = \{n \mid \exists\, m \in J_2,\ m \,|\, n, \text{ and } n \leq m^{24}\}.$$

The main result of this section is Theorem 4.4 below, which proves in particular that $\mathrm{I}_{\mathrm{Lie}} \cap I_2 \subseteq I_3$. We shall also show that $I_3(x) = O(x^{48/49})$, and this will complete the proof of Theorem 1.3.

We need some preparations.

Lemma 4.1 *There exists a constant c such that, for $y > 0$,*

$$\sum_{m \in J_2, m \geq y} m^{-1} \leq cy^{-1/2}.$$

In particular, $\sum_{m \in J_2} m^{-1} < \infty$.

Proof. As noted in the Introduction it follows from [CNT] that $J_2(x) \leq c'x^{1/2}$ for some constant c' (in fact any $c' > 2^{1/2}$ will do for large x). Now let $k \geq 0$. Then

$$\sum_{\substack{m \in J_2 \\ 2^k y \leq m < 2^{k+1} y}} m^{-1} \leq \frac{J_2(2^{k+1}y)}{2^k y} \leq \frac{c'(2^{k+1}y)^{1/2}}{2^k y} = c' 2^{1/2} 2^{-k/2} y^{-1/2}.$$

Therefore

$$\sum_{m \in J_2, m \geq y} m^{-1} \leq \sum_{k \geq 0} \sum_{\substack{m \in J_2 \\ 2^k y \leq m < 2^{k+1} y}} m^{-1} \leq c' 2^{1/2} y^{-1/2} \sum_{k \geq 0} 2^{-k/2} < cy^{-1/2}.$$

■

Lemma 4.2 *With the above notation we have $I_3(x) = O(x^{48/49})$.*

Proof. Let $n \in I_3$ with $x^{48/49} < n \leq x$. Then n has the form md for some $m \in J_2$ satisfying $m^{24} \geq n$. Thus $m^{24} > x^{48/49}$ and so $m \geq y$, where $y = x^{2/49}$. Given such an m, the integer d can be chosen in at most xm^{-1} ways, and we see that

$$I_3(x) \leq x^{48/49} + x \cdot \sum_{m \in J_2, m \geq y} m^{-1}.$$

Applying Lemma 4.1 we obtain

$$I_3(x) \leq x^{48/49} + x \cdot cy^{-1/2} = x^{48/49} + cx^{1-1/49} = (c+1)x^{48/49}.$$

■

We shall need the following information about orders of classical simple groups and numbers of subspaces.

Lemma 4.3 *(a)*

$$\begin{array}{ccccc}
q^{n^2-2} & < & |\mathrm{PSL}(n,q)| \leq |\mathrm{SL}(n,q)| & < & q^{n^2-1} \\
q^{n^2-3} & < & |\mathrm{PSU}(n,q)| \leq |\mathrm{SU}(n,q)| & < & q^{n^2} \\
q^{n^2/2+n/2-1} & < & |\mathrm{PSp}(n,q)| \leq |\mathrm{Sp}(n,q)| & < & q^{n^2/2+n/2} \\
q^{n^2/2-[n/2]-1} & < & |\mathrm{P}\Omega^\circ(n,q)| & < & q^{n^2/2-[n/2]}.
\end{array}$$

(b) For positive integers m, t, q with $t \leq m$, set

$$\left[\begin{array}{c} m \\ t \end{array} \right]_q = q^{t(m-t)} \prod_{i=0}^{t-1} \frac{1-q^{-(m-i)}}{1-q^{-(t-i)}}.$$

Then, for any constant ν,

$$\left[\begin{array}{c} m \\ t \end{array} \right]_q \prod_{i=0}^{t-1} (q^{m-\nu-i}+1) > q^{t(2m-\nu-3t/2+1/2)}.$$

(c) Let G be an n-dimensional classical simple group and V the underlying vector space over a field of order q, or order q^2 if G is of unitary type. Then the table below contains a lower bound for the number of t-dimensional subspaces of V in the linear case, and the number of totally singular t-dimensional subspaces in the other cases (when such exist).

Type	G	*Lower bound*
linear	$\mathrm{PSL}(n,q)$	$q^{t(n-t)}$
unitary	$\mathrm{PSU}(n,q)$	$q^{t(n-3t/2)}$
symplectic	$\mathrm{PSp}(n,q)$	$q^{t(n-3t/2+1/2)}$
orthogonal	$\mathrm{P\Omega}^\circ(n,q)$	$q^{t(n-3t/2-1/2)}$

Proof. For the linear groups we have $\gcd(n, q-1)\,|\mathrm{PSL}(n,q)| = |\mathrm{SL}(n,q)| = q^{n^2-1}\prod_{i=2}^{n}(1-q^{-i})$, and for $n \geq 2$ (see for example [NePr, Lemma 3.5])

$$1 - q^{-1} - q^{-2} < \prod_{i=1}^{n}(1-q^{-i}) < 1 - q^{-1}. \tag{12}$$

This yields the upper bound, and the lower bound follows from

$$|\mathrm{SL}(n,q)| > q^{n^2-2}(q^2-q-1)/(q-1) = q^{n^2-2}(q-\frac{1}{q-1}) \geq \gcd(n,q-1)q^{n^2-2}.$$

The other inequalities follow in a similar manner. For the unitary case,

$$\begin{aligned} \gcd(n,q+1)\,|\mathrm{PSU}(n,q)| &= |\mathrm{SU}(n,q)| = q^{n^2-1}\prod_{i=2}^{n}(1-(-q)^{-i}) \\ &\leq q^{n^2-1} \prod_{i\,\mathrm{odd},\,3\leq i\leq n} (1+q^{-i}) \\ &\leq q^{n^2-1}\Big(\prod_{i\,\mathrm{odd},\,i\geq 3} (1-q^{-i})\Big)^{-1} \end{aligned}$$

and by (12) this is less than

$$q^{n^2-1}\frac{1-q^{-1}}{1-q^{-1}-q^{-2}} < q^{n^2}.$$

Also

$$\begin{aligned} |\mathrm{PSU}(n,q)| &= \frac{q^{n^2-1}}{\gcd(n,q+1)}\prod_{i=2}^{n}(1-(-q)^{-i}) \\ &> \frac{q^{n^2-1}}{q+1}\prod_{j\le n/2}(1-q^{-2j}) > \frac{q^{n^2-1}}{q+1}(1-q^{-2}-q^{-4}) \end{aligned}$$

which is greater than q^{n^2-3} if $q \geq 3$, and the same lower bound holds also if $q = 2$ (we need to be a little more careful). The argument for $\mathrm{PSp}(n,q)$ and $\mathrm{P\Omega}^\circ(n,q)$ are similar.

To prove (b), note that since $t \leq m$, each of the factors in the product defining $\begin{bmatrix} m \\ t \end{bmatrix}_q$ is at least 1, and hence $\begin{bmatrix} m \\ t \end{bmatrix}_q \geq q^{t(m-t)}$.

Since the number of t-dimensional subspaces of V is $\begin{bmatrix} n \\ t \end{bmatrix}_q$ we have the required lower bound for the linear case of (c). For the other cases (see [T, p. 174]) the number of totally singular t-dimensional subspaces of V is given by the expression in (b) where m is the Lie rank of G, and ν takes the following values.

G	n	ν	Comments
$\mathrm{PSU}(n,q)$	$2m+1$	$-1/2$	$n-1/2 = 2m-\nu$
	$2m$	$1/2$	$n-1/2 = 2m-\nu$
$\mathrm{PSp}(n,q)$	$2m$	0	
$\mathrm{P\Omega}^+(n,q)$	$2m$	1	$n-1 = 2m-\nu$
$\mathrm{P\Omega}^-(n,q)$	$2m+2$	-1	$n-1 = 2m-\nu$
$\mathrm{P\Omega}(n,q)$	$2m+1$	0	$n-1 = 2m-\nu$

Note that $t \leq m$. The lower bounds in (c) now follow immediately from (b). ∎

A *section* of a group G is a factor group A/B where $B \leq A \leq G$ and $B \lhd A$. If a section is a simple group of Lie type we shall say that the section is of Lie type, and if it is a classical simple group we shall call it a classical section.

We shall say that an index $|G:H| \in \mathrm{I}_{\mathrm{Lie}}$ is *nested* relative to m, where G is a simple group of Lie type and $H < G$, if there exists a Lie type section T of G and a maximal subgroup M of T such that $m = |T:M|$, m

divides $|G:H|$, and $m^{24} \geq |G|$. Note that this implies $|G:H| \in I_3$, unless $T = \mathrm{PSL}(2,p)$ and $m = p+1$.

Theorem 4.4 below refers to the type of a classical simple group: the possibilities are that the type is *linear* for $G = \mathrm{PSL}(n,q)$ $(n \geq 2)$, *unitary* for $G = \mathrm{PSU}(n,q)$ $(n \geq 3)$, *symplectic* for $G = \mathrm{PSp}(n,q)$ $(n \geq 4,\ n$ even), or *orthogonal* for $G = \mathrm{P}\Omega^{\circ}(n,q)$ (where $\circ$ is $\pm$ with n even, or 'blank' with nq odd; also $n \geq 7$).

Theorem 4.4 *(a)* $\mathrm{I}_{\mathrm{Lie}} \cap I_2 \subseteq I_3$.

(b) Let $|G:H| \in \mathrm{I}_{\mathrm{Lie}}$, where G is a simple group of Lie type, $G \ncong A_5, A_6, A_8$, and $H < G$. Then either

(i) $|G:H|$ is nested relative to some m, or

(ii) G is a classical simple group of dimension $n \geq n_0$, H is reducible inducing a classical group of the same type as G on a composition factor of dimension $s > s_0(n)$, and $|G:H| > q^{3(n^2-s^2)/32}$, where $(n_0, s_0(n))$ is $(24, 3n/4)$ if $G = \mathrm{PSL}(n,q)$ and $(45, 9n/16)$ in the other cases.

Proof. Let M be a maximal subgroup of G containing H, so $|G:H|$ is divisible by $|G:M|$. If G is a simple classical group then the minimal index of a maximal subgroup is given in [C] and upper bounds for $|G|$ in Lemma 4.3. For $G = \mathrm{PSL}(n,q)$ we have $|G:M| \geq q^{n-1}$ and so $|G:H|^{24} \geq q^{24(n-1)} \geq q^{n^2-1} > |G|$ if $n \leq 23$. Similarly $|G:H|^{24} \geq |G|$ for $G = \mathrm{PSU}(n,q)$, $\mathrm{PSp}(n,q)$ or $\mathrm{P}\Omega^{\circ}(n,q)$ if $n \leq 46, 44$, or 44 respectively. For all these groups $|G:H|$ is nested relative to $m = |G:M|$ and either $m \in J_2$ whence $|G:H| \in I_3$, or $G = \mathrm{PSL}_2(p)$ and $m = p+1$ with p prime. In the latter case, if p does not divide $|H|$, then H is cyclic of order dividing $(p-1)/2$ and H is also contained in a maximal subgroup M_2 that is dihedral of order $p-1$. Using M_2 in place of M we see that $|G:H|$ is nested relative to $|G:M_2| \in J_2$ so $|G:H| \in I_3$. On the other hand if p divides $|H|$, then $H \in S(p)$ and $|G:H|$ is nested relative to $p+1$. Moreover, if we assume $|G:H| \in I_2$ we can exclude the latter case and conclude that $|G:H| \in I_3$, as required in part (a).

In a similar fashion we can show that if G is an exceptional Lie type group then $|G:H|$ is nested relative to some $m = |G:M| \in J_2$ using information about the minimal index of a maximal subgroup M (see, for example, [LS1]). Thus $|G:H| \in I_3$.

Therefore we may assume that G is a classical simple group with dimension n at least 24, 47, 46, or 45 for the linear, unitary, symplectic or orthogonal types respectively. Let V denote the underlying vector space over a field F of order q, or of order q^2 in the unitary case. We deal with the linear case first to demonstrate the broad strategy of our arguments. The other cases are more complicated and deserve separate treatment.

Linear case. Here $G = \mathrm{PSL}(n,q)$ with $n \geq 24$. Suppose first that H leaves invariant a t-dimensional subspace U of V with $n/8 \leq t \leq 7n/8$. Let M denote the stabiliser of U in G, so M is maximal in G and $H \leq M < G$. By Lemma 4.3, $|G:M| \geq q^{t(n-t)} \geq q^{7n^2/64} > |G|^{7/64}$, and hence $|G:H|$ is nested relative to $|G:M| \in J_2$ and $|G:H| \in I_3$. Thus we may assume that any proper non-trivial H-invariant subspace has dimension less than $n/8$ or greater than $7n/8$. Let $0 = V_0 < V_1 < \ldots < V_k = V$ be a composition series for V as an FH-module, where $k \geq 1$. Then H induces an irreducible subgroup H_i on V_i/V_{i-1} $(i = 1, \ldots, k)$. Set $n_i = \dim(V_i/V_{i-1})$, and $s_i = \dim(V_i) = \sum_{j=1}^{i} n_j$, for each $i = 1, \ldots, k$. Then for each i, $s_i < n/8$ or $s_i > 7n/8$. It follows that there is an ℓ such that $n_\ell > 3n/4$. Suppose that H_ℓ does not contain $\mathrm{SL}(n_\ell, q)$ and let M be a maximal subgroup of $\mathrm{SL}(n_\ell, q)$ that contains $H_\ell \cap \mathrm{SL}(n_\ell, q)$. Let $\bar{M}$ be the subgroup of $T = \mathrm{PSL}(n_\ell, q)$ corresponding to M, so $\bar{M}$ is a proper irreducible subgroup of T and is maximal in T. By [LS2], Proposition 2, we have $|T:\bar{M}|^5 \geq |T|$. Hence, by Lemma 4.3, $|T:\bar{M}|^{24} \geq |T|^{24/5} > q^{24(n_\ell^2-2)/5} > q^{24(9n^2/16-2)/5} > q^{n^2} > |G|$, so $|G:H|$ is nested relative to $|T:\bar{M}| \in J_2$ and $|G:H| \in I_3$.

This leaves the case where H_ℓ contains $\mathrm{SL}(n_\ell, q)$. In particular H is reducible, and stabilises V_ℓ and $V_{\ell-1}$. Let M be the stabiliser in G of V_ℓ, and let N be the stabiliser in M of $V_{\ell-1}$. Then by Lemma 4.3, $|G:H|$ is divisible by $|G:M|\,|M:N| > q^{s_\ell(n-s_\ell)}\, q^{n_\ell(s_\ell-n_\ell)} \geq q^{n_\ell(n-n_\ell)}$; this is greater than $q^{3(n^2-n_\ell^2)/32}$. Thus (b) (ii) holds. Finally we show that $|G:H| \in I_3$. By Lemma 4.3, $|G:H| \leq |G|/|\mathrm{PSL}(n_\ell, q)| < q^{n^2-n_\ell^2+1}$. If $n - s_\ell = \dim(V/V_\ell) \geq (n-n_\ell)/2$, take M to be the stabiliser in G of V_ℓ so that $|G:M| > q^{s_\ell(n-s_\ell)} \geq q^{(n^2-n_\ell^2)/4}$. On the other hand if $n - s_\ell < (n-n_\ell)/2$ so that $s_\ell - n_\ell = \dim(V_{\ell-1}) > (n-n_\ell)/2$, take M to be the stabiliser in G of $V_{\ell-1}$, so that again $|G:M| > q^{(s_\ell-n_\ell)(n-s_\ell+n_\ell)} \geq q^{(n^2-n_\ell^2)/4}$. In either case we have $|G:M|^{24} > |G:H|$ and $|G:M| \in J_2$, so $|G:H| \in I_3$.

Classical case. In these remaining cases G preserves a non-degenerate bilinear, sesqui-linear or quadratic form on V. Let W be an H-invariant subspace of V that is maximal subject to being totally singular; possibly $W = 0$. Then $W \subseteq W^\perp$. Let $t = \dim(W)$ and suppose first that $t \geq n/8$. Then, for M the stabiliser of W in G, it follows from Lemma 4.3 that $|G:M|^{24} > |G|$ so $|G:H|$ is nested relative to $|G:M| \in J_2$ and $|G:H| \in I_3$. Thus we may assume that $0 \leq t < n/8$. In particular $W \neq W^\perp$, $W^\perp/W$ is nonsingular and G induces on $W^\perp/W$ a classical group of the same type as G. Set $m = n - 2t = \dim(W^\perp/W)$, so $m > 3n/4$.

Let $W = V_0 < V_1 < \ldots < V_k = W^\perp$ $(k \geq 1)$ correspond to a composition series for $W^\perp/W$ as an FH-module. For a subspace Y such that $W \leq Y \leq W^\perp$, set $\overline{Y} = Y/W$, so $\overline{V_k} = W^\perp/W$ and $\overline{V_0} = 0$. Also set $n_i = \dim(V_i/V_{i-1})$ and $s_i = \sum_{j=1}^{i} n_j = \dim(\overline{V_i})$ for $1 \leq i \leq k$. For $i > 0$, $V_i^\perp \subset W^\perp$ since $V_i \supset W$; also $V_i^\perp \supset W$ since $V_i \subset W^\perp$. Thus $W \leq V_i^\perp \leq W^\perp$. Moreover $V_i^\perp \cap V_i$ is a totally singular H-invariant subspace containing W, so by the

maximality of W, $V_i^\perp \cap V_i = W$. Thus $\overline{V_i} \cap \overline{V_i^\perp} = 0$, and it follows that $\overline{V_i}$ is nonsingular and $(\overline{V_i})^\perp = \overline{V_i^\perp}$. Moreover $\overline{V_{i-1}} < \overline{V_i}$, so $(\overline{V_{i-1}})^\perp > (\overline{V_i})^\perp$. Set $\overline{W_i} := (\overline{V_{i-1}})^\perp \cap \overline{V_i}$ and let W_i be the subspace of $W^\perp$ containing W such that $W_i/W = \overline{W_i}$. Then $\overline{V_{i-1}}$ is the orthogonal direct sum $\overline{W_i} \perp \overline{V_{i-1}}$ and $\overline{W_i}$ is nonsingular of dimension n_i. It follows that $\overline{V_k} = \overline{W_1} \perp \ldots \perp \overline{W_k}$. Note that the stabiliser in G of V_i and V_{i-1} also leaves invariant $W = V_i^\perp \cap V_i$ and W_i, and induces on $\overline{W_i}$ a classical group of the same type as G.

Suppose next that for some ℓ, $m/8 \leq s_\ell \leq 7m/8$. In this case let T be the classical simple group induced by G on $\overline{V_k}$, so T is of dimension m and of the same type as G. Let M be the stabiliser in T of the nonsingular s_ℓ-dimensional subspace $\overline{V_\ell}$ of $\overline{V_k}$. Then $|T : M|$ divides $|G : H|$. Now M is a central product of the classical groups induced on $\overline{V_\ell}$ and $\overline{V_\ell}^\perp$. For each of the three types, using the bounds from Lemma 4.3 (a), we find that $|T : M|^{24} > |G|$ and hence $|G : H|$ is nested relative to $|T : M| \in J_2$ and $|G : H| \in I_3$.

We may now assume that for each ℓ, either $s_\ell < m/8$ or $s_\ell > 7m/8$. Thus there exists ℓ such that $n_\ell > 3m/4 > 9n/16 \geq 25$. Let H_ℓ, G_ℓ denote the groups induced by H, G on $\overline{W_\ell}$. Then H_ℓ is an irreducible subgroup of G_ℓ. Let S be the subgroup $\mathrm{SU}(m,q), \mathrm{Sp}(m,q)$ or $\Omega^\circ(m,q)$ of G_ℓ in the unitary, symplectic or orthogonal cases respectively, and let $\overline{S}$ be the simple classical group corresponding to S. Suppose now that H_ℓ does not contain S, and let $\overline{H_\ell}$ be the subgroup of $\overline{S}$ corresponding to $H_\ell \cap S$. Then $\overline{H_\ell}$ is a proper irreducible subgroup of $\overline{S}$. Let M be a maximal subgroup of $\overline{S}$ containing $\overline{H_\ell}$. Then by [LS2], Proposition 2, $|\overline{S} : M|^5 > |\overline{S}|$, so $|\overline{S} : M|^{24} > |\overline{S}|^{24/5}$ and again using the bounds for Lemma 4.3 we find that $|\overline{S} : M|^{24} > |G|$. Since $|\overline{S} : M|$ divides $|G : H|$, we have that $|G : H|$ is nested relative to $|\overline{S} : M| \in J_2$ and $|G : H| \in I_3$. Thus we may assume that H_ℓ contains S. This means in particular that $s_\ell < n$ so that H is reducible.

We have $|G : H| \leq |G|/|\overline{S}|$, and by Lemma 4.3 (a), this is at most q^x where $x = n^2 - n_\ell^2 + 3$, $\frac{n^2}{2} + \frac{n}{2} - \frac{n_\ell^2}{2} - \frac{n_\ell}{2} + 1$, or $\frac{n^2}{2} - [\frac{n}{2}] - \frac{n_\ell^2}{2} + [\frac{n_\ell}{2}] + 1$ for the unitary, symplectic, or orthogonal types respectively. Suppose first that $t \geq (n - n_\ell)/4$. Take $T = G$ and M to be the stabiliser in G of W. Then $|T : M|$ divides $|G : H|$ and by Lemma 4.3 (c), $|T : M| \geq q^y$ where (recall that $t < n/8$)

$$\begin{aligned} y &\geq t(n - \frac{3}{2}t - \frac{1}{2}) \\ &\geq \frac{1}{4}(n - n_\ell)(n - \frac{3}{8}(n - n_\ell) - \frac{1}{2}) \\ &= \frac{1}{32}(n - n_\ell)(5n + 3n_\ell - 4) \\ &> \frac{3}{32}(n^2 - n_\ell^2) \end{aligned}$$

so that (b) (ii) holds, and in all cases $24y > x$ so $|G : H| \in I_3$. Thus we

may assume that $t < (n-n_\ell)/4$, whence $m - n_\ell = n - 2t - n_\ell > (n-n_\ell)/2$. Also, since $n_\ell > 9n/16$, we have that $n_\ell > 9(n+n_\ell)/25$. Take T to be the classical simple group induced by G on $\overline{V_k}$, and M to be the stabiliser in T of the nonsingular n_ℓ-dimensional subspace $\overline{W_\ell}$. Then $|G:H|$ is divisible by $|T:M|$, and by Lemma 4.3 (a), $|T:M| \geq q^y$ where in the unitary case

$$\begin{aligned} y &\geq m^2 - 3 - n_\ell^2 - (m-n_\ell)^2 \\ &= 2n_\ell(m-n_\ell) - 3 \\ &> 2 \cdot \frac{9}{25}(n+n_\ell)(\frac{n-n_\ell}{2}) - 3 \\ &> \frac{3}{32}(n^2 - n_\ell^2) \end{aligned}$$

and $24y > x$ so (b) (ii) holds and $|G:H| \in I_3$. In the symplectic and orthogonal cases,

$$\begin{aligned} y &\geq \frac{m^2}{2} \pm \lfloor \frac{m}{2} \rfloor - 1 - \frac{n_\ell^2}{2} \mp \lfloor \frac{n_\ell}{2} \rfloor - \frac{(m-n_\ell)^2}{2} \mp \lfloor \frac{m-n_\ell}{2} \rfloor \\ &\geq n_\ell(m-n_\ell) - 1 \end{aligned}$$

and as in the unitary case this is greater than $\frac{3}{32}(n^2 - n_\ell^2)$ and $24y > x$. Thus in all cases (b) (ii) holds and $|G:H| \in I_3$. This completes the proof. ∎

Combining Lemma 4.2 with Theorem 4.4(a) we obtain the following.

Corollary 4.5 $(\mathrm{I}_{\mathrm{Lie}} \cap I_2)(x) = O(x^{48/49})$.

We complete this section by proving Theorem 1.3.

Note that $I_2 = \mathrm{I}_{\mathrm{Alt}} \cup (\mathrm{I}_{\mathrm{Lie}} \cap I_2) \cup \mathrm{I}_{\mathrm{Spor}}$, where

$$\mathrm{I}_{\mathrm{Spor}} = \{|G:H| \mid G \text{ a finite sporadic simple group, } H < G\}.$$

Applying Theorem 3.1, Corollary 4.5, and the finiteness of $\mathrm{I}_{\mathrm{Spor}}$ we obtain

$$I_2(x) = O(x^{1/2}) + O(x^{48/49}) + O(1) = O(x^{48/49}).$$

Theorem 1.3 is proved.

5 Quasiprimitive and innately transitive groups

In this section we prove Theorems 1.5 and 1.6. Let G be a quasiprimitive or innately transitive permutation group on a set Ω of size n such that $G \neq A_n$ or S_n. Then n lies in the set $\mathrm{Deg}_{\mathrm{qp}}$ or $\mathrm{Deg}_{\mathrm{it}}$, respectively, as defined in the

Introduction. It was shown, in [Pr] and [BPr] respectively, that the finite quasiprimitive and innately transitive groups satisfy theorems similar to the O'Nan–Scott Theorem for finite primitive groups. In particular the results of [BPr, Pr] imply that either n is the degree of a primitive permutation group, or $n \in I$, or G has a unique transitive minimal normal subgroup N, and N has the form

$$N = T_1 \times T_2 \times \ldots \times T_k \cong T^k$$

for some nonabelian simple group T and integer $k \geq 2$; and moreover there is a proper nontrivial subgroup R of T such that a point stabiliser in N is a subdirect subgroup of R^k. This means that

$$n = dm^k, \text{ where } m = |T : R|,\ k \geq 2, \text{ and } d \text{ divides } |R|^{k-1}. \qquad (13)$$

Thus in order to prove Theorems 1.5 and 1.6, we need to deal with quasiprimitive and innately transitive groups G of degree n as in (13).

Define

$$\text{Prod} \quad = \quad \{n \mid n = dm^k \text{ as in (13)}\}$$

and set

$$\text{Prod}_{\text{qp}} := \text{Prod} \cap \text{Deg}_{\text{qp}} \quad \text{and} \quad \text{Prod}_{\text{it}} := \text{Prod} \cap \text{Deg}_{\text{it}}. \qquad (14)$$

The main result of this section is the following.

Theorem 5.1 *With the above notation we have*

$$\text{Prod}(x) = O(x^{48/49}).$$

Before proceeding to prove this result we show how it can be used to prove Theorems 1.5 and 1.6.

Proofs of Theorems 1.5 and 1.6: From the results in [BPr, Pr], as discussed above, we have

$$\text{Deg}_{\text{qp}} = \text{Deg}_{\text{prim}} \cup I \cup \text{Prod}_{\text{qp}} \quad \text{and} \quad \text{Deg}_{\text{it}} = \text{Deg}_{\text{prim}} \cup I \cup \text{Prod}_{\text{it}}$$

with Prod_{qp} and Prod_{it} as in (14). From the definitions of I and J in the Introduction, we have $I = I_1 \cup I_2$ and $I \cap \text{Deg}_{\text{prim}} = J = J_1 \cup J_2$, where for $\ell = 1, 2$, $I_\ell \cap \text{Deg}_{\text{prim}} = J_\ell$. Moreover it was proved in [CNT] (see the Introduction) that

$$J_1(x) = \frac{x}{\log x} + O(\frac{x}{(\log x)^2}) \sim \frac{x}{\log x} \quad \text{and} \quad J_2(x) = O(x^{1/2}).$$

Thus

$$(I \cap \mathrm{Deg}_{\mathrm{prim}})(x) = J(x) \sim \frac{x}{\log x},$$

Combining this with Theorem 5.1 we conclude that, for $D = \mathrm{Deg}_{\mathrm{qp}}$ or $\mathrm{Deg}_{\mathrm{it}}$,

$$D(x) \sim \mathrm{Deg}_{\mathrm{prim}}(x) + I(x) - \frac{x}{\log x} + O(x^{48/49}),$$

which, by [CNT] and Theorem 1.1 yields

$$D(x) \sim 2\frac{x}{\log x} + h\frac{x}{\log x} - \frac{x}{\log x} = (h+1)\frac{x}{\log x},$$

or, using Theorems 1.2 and 1.3 (instead of Theorem 1.1),

$$D(x) = \mathrm{Deg}_{\mathrm{prim}}(x) + I(x) - J(x) + O(x^{48/49}) = (h+1)\frac{x}{\log x} + O(\frac{x}{(\log x)^2}).$$

This completes the proofs of Theorems 1.5 and 1.6. ∎

Now we prove Theorem 5.1. We need additional notation. Define

$$\begin{aligned}
\mathrm{Prod}_{\mathrm{Alt}} &= \{n \mid n = dm^k \text{ as in (13) with } T \text{ an alternating group}\} \\
\mathrm{Prod}_{\mathrm{Lie}} &= \{n \mid n = dm^k \text{ as in (13) with } T \text{ a Lie type simple group} \\
&\quad G \ncong A_5, A_6, A_8\} \\
\mathrm{Prod}_{\mathrm{Spor}} &= \{n \mid n = dm^k \text{ as in (13) with } T \text{ a sporadic simple group}\}.
\end{aligned}$$

Clearly $\mathrm{Prod} = \mathrm{Prod}_{\mathrm{Alt}} \cup \mathrm{Prod}_{\mathrm{Lie}} \cup \mathrm{Prod}_{\mathrm{Spor}}$. Since there are only finitely many sporadic simple groups, there are finitely many primes $p_1, \ldots, p_l$ such that the indices $n \in \mathrm{Prod}_{\mathrm{Spor}}$ have the form $p_1^{a_1} \cdots p_l^{a_l}$ where $a_i \geq 0$, and this implies

$$\mathrm{Prod}_{\mathrm{Spor}}(x) = O(x^\epsilon) \text{ for any } \epsilon > 0.$$

We complete the determination of $\mathrm{Prod}(x)$ by considering separately the alternating groups and the groups of Lie type. Note that, for $n \leq x$ as in (13), we have $x \geq dm^k \geq m^k$, so $m \leq x^{1/k}$ and also $k \leq \log x / \log 5 < \log x$ (since $m = |T : R| \geq 5$).

Lemma 5.2 $\mathrm{Prod}_{\mathrm{Alt}}(x) = 2x^{1/2} + O(x^{1/3}(\log x)^2)$.

Proof. Let $n = dm^k \in \mathrm{Prod}_{\mathrm{Alt}}$ with $n \leq x$, so $m = |T : R|$ with $T = A_r$ for some $r \geq 5$. We divide the proof into three cases: (1) $m = r$, (2) $m \geq 2^{r/3}$, and (3) $r < m < 2^{r/3}$.

Case (1). Here the stabiliser N_α in N of a point α is a G_α-invariant subdirect subgroup of A_{m-1}^k. We shall show that the contribution to $\mathrm{Prod}_{\mathrm{Alt}}(x)$ from this case is $2x^{1/2} + O(x^{1/3}(\log x)^2)$. Since N is a minimal normal subgroup

of G and $G = NG_\alpha$, it follows that, for $m \geq 6$, G_α is transitive on the simple direct factors of A_{m-1}^k. Therefore N_α is isomorphic to A_{m-1}^ℓ for some divisor ℓ of k. Thus the number of choices for d, given m and k, is the number $d(k)$ of divisors of k. Therefore the contribution to $\mathrm{Prod}_{\mathrm{Alt}}(x)$ from case (1) is

$$\begin{aligned}\sum_{k=2}^{\log x} \sum_{m \leq x^{1/k}} d(k) &= 2x^{1/2} + O(\sum_{k=3}^{\log x} kx^{1/k}) \\ &= 2x^{1/2} + O(x^{1/3}(\log x)^2).\end{aligned}$$

For $m = 5$, the socle of N_α is elementary abelian of order 2^{2l} for some divisor l of k, and $|N_\alpha| = 4^l 3^{l'}$ for some $l' \leq l$. So the number of choices for d is at most

$$\sum_{k=2}^{\log_5 x} (k+1)(k+2)/2 \leq c(\log x)^3.$$

Case (2). Here $m \geq 2^{r/3}$, so $2^{rk/3} \leq n \leq x$, that is, $5k \leq rk \leq 3\log x/\log 2$. We shall show that the contribution to $\mathrm{Prod}_{\mathrm{Alt}}(x)$ from this case is at most $x^{c/\log\log x}$ for some constant c. Since N is transitive, n divides $(r!)^k$. Thus the contribution is at most

$$\sum_{k=2}^{3\log x/5\log 2} \Big(\sum_{r=5}^{3\log x/k\log 2} d((r!)^k)\Big),$$

which by Lemma 3.2 is at most

$$\sum_{k=2}^{3\log x/5\log 2} \Big(\sum_{r=5}^{3\log x/k\log 2} e^{(c+\log k)r/\log r}\Big).$$

Since $r/\log r$ is an increasing function, this is at most

$$\sum_{k=2}^{3\log x/5\log 2} \frac{3\log x}{k\log 2}\, e^{r_0(k,x)}$$

where $r_0(k,x) = (c+\log k)\cdot \frac{3\log x}{k\log 2}\cdot (\log(\frac{3\log x}{k\log 2}))^{-1}$. Consider the partial sum for $k < \sqrt{\log x}$. For such k, $\frac{3\log x}{k\log 2} \geq \frac{3}{2}\sqrt{\log x}$ and so $r_0(k,x) \leq c_2 \log x/\log\log x$ for some constant c_2. So this partial sum is at most

$$c_1 x^{c_2/\log\log x} \log x \sum_{k\ <\sqrt{\log x}} \frac{1}{k} \leq x^{c_3/\log\log x}$$

for some constants c_1, c_3. Now for $k \geq \sqrt{\log x}$, $r_0(k,x)$ is decreasing with k and is at most $c_2'(\log x)^{1/2}$. Thus the second partial sum is at most

$$c_1' e^{c_2'(\log x)^{1/2}} \log x \sum_{k=\sqrt{\log x}}^{3\log x/5\log 2} \frac{1}{k} < x^{c_3'/\log\log x}$$

for some constants c_1', c_2', c_3'.

Case (3). Here $6 \leq r+1 \leq m < 2^{r/3}$, so in particular $r > 10$. We shall show that the contribution to $\mathrm{Prod}_{\mathrm{Alt}}(x)$ is at most $x^{c/\log\log x}$ for some constant c. Again n divides $(r!)^k$. Note that

$$\binom{r}{\lfloor r/3 \rfloor} \geq 3^{r/3} > 2^{3r} > m$$

whence by [DM, Theorem 5.7] it follows that R induces A_s on some s-subset, where $s > 2r/3$, (so $s \geq 7$). Since N_α is a subdirect subgroup of R^k, and since G_α is transitive on the k direct factors of R^k, it follows that N_α has l composition factors isomorphic to A_s, for some divisor l of k. Thus n is of the form

$$n = \binom{r}{s}^k \cdot (s!/2)^{k-l} \cdot d'$$

where d' divides $(r-s)!^k$. Now $x \geq n \geq \binom{r}{s}^k \geq 2^{sk}$, so $sk \leq \log x/\log 2$. Given s and k satisfying this inequality, we choose r to satisfy $s+2 \leq r < 3s/2$, then we choose a divisor l of k and a divisor d' of $(r-s)!^k$. Thus the contribution from this case is at most

$$\sum_{k=2}^{\frac{\log x}{\log 2}} \sum_{s=7}^{\frac{\log x}{k\log 2}} \Big(\sum_{s+2 \leq r < 3s/2} d(k) \cdot d((r-s)!^k) \Big).$$

Now $d(k) \leq k < \log x$ and we use Lemma 3.2 to bound $d((r-s)!^k)$. This shows that the contribution is at most

$$\log x \sum_{k=2}^{\frac{\log x}{\log 2}} \sum_{s=7}^{\frac{\log x}{k\log 2}} \Big(\sum_{s+2 \leq r < 3s/2} e^{(c+\log k)(r-s)/\log(r-s)} \Big).$$

Since $(r-s)/\log(r-s)$ is increasing with r, performing the inner summation over the s summands we see that this is at most

$$\log x \sum_{k=2}^{\frac{\log x}{\log 2}} \sum_{s=7}^{\frac{\log x}{k\log 2}} s \cdot e^{(c+\log k)s/(2\log(s/2))}.$$

Again, since the summand is an increasing function of s, performing the inner summation over the $\log x/(k\log 2)$ summands we see that this is at most

$$\log x \sum_{k=2}^{\frac{\log x}{\log 2}} \Big(\frac{\log x}{k\log 2}\Big)^2 \cdot e^{(c+\log k)(\frac{\log x}{2k\log 2})/\log(\frac{\log x}{2k\log 2})}.$$

Now the exponent of e in the last factor is a decreasing function of k, so this is at most

$$c(\log x)^3\, e^{c'\log x/\log\log x} \sum_{k=2}^{\frac{\log x}{\log 2}} \frac{1}{k^2} \leq c'' e^{c'\log x/\log\log x}$$

for some constants c, c', c''. ∎

Finally we consider the Lie type groups.

Lemma 5.3 *For x sufficiently large,* $\mathrm{Prod}_{\mathrm{Lie}}(x) < 4x^{48/49}$.

Proof. Let $n \in \mathrm{Prod}_{\mathrm{Lie}}$ with $n \leq x$. Then $n = m^k d$ with $k \geq 2$, $m = |T : R|$, and d divides $|R|^{k-1}$, where T is a Lie type simple group and $R < T$. By Theorem 4.4, we may divide these possibilities into two cases: (1) $m = |T : R|$ is nested, and (2) the case where T, R are as in Theorem 4.4 (b) (ii).

Case (1). In this case there exists a simple Lie type section T' of T and a maximal subgroup M of T' such that, for $u = |T' : M|$, u divides m and $u^{24} \geq |T|$. There are at most $x^{48/49}$ of these indices n such that $n \leq x^{48/49}$, and we shall show that, for large x, there are less than $2x^{48/49}$ such indices in the range $x^{48/49} < n \leq x$. So assume now that $x^{48/49} < n \leq x$. Then as $n < |T|^k \leq u^{24k}$, we have $u > x^{2/49k}$. Now $n = u^k d' \leq x$, for some d' satisfying $d' \leq x/u^k$. Hence the number of such n is at most

$$\begin{aligned}
\sum_{k=2}^{\log_5 x} \sum_{u > x^{2/49k}} \frac{x}{u^k} &\leq x \sum_{k=2}^{\log_5 x} \int_{x^{2/49k}}^{\infty} \frac{du}{u^k} \\
&= x \sum_{k=2}^{\log_5 x} \frac{1}{(k-1)x^{2(k-1)/49k}} \\
&= x^{48/49} + x^{47/49} \sum_{k=3}^{\log_5 x} \frac{x^{2/49k}}{(k-1)} \\
&\leq x^{48/49} + x^{143/147} \log_5 x < 2x^{48/49}.
\end{aligned}$$

Thus, for x sufficiently large, there are less than $3x^{48/49}$ indices n arising from Case (1).

Case (2). Here T is a classical simple group of dimension $r \geq r_0$ over a field of order q, R is reducible on the underlying vector space and induces a classical group T' of the same type as T on a composition factor of dimension $s > s_0(r)$, and $m = |T : R| > q^{3(r^2-s^2)/32}$, where $(r_0, s_0(r)) = (24, 3r/4)$ if $T = \mathrm{PSL}(r, q)$ and $(45, 9r/16)$ for the other types. In particular, we have $s \geq 19$ and $r^2 - s^2 \geq r^2 - s_0(r)^2 \geq 252$. Now $q^{3k(r^2-s^2)/32} < m^k \leq n \leq x$, so $q \leq x^{32/(3k(r^2-s^2))}$. Also $m > q^{3(r^2-s^2)/32} \geq 2^{(3\times 252)/32} > 2^{23}$, so $k \leq$

$\log x/\log m \le \log x/(23\log 2)$; and for a given k, since $x \ge q^{3k(r^2-s^2)/32} \ge q^{3k(r+s)/32} > 2^{3ks/16}$, we have $s \le \frac{16\log x}{3k\log 2}$.

Since N_α is a subdirect subgroup of R^k, and G_α is transitive on the k direct factors R, it follows that N_α has l composition factors isomorphic to T', for some divisor l of k. Thus the degree n is of the form $n = m^k \cdot |T'|^{k-l} \cdot d'$ where d' divides $D := (|T|/(|T'|m))^k$. We use the bounds in Lemma 4.3 (a) to obtain upper bounds for D. Let $D = q^z$ where $z = \log D/\log q$. Then in the linear case we have

$$\begin{aligned} z &\le k((r^2-1)-(s^2-2)-\frac{3}{32}(r^2-s^2)) \\ &= k(\frac{29}{32}(r^2-s^2)+1) < \frac{30}{32}k(r^2-s^2) \end{aligned}$$

so $D < x^{10}$. Similar computations in the unitary case give $D < x^{31/3}$, and in the symplectic and orthogonal cases give $D < x^{14/3}$. In all cases $D < x^{11}$.

Suppose that k is given. Since $m^k \le x$ we have at most $x^{1/k}$ choices for m; since $s \le \frac{16\log x}{3k\log 2}$ we have less than $\frac{16\log x}{3k\log 2}$ choices for s; and since $q \le x^{32/(3k(r^2-s^2))} < x^{32/756k}$ (since $r^2-s^2 \ge 252$), the number of choices for q is less than $x^{32/756k}$. For a given s and q, the number of choices for T' is at most 5. Next, the number of choices for ℓ dividing k is $d(k) \le k \le \log x$, and the number of choices for d' dividing D is $d(D) \le x^{c/\log\log x}$ (since $D < x^{11}$). Hence, given k, the number of choices for the degree $n = m^k|T'|^{k-\ell}d'$ is less than

$$x^{1/k} \cdot \frac{16\log x}{3k\log 2} \cdot x^{32/756k} \cdot 5 \cdot \log x \cdot x^{c/\log\log x},$$

and this is less than $x^{788/756k+\epsilon}$ for any $\epsilon > 0$ and large enough x. Since $k \ge 2$, this quantity is at most $x^{197/378+\epsilon}$. Finally, since $k \le \log x$, it follows that the total number of degrees in Case (2) is less than $x^{197/378+\epsilon}$ for any $\epsilon > 0$ and sufficiently large x. In particular, for large x, there are at most $x^{48/49}$ indices n arising from Case (2), and this yields the required conclusion. ∎

Proof of Theorem 5.1: This follows immediately from Lemma 5.2 and Lemma 5.3. ∎

References

[BPr] J. Bamberg and C. E. Praeger, Finite permutation groups with a transitive minimal normal subgroup, *Proc. London Math. Soc.*, to appear.

[CNT] P.J. Cameron, P.M. Neumann and D.N. Teague, On the degrees of primitive permutation groups, *Math. Z.* **180** (1982), 141–149.

[C] B. N. Cooperstein, Minimal degree for a permutation representation of a classical group, *Israel J. Math.* **30** (1978), 213–235.

[D] H. Davenport, *Multiplicative number theory,* Graduate Texts in Mathematics, 74, Springer-Verlag, New York, 2000.

[DM] J. Dixon and B. Mortimer, *Permutation groups*, Springer-Verlag, New York, 1996.

[HR] H. Halberstam and H.-E. Richert, *Sieve methods,* Academic Press, London, 1974.

[LS1] M. W. Liebeck and J. Saxl, On the orders of maximal subgroups of the finite exceptional groups of Lie type, *Proc. London Math. Soc. (3)* **55** (1987), 299–330.

[LS2] M. W. Liebeck and J. Saxl, Maximal subgroups of finite simple groups and their automorphism groups, *Contemporary Math.* **131** (1992), 243–259.

[NePr] P.M. Neumann and C.E. Praeger, Cyclic matrices over finite fields, *J. London Math. Soc.* **52** (1995), 263–284.

[Pr] C.E. Praeger, An O'Nan-Scott Theorem for finite quasiprimitive permutation groups, and an application to 2-arc transitive graphs, *J. London Math. Soc.*(2) **47** (1993), 227–239.

[PrSh] C.E. Praeger and A. Shalev, Bounds on finite quasiprimitive permutation groups, *J. Austral. Math. Soc.* **71** (2001), 243–258.

[SS] W. Schwarz and J. Spilker, *Arithmetic Functions*, London Math. Soc. Lecture Note Series **184**, Cambridge Univ. Press, Cambridge, 1994.

[T] D.E. Taylor, *The geometry of the classsical groups*, Heldermann Verlag, Berlin, 1992.