NORMALIZERS OF PRIMITIVE PERMUTATION GROUPS

ROBERT M. GURALNICK, ATTILA MARÓTI, AND LÁSZLÓ PYBER

ABSTRACT. Let G be a transitive normal subgroup of a permutation group A of finite degree n. The factor group A/G can be considered as a certain Galois group and one would like to bound its size. One of the results of the paper is that $|A/G| < n$ if G is primitive unless $n = 3^4$, 5^4, 3^8, 5^8, or 3^{16}. This bound is sharp when n is prime. In fact, when G is primitive, $|\mathrm{Out}(G)| < n$ unless G is a member of a given infinite sequence of primitive groups and n is different from the previously listed integers. Many other results of this flavor are established not only for permutation groups but also for linear groups and Galois groups.

1. INTRODUCTION

1.1. **Permutation groups.** Aschbacher and the first author showed [AG2] that if A is a finite permutation group of degree n and A' is its commutator subgroup, then $|A : A'| \leq 3^{n/3}$, furthermore if A is primitive, then $|A : A'| \leq n$. These results were motivated by a problem in Galois theory. For another motivation for the present paper we need a definition. Let $\mathcal{N}$ be a normal series for a finite group X such that every quotient in $\mathcal{N}$ either involves only noncentral chief factors or is an elementary abelian group with at least one central chief factor. Define $\mu(\mathcal{N})$ to be the product of the exponents of the quotients which involve central chief factors. Let $\mu(X)$ be the minimum of the $\mu(\mathcal{N})$ for all possible choices of $\mathcal{N}$. This invariant is an upper bound for the exponent of X/X'. In [G2] it was shown that if A is a permutation group of degree n, then $\mu(A) \leq 3^{n/3}$, furthermore if A is transitive, then $\mu(A) \leq n$, and if A is primitive with $A'' \neq 1$, then the exponent of A/A' is at most $2 \cdot n^{1/2}$. These results were also motivated by Galois theory. In this paper we prove similar statements and obtain corresponding results in Galois theory.

Let G be a normal subgroup of a permutation group A of finite degree n. In this paper the factor group A/G is studied. It is often assumed that G is transitive (this

is very natural from the point of view of Galois groups and the results are much weaker without this assumption). Throughout the paper the base of the logarithms is 2 unless otherwise stated. Our first result is the following.

Theorem 1.1. *Let G and A be permutation groups of finite degree n with $G \lhd A$. Suppose that G is primitive. Then $|A/G| < n$ unless G is an affine primitive permutation group and the pair $(n, A/G)$ is $(3^4, \mathrm{O}_4^-(2))$, $(5^4, \mathrm{Sp}_4(2))$, $(3^8, \mathrm{O}_6^-(2))$, $(3^8, \mathrm{SO}_6^-(2))$, $(3^8, \mathrm{O}_6^+(2))$, $(3^8, \mathrm{SO}_6^+(2))$, $(5^8, \mathrm{Sp}_6(2))$, $(3^{16}, \mathrm{O}_8^-(2))$, $(3^{16}, \mathrm{SO}_8^-(2))$, $(3^{16}, \mathrm{O}_8^+(2))$, or $(3^{16}, \mathrm{SO}_8^+(2))$. Moreover if A/G is not a section of $\Gamma\mathrm{L}_1(q)$ when $n = q$ is a prime power, then $|A/G| < n^{1/2} \log n$ for $n \geq 2^{14000}$.*

The $n - 1$ bound in Theorem 1.1 is sharp when n is prime and G is a cyclic group of order n. For more information about the eleven exceptions in Theorem 1.1 and for a few other examples see Section 3. Note that for every prime p there are infinitely many primes r such that the primitive permutation group $G \leq \mathrm{A\Gamma L}_1(q)$ of order $np = qp = r^{p-1}p$ satisfies $|N_{\mathrm{S}_n}(G)/G| = (n-1)(p-1)/p$. It will also be clear from our proofs that the bound $n^{1/2} \log n$ in Theorem 1.1 is asymptotically sharp apart from a constant factor at least $\log_9 8$ and at most 1.

Our second result concerns the size of the outer automorphism group $\mathrm{Out}(G)$ of a primitive subgroup G of the finite symmetric group S_n.

Theorem 1.2. *Let $G \leq \mathrm{S}_n$ be a primitive permutation group. Then $|\mathrm{Out}(G)| < n$ unless G is an affine primitive permutation group and one of the following holds.*

(1) $n = 3^4$, $G = (C_3)^4 : (D_8 \circ Q_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_4^-(2)$.
(2) $n = 5^4$, $G = (C_5)^4 : (C_4 \circ D_8 \circ D_8)$ and $\mathrm{Out}(G) \cong \mathrm{Sp}_4(2)$.
(3) $n = 3^8$, $G = (C_3)^8 : (D_8 \circ D_8 \circ Q_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_6^-(2)$.
(4) $n = 3^8$, $G = (C_3)^8 : (D_8 \circ D_8 \circ D_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_6^+(2)$.
(5) $n = 5^8$, $G = (C_5)^8 : (C_4 \circ D_8 \circ D_8 \circ D_8)$ and $\mathrm{Out}(G) \cong \mathrm{Sp}_6(2)$.
(6) $n = 3^{16}$, $G = (C_3)^{16} : (D_8 \circ D_8 \circ D_8 \circ Q_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_8^-(2)$.
(7) $n = 3^{16}$, $G = (C_3)^{16} : (D_8 \circ D_8 \circ D_8 \circ D_8)$ and $\mathrm{Out}(G) \cong \mathrm{O}_8^+(2)$.
(8) $n = q^2$ with $q = 2^e$, $e > 1$, $G = (C_2)^{2e} : \mathrm{L}_2(q)$ and $|\mathrm{Out}(G)| = q(q-1)e$.

If G is any of the groups in (1)-(7) of Theorem 1.2, then $\mathrm{Out}(G) \cong N_{\mathrm{S}_n}(G)/G$. This indicates why there are only seven exceptional groups in the statement of Theorem 1.2 and not eleven as in the statement of Theorem 1.1. (For in four cases in Theorem 1.1 the group A has index 2 in $N_{\mathrm{S}_n}(G)$.)

Next we state an asymptotic version of Theorem 1.2. For this we need a definition. Let $\mathcal{C}$ be the class of all affine primitive permutation groups G with an almost simple point-stabilizer H with the property that the socle $\mathrm{Soc}(H)$ of H acts irreducibly on the socle of G and $\mathrm{Soc}(H)$ is isomorphic to a finite simple classical group such that its natural module has dimension at most 6.

Theorem 1.3. *Let $G \leq \mathrm{S}_n$ be a primitive permutation group. Suppose that if $n = q$ is a prime power then G is not a subgroup of $\mathrm{A\Gamma L}_1(q)$. If G is not a member of the infinite sequence of examples in Theorem 1.2, then $|\mathrm{Out}(G)| < 2 \cdot n^{3/4}$ for $n \geq 2^{14000}$. Moreover if G is not a member of $\mathcal{C}$, then $|\mathrm{Out}(G)| < n^{1/2} \log n$ for $n \geq 2^{14000}$.*

As mentioned earlier, the bound $n^{1/2} \log n$ in Theorem 1.3 is asymptotically sharp apart from a constant factor close to 1.

The proof of Theorem 1.1 requires a careful analysis of the abelian and the nonabelian composition factors of A/G where A and G are finite groups. For this purpose for a finite group X we denote the product of the orders of the abelian and the nonabelian composition factors of a composition series for X by $a(X)$ and $b(X)$ respectively. Clearly $|X| = a(X)b(X)$.

The next result deals with $b(A/G)$ in the general case when G is transitive and in the more special situation when G is primitive.

Theorem 1.4. *Let A and G be permutation groups with $G \lhd A \leq S_n$. If G is transitive, then $b(A/G) \leq n^{\log n}$. If G is primitive, then $b(A/G) \leq (\log n)^{2 \log \log n}$.*

In order to give a sharp bound for $a(A/G)$ when G is a primitive permutation group, interestingly, it is first necessary to bound $a(A)$ (for A primitive). In 1982 Pálfy [Pá] and Wolf [W] independently showed that $|A| \leq 24^{-1/3}n^{1+c_1}$ for a solvable primitive permutation group A of degree n where c_1 is the constant $\log_9(48 \cdot 24^{1/3})$ which is close to 2.24399. Equality occurs infinitely often. In fact $a(A) \leq 24^{-1/3}n^{1+c_1}$ holds [Py] for any primitive permutation group A of degree n. Using the classification theorem of finite simple groups we extend these results to the following, where for a finite group X and a prime p we denote the product of the orders of the p-solvable composition factors of X by $a_p(X)$.

Theorem 1.5. *Let $G \leq S_n$ be primitive, let p be a prime divisor of n and let c_1 be as before. Then $a_p(G)|\mathrm{Out}(G)| \leq 24^{-1/3}n^{1+c_1}$.*

Wolf [W] also showed that if G is a finite nilpotent group acting faithfully and completely reducibly on a finite vector space V, then $|G| \leq |V|^{c_2}/2$ where c_2 is the constant $\log_9 32$ close to 1.57732. In order to generalize this result we set $c(X)$ to be the product of the orders of the central chief factors in a chief series of a finite group X. In particular we have $c(X) = |X|$ for a nilpotent group X. The following theorem extends Wolf's result.

Theorem 1.6. *Let $G \leq S_n$ be a primitive permutation group. Then $c(G) \leq n^{c_2}/2$ where c_2 is as above.*

Some technical, module theoretic results enable us to show that if $G \lhd A \leq S_n$ are transitive permutation groups, then $a(A/G) \leq 6^{n/4}$ (see Theorem 7.4). In fact, we show that $a(A/G) \leq 4^{n/\sqrt{\log n}}$ whenever $n \geq 2$ (see Theorem 7.6). This together with Theorem 1.4 give the following.

Theorem 1.7. *We have $|A : G| \leq 4^{n/\sqrt{\log n}} \cdot n^{\log n}$ whenever G and A are transitive permutation groups with $G \lhd A \leq S_n$ and $n \geq 2$.*

For an exponential bound in Theorem 1.7 we can have $168^{(n-1)/7}$ (see Theorem 8.1). See [Py, Proposition 4.3] for examples of transitive p-groups (p a prime) showing that Theorem 1.7 is essentially the best one could hope for apart from the constant 4. It is also worth mentioning that a $c^{n/\sqrt{\log n}}$ type bound fails in case we relax the condition $G \lhd A$ to $G \lhd\lhd A$. Indeed, if A is a Sylow 2-subgroup of S_n for n a power of 2 and G is a regular elementary abelian subgroup inside A, then

$|A : G| = 2^n/2n$. The next result shows that an exponential bound in n holds in general for the index of a transitive subnormal subgroup of a permutation group of degree n.

Theorem 1.8. *Let $G \lhd\lhd A \leq \mathrm{S}_n$. If G is transitive, then $|A : G| \leq 5^{n-1}$.*

The proof of Theorem 1.8 avoids the use of the classification theorem for finite simple groups. Using the classification it is possible to replace the 5^{n-1} bound with 3^{n-1}. It would be interesting to know whether $|A : G| \leq 2^n$ holds for transitive permutation groups G and A with $G \lhd\lhd A \leq \mathrm{S}_n$.

We note that the paper contains sharp bounds for $|A : G|$, $b(A/G)$ and $a(A/G)$ in case A is a primitive permutation group of degree n and G is a transitive normal subgroup of A. These are $n^{\log n}$ in the first two cases (see the proofs of Theorems 1.11 and 5.1), and it is $24^{-1/3}n^{c_1}$ in the third case (see Corollary 6.6).

1.2. Galois groups.
As briefly mentioned earlier the above results are also motivated by questions in Galois theory. We need to introduce some definitions.

Let $k \leq F \leq E$ be three fields such that k is algebraically closed in E and the field extension $E \mid F$ is finite and separable. Let the degree of the extension $E \mid F$ be n. Let L be the Galois closure of $E \mid F$. Let k' denote the algebraic closure of k in L. Since $L \mid F$ is a Galois extension, so are $L \mid k'F$ and $L \mid E$ (where $k'F$ denotes the compositum over k of the subfields k' and F of L). We set $A = \mathrm{Gal}(L \mid F)$, $G = \mathrm{Gal}(L \mid k'F)$, and $H = \mathrm{Gal}(L \mid E)$.

By the definition of k', the Galois group A leaves k' invariant. Since G is the kernel of this action, G is normal in A and $A/G \cong \mathrm{Gal}(k'F \mid F)$. Furthermore $A/G \cong \mathrm{Gal}(k' \mid k)$ (since A/G embeds in $\mathrm{Gal}(k' \mid k)$ which embeds in $\mathrm{Gal}(k'F \mid F)$).

Since k' is linearly disjoint from both E and F, viewed as extensions of k, we have that $n = |E : F| = |Ek' : Fk'|$. Since $G \cap H \cong \mathrm{Gal}(L \mid k'E)$, the index of $G \cap H$ in G is n. Thus G is transitive on the A-set A/H.

We can take E and F to be function fields of k-varieties and the extension $E \mid F$ arising from a separable map between varieties. One of the original motivations for studying problems of this sort was the particular case when E and F are function fields of curves over k.

We say that $E \mid F$ is indecomposable if it is a minimal field extension. This is equivalent to saying that A acts primitively on A/H. We say that $E \mid F$ is geometrically indecomposable if $Ek' \mid Fk'$ is a minimal field extension, or equivalently G is primitive on A/H (this terminology comes from the case of considering covers of curves).

We recall a theorem [G2] of the first author in this setting. If $E \mid F$ is indecomposable and k is procyclic (its absolute Galois group is procyclic; eg., if k is finite), then $|k' : k| < n$. Another theorem of a similar nature had been obtained earlier by Aschbacher and the first author in [AG2]. If $E \mid F$ is indecomposable and $K \mid F$ is an abelian extension (a Galois extension whose Galois group is abelian) with $K \subseteq L$, then $|K : F| \leq n$.

We now recast two of our results using the notation and assumptions made above. Theorem 1.7 implies the following.

Theorem 1.9. $|k' : k| \leq 4^{n/\sqrt{\log n}} \cdot n^{\log n}$ *for* $n \geq 2$.

Theorem 1.1 can be stated in the following form.

Theorem 1.10. *Let* $E \mid F$ *be geometrically indecomposable. Then* $|k' : k| < n$ *unless the pair* $(n, \mathrm{Gal}(k' \mid k))$ *is among the eleven exceptions in Theorem 1.1. Moreover if* $\mathrm{Gal}(k' \mid k)$ *is not a section of* $\Gamma\mathrm{L}_1(q)$ *when* $q = n$ *is a prime power, then* $|k' : k| < n^{1/2} \log n$ *for* $n \geq 2^{14000}$.

Finally we discuss the situation when the extension $E \mid F$ is indecomposable.

Theorem 1.11. *If* $E \mid F$ *is indecomposable, then* $|k' : k| < n^{\log n}$.

Proof. If $|A| < n^{1+\log n}$ or if A is simple, the result follows. Otherwise, by [M, Theorem 1.1], we have that A is a subgroup of $\mathrm{S}_m \wr \mathrm{S}_r$ containing $N = (\mathrm{A}_m)^r$, where the action of S_m is on k-element subsets of $\{1, \ldots, m\}$ and the wreath product has the product action of degree $n = \binom{m}{k}^r$. It can be shown that N is the unique minimal normal subgroup of A and so $|A/G| \leq |A/N| < n^{\log n}$. $\square$

It follows by [GS] that Theorems 1.9, 1.10, 1.11 are in fact equivalent to the corresponding group theoretic theorems.

1.3. **Structure of the paper.** In this subsection we provide an overview of the present paper. The paper is organized as follows.

(1) Let $G \lhd A$ be certain finite groups. In Section 2 a technical result (see Theorem 2.3) is proved to bound the product $b(A/G)$ of the sizes of the nonabelian composition factors of a composition series of the factor group A/G. In specific situations this is an important tool in dealing with non-abelian composition factors.
(2) Section 3 provides some examples of groups $G \lhd A \leq \mathrm{S}_n$ for which $b(A/G)$ is large. These examples demonstrate the sharpness of some of our main results. In particular, Example 3.3 sheds more light on the eleven exceptions in Theorem 1.1 and also on the seven exceptions in Theorem 1.2.
(3) Let $G \lhd A \leq \mathrm{GL}(V)$ be finite groups where V is a finite vector space. Suppose that V is an irreducible G-module. The purpose of Section 4 is to bound $b(A/G)$ in terms of $n = |V|$. Theorem 4.2 states that if $n \geq 3$, then $b(A/G) < (\log n)^{2 \log \log n}$.
(4) Section 5 finishes the sole treatment of nonabelian composition factors and this is where the proof of Theorem 1.4 is completed. This is done by proving Theorem 5.1 and Theorem 5.2. Note that Theorem 5.1 is also used in Section 4.
(5) For a finite group G and a prime p let $a_p(G)$ be the product of the orders of the p-solvable composition factors in a composition series for G. The key observation (see Theorem 6.4) in Section 6 is that for any finite group G and any prime p the invariant $a_p(G)$ is bounded from above by the size of a p-solvable subgroup of G. Section 6 initiates the study of abelian composition factors and establishes a part of Theorem 1.5.

(6) Section 7 introduces the basic tools for working with abelian composition factors. Lemma 7.1 collects a few results on the closely related invariant $t_G(V)$ which, for a finite group G, is defined to be the smallest number r such that every submodule of a G-module V can be generated by r elements. This result is used to show Theorem 1.7. Lemmas 7.7 and 7.8 are basic tools concerning the solvable group $\mathrm{Out}(S)$ where S is a nonabelian finite simple group.

(7) We consider groups G and A with $G \lhd\lhd A \leq \mathrm{S}_n$. In Section 8 we prove Theorem 1.8 stating that $|A : G| \leq 5^{n-1}$ provided that G is transitive. However later a stronger bound with a stronger hypothesis is needed (see Theorem 8.1).

(8) In Section 9 an important structure theorem is given for primitive linear groups and this is applied for groups acting on a vector space of size larger than 3^{16}. In particular Theorem 9.3 is proved stating that $a(A/G) < n$ where $G \lhd A$ are primitive permutation groups of degree $n \geq 3^{16}$. Here $a(A/G)$ is the product of the sizes of the abelian composition factors in a composition series for A/G.

(9) While Section 9 deals only with abelian composition factors ($a(A/G)$), Section 10 considers both abelian and nonabelian composition factors of finite groups ($a(A/G)$ and $b(A/G)$), still assuming that the number of elements in the vector space (or the permutation domain of an affine permutation group) is larger than 3^{16}.

(10) In Section 11 we continue the previous investigations. However here the vector space (or the permutation domain) has size at most 3^{16}. This is the section where the first half of the proof of Theorem 1.1 is completed. Special care is required here because all the eleven exceptions in Theorem 1.1 satisfy $n \leq 3^{16}$.

(11) In Section 12 we bound the size of the outer automorphism group of a primitive permutation group of degree n. It turns out that a bound of n is a natural estimate (with few exceptions). Use of deep properties of the first cohomology group are required. In this section Theorem 1.2 is proved which may be considered as an extension of the first half of Theorem 1.1.

(12) In Section 13 we continue the study of the invariant $a_p(G)$ for a finite group G and a prime p. We use the methods and results we developed in earlier sections and we complete the proof of Theorem 1.5. We work with the so-called Pálfy-Wolf constant.

(13) For a finite group G let $c(G)$ denote the product of the orders of the central chief factors in a chief series for G. In Section 14 this invariant is considered when G is a primitive permutation group. It again turns out that affine primitive groups G are of central importance. The aim of the section is to prove Theorem 1.6.

(14) Finally, in Section 15 we use slightly different methods to prove asymptotic statements holding for very large values of n. This is where the missing parts of the statements of the Introduction are established. These are the second half of Theorem 1.1 and Theorem 1.3.

2. Basic results on nonabelian composition factors

If G is a finite group, define $b(G)$ to be the product of the orders of all the nonabelian simple composition factors of G in a composition series for G. Two trivial observations that we shall use without comment are:

1. if G is normal in A, then $b(A) = b(A/G)b(G)$; and

2. if $A \leq B$, then $b(A) \leq b(B)$ (choose a normal series for B and intersect A with this series – abelian quotients stay abelian and the nonabelian quotients can only get smaller).

The first lemma of the paper is not used in later parts of the work, nevertheless it is worth mentioning.

Lemma 2.1. Let X_1 and X_2 be two finite groups, $A \leq X_1 \times X_2$, and $G \lhd A$. For $i = 1, 2$ let π_i denote the projection into X_i. (We consider $\pi_i(A)$ and $\pi_i(G)$ as subgroups of X_i.) Then

$$b(A/G) \leq b(\pi_1(A)/\pi_1(G))b(\pi_2(A)/\pi_2(G)).$$

Proof. Let K denote the kernel of π_1 on A. Notice that if $x \in \pi_2(K)$ and $y \in \pi_2(G)$ then $[x, y] \in \pi_2(G \cap K)$. Hence $b((\pi_2(K) \cap \pi_2(G))/\pi_2(K \cap G)) = 1$. From this we get

$$b(K/(K \cap G)) = b(\pi_2(K)/(\pi_2(K \cap G))) = b(\pi_2(K)/(\pi_2(K) \cap \pi_2(G))) =$$

$$= b(\pi_2(K)\pi_2(G)/\pi_2(G)) \leq b(\pi_2(A)/\pi_2(G)).$$

Since $b(A/G) = b(A/GK)b(GK/G) = b(\pi_1(A)/\pi_1(G))b(K/(K \cap G))$, the result follows. □

The next lemma is needed for a technical result (see Theorem 2.3) for dealing with nonabelian composition factors.

Lemma 2.2. Let $J \leq Y := X_1 \times \cdots \times X_t$ and assume that $\pi_i(J) = X_i$ for all i (where π_i is the projection onto the ith factor). Then $N_Y(J)/J$ is solvable.

Proof. Set $N = N_Y(J)$. Let M be the final term in the derived series of N. Let $B_i = \ker \pi_i' \cap J$ where π_i' is the projection of Y onto the direct product of all but the ith term (so $B_i = J \cap X_i$).

Set $R = B_1 \times \cdots \times B_t$. Note that $R \lhd J$ and that R is also normal in Y since $\pi_i(J) = X_i$ for all i, whence we may pass to Y/R. If we prove the result in this case, then $MR/R \leq J/R$, and so $M \leq J$. Hence we may assume from now on that $R = 1$. If we prove the result in this case, then $MR/R \leq J/R$, whence $M \leq J$.

We induct on t. If $t = 1$, the result is clear.

Suppose that $t = 2$. Since $R = 1$, we may identify J as a diagonal subgroup of $X_1 \times X_2$ and the normalizer N is $J(Z \times Z)$ where $Z = Z(J)$, whence the result.

So now assume that $t > 2$. By induction, we have $\pi_i'(M) \leq \pi_i'(J)$, whence $M \leq J(N \cap X_i)$. Note that $[N \cap X_i, X_i] = [N \cap X_i, J] \leq X_i \cap J = 1$. Thus, $M = [M, M] \leq [J(N \cap X_i), J(N \cap X_i)] \leq J$ as claimed. □

Note that the proof shows that the derived length of $N_Y(J)/J$ is at most $t-1$.

We now come to one of our major tools in studying $b(A/G)$.

Theorem 2.3. *Assume that $G \lhd A \leq B = X \wr \mathrm{S}_t = (X_1 \times \cdots \times X_t).\mathrm{S}_t = Y.\mathrm{S}_t$ and that G acts transitively on $\{X_1, \ldots, X_t\}$ by conjugation. Assume that the projection of $N_A(X_i)$ into X_i is X_i (note that $N_A(X_i) \leq X_i \times X_i'$ for an obvious choice of X_i'). Let $N_i = N_G(X_i)$ and set M_i to be the projection of N_i into X_i. Let K be the subgroup of A normalizing each X_i. Then*

$$b(A/G) \leq b(A/GK)b(X_1/M_1).$$

Proof. We have that $b(A/G) = b(A/GK)b(GK/G)$. So we only need to show that $b(GK/G) \leq b(X_1/M_1)$. Let $M = M_1 \times \cdots \times M_t$. Let $I = J_1 \times \cdots \times J_t$ where J_i is the projection of $J = K \cap G$ into X_i.

Note first that $[K, K \cap M] \leq I$ (since $[K, N_i] \leq [K, G] \leq J$). In particular, $(K\cap M)/(K\cap I)$ is abelian. By Lemma 2.2, $(K\cap I)/J$ is solvable. Thus, $(K\cap M)/J$ is solvable and in particular, $b((K \cap M)/J) = 1$. Thus,

$$b(GK/G) = b(K/J) = b(K/(K \cap M)) = b(KM/M).$$

Put $H = \{y \in Y : [g, y] \in M \text{ for all } g \in G\}$. Notice that $KM \leq H$. From this $KM/M \leq H/M \leq Y/M$ follows. Since G permutes the t direct factors transitively, we see that H/M (and so KM/M) is contained in a full diagonal subgroup of $Y/M = \prod(X_i/M_i)$. Thus, $b(KM/M) \leq b(X_1/M_1)$ as claimed. $\qquad\square$

We will use the following lemma.

Lemma 2.4. *Suppose that $n = m^t$. Then*

$$t^{\log t}(\log m)^{\log \log m} \leq (\log n)^{\log \log n}.$$

Proof. It suffices to prove that $(\log t)^2 + (\log \log m)^2 \leq (\log \log n)^2$. The right-hand side is equal to $(\log t + \log \log m)^2$, whence the result. $\qquad\square$

3. Some examples

In this section, we consider several examples with $G \lhd A \leq \mathrm{S}_n$ always with A and G transitive. The first example shows that $|A/G| = n - 1$ may hold even with G primitive and that $b(A/G)$ can be on the order of $n^{\log n}$ if we only assume that G is transitive (note that when $n = 2^a$ for an integer a, then it is easy to see that $n^{\frac{1}{2}\log n} < |\mathrm{L}_a(2)| < n^{\log n}$). The third example shows that $b(A/G)$ can be close to $(\log n)^{2\log \log n}$ even when G is primitive.

Example 3.1. *Let p be a prime. Let V be a vector space over $\mathbb{F}_p$ of dimension a. Let $A = \mathrm{AGL}_a(p) = \mathrm{AGL}(V)$ be the full group of affine transformations of V. Let G be the normal subgroup of translations.*

(1) $G \lhd A$, G is transitive on V and A is primitive on V;
(2) If $a = 1$, then G is primitive on V and $|A/G| = p - 1$;
(3) If $a > 1$ and $(p, a) \neq (2, 2), (2, 3)$, then $b(A/G) = |\mathrm{L}_a(p)|$.

Example 3.2. *Let $C \lhd D$ be transitive groups of degree t. Let $A = A_5 \wr D$ and $G = A_5 \wr C$. Then $G \lhd A$ and they both act primitively on a set of cardinality 5^t. Then $b(A/G) = b(D/C)$. In particular, considering the previous example yields examples of primitive A and G with $b(A/G) > t^{\frac{1}{2} \log t} > (\frac{1}{3} \log n)^{(\frac{1}{2} \log \log n) - 2}$.*

For the third example and for later use the full symplectic group of dimension $2a$ (a and integer) over the prime field of order p is denoted by $\mathrm{Sp}_{2a}(p)$. Its order is $p^{a^2} \prod_{i=1}^{a} (p^{2i} - 1)$. The group $\mathrm{Sp}_{2a}(p)$ has a center of size $(2, p - 1)$, the greatest common divisor of 2 and $p - 1$, and the corresponding factor group is denoted by $\mathrm{PSp}_{2a}(p)$. We will also need the orthogonal groups in this paper however only for the field of size 2 (apart from Lemma 7.7). We denote the full orthogonal groups of dimension $2a$ (a and integer) over the field of order 2 by $\mathrm{O}_{2a}^{\epsilon}(2)$ where $\epsilon = \pm 1$. Their order is $2 \cdot 2^{a(a-1)}(2^a - \epsilon) \prod_{i=1}^{a-1} (2^{2i} - 1)$. The groups $\mathrm{O}_{2a}^{\epsilon}(2)$ have a subgroup of index 2 which we denote by $\mathrm{SO}_{2a}^{\epsilon}(2)$.

Example 3.3. *Let p be a prime. Let R be a p-group of symplectic type – i.e. $Z(R)$ is cyclic of order p or 4, $R/Z(R)$ is elementary abelian of order p^{2a} for an integer a and R has exponent p for p odd and exponent 4 for $p = 2$. Let q be a prime power such that $q - 1$ is a multiple of p and a multiple of 4 if $|Z(R)| = 4$. Then R embeds in the group $\mathrm{GL}_{p^a}(q) = \mathrm{GL}(V)$. Let N be the normalizer of R in $\mathrm{GL}(V)$ and Z the group of scalars. Then $N/RZ \cong \mathrm{Sp}_{2a}(p)$ or $N/RZ \cong \mathrm{O}_{2a}^{\epsilon}(2)$ with the latter possibility occurring when $p = 2$ and $Z(R)$ is cyclic of order 2. In particular (except for some very small cases), $b(N/R) = |\mathrm{PSp}_{2a}(p)|$ or $|\mathrm{SO}_{2a}^{\epsilon}(2)|$. Let $G = VR$ and $A = VN$. Then A and G are primitive permutation groups on V and $b(A/G) = |\mathrm{PSp}_{2a}(p)|$ or $|\mathrm{SO}_{2a}^{\epsilon}(2)|$. In particular, when $q = 3$, $p = 2$ we obtain examples where $b(A/G)$ has size approximately $(\log n)^{2 \log \log n}$.*

For the proof of Theorem 1.2 we will need more information about 2-groups of symplectic type. By [A, (23.14)] there are, for each positive integer a, two extraspecial groups of order 2^{2a+1}. These are the central product of a copies of D_8 and the central product of $a - 1$ copies of D_8 with one copy of Q_8. The first can be thought of as an orthogonal space of $+$ type and the other an orthogonal space of $-$ type. The central product of a copies of D_8 with one copy of C_4 can be thought of as a symplectic space.

4. Normalizers of irreducible linear groups – Nonabelian composition factors

In this section, we consider $G \lhd A \leq \mathrm{GL}(V) = \mathrm{GL}_d(q)$ where V is a vector space of dimension d over the finite field of order q and want to bound $b(A/G)$ when G is irreducible on V. Of course, this is a special case of the problem for general pairs of primitive groups – this is equivalent to the setup for the case of groups acting primitively on an affine space.

Recall that a subgroup A of $\mathrm{GL}(V)$ is called primitive if it preserves no additive decomposition of V (i.e. there is no A-invariant collection of subspaces $V_1, \ldots, V_t$ with $V = \oplus_i V_i$). In particular, this implies that A is irreducible and every normal subgroup of A acts homogeneously on V (i.e. any two simple submodules are isomorphic). Recall also the definition of a p-group of symplectic type (see Example 3.3).

Theorem 4.1. *Let $G \lhd A \leq \mathrm{GL}(V) = \mathrm{GL}_d(q)$. Set $n = q^d \geq 3$. Assume that G acts irreducibly on V and that A acts primitively on V. Assume that every irreducible J-submodule of V is absolutely irreducible for any normal subgroup J of G. Then $b(A/G) < (\log n)^{2 \log \log n}$.*

Proof. As we have already noted, every normal subgroup of A acts homogeneously on V. In particular, any abelian normal subgroup acts homogeneously and so is cyclic by Schur's Lemma. By hypothesis, it must be central. There is no harm in assuming that G contains all solvable normal subgroups of A (since that does not affect $b(A/G)$).

We claim that any normal subgroup R of A which is minimal with respect to being non-central is contained in G.

By the first paragraph we may assume that R is not solvable.

So $Z(R) \leq Z(A)$ consists of scalars and $R/Z(R)$ is characteristically simple. So either R is a central product of say t quasisimple groups Q_i (with $Q_i/Z(Q_i)$ all isomorphic) or $R/Z(R)$ is an elementary abelian r-group for some prime r. In the second case it follows easily that R is of symplectic type with $|R/Z(R)| = r^{2a}$ for some a, however we may exclude this case in the proof of the claim since R must be non-solvable.

So R is perfect. Since G acts irreducibly, $C_A(G) = Z(A)$. In particular, R cannot centralize G. Suppose that R is not contained in G. Then $G \cap R \leq Z(A)$. It follows by the Three Subgroup Lemma [A, Page 26] that $R = [R, R]$ centralizes G, a contradiction.

This proves our claim that every normal subgroup of A which is minimal with respect to being non-central is contained in G.

Let $J_1, \ldots, J_k$ denote the distinct normal subgroups of A that are minimal with respect to being noncentral in A. Let $J = J_1 \cdots J_k$ be the central product of these subgroups. We have shown that $J \leq G$. Then $C_A(J) = Z(A)$ (for otherwise the normal subgroup $C_A(J)$ of A would contain a normal subgroup, say J_1 of A which is minimal with respect to being non-central, then $J_1 \leq Z(J)$ which implies that J_1 is abelian).

Thus, $A/Z(A)J$ embeds into the direct product of the outer automorphism groups of the normal subgroups of A which are minimal subject to being non-central. If J_i is such a normal subgroup and is perfect with t components, then either $t < 5$ and this outer automorphism group is solvable or $t \geq 5$ and modulo its solvable radical is S_t.

If J_i is of symplectic type with $|J_i/Z(J_i)| = r^{2a}$, then this outer automorphism group has at most one non-solvable composition factor – $\mathrm{PSp}_{2a}(r)$ or $\mathrm{SO}_{2a}^\epsilon(2)$.

This gives us our upper bound on $b(A/J)$ and so also on $b(A/G)$. Let W be an irreducible constitutent for J. Since A is primitive on V, it follows that J acts homogeneously on V. It follows by [KL, Lemma 5.5.5, page 205 and Lemma 2.10.1, pages 47-48] that $W \cong U_1 \otimes \cdots \otimes U_k$ where U_i is an irreducible J_i-module. In particular, if J_i is the central product of t copies of a nonabelian simple group,

then $\dim U_i \geq 2^t$ and if J_i is of symplectic type with $J_i/Z(J_i)$ of order r^{2a}, then $\dim U_i = r^a$. Moreover, since U_i is absolutely irreducible, $r|(q-1)$.

A straightforward computation shows that $\prod_i b(\mathrm{Out}(J_i)) < (\log n)^{2\log\log n}$ and this finishes the proof. $\qquad\square$

Theorem 4.2. *Let $G \lhd A \leq \mathrm{GL}(V) = \mathrm{GL}_d(q)$. Set $n = q^d \geq 3$. Assume that G acts irreducibly on V. Then $b(A/G) < (\log n)^{2\log\log n}$.*

Proof. Consider a counterexample with d minimal. We claim that G acts absolutely irreducibly on V. If not, let $E = \mathrm{End}_G(V)$ and let C be the group of units in the field E. So $|E| = q^e > q$.

There is no harm in replacing G by GC and A by AC and so assume $C \leq G$. Let $A_0 = C_A(C)$. Then A/A_0 is abelian (since it embeds in the automorphism group of C) and so $b(A/G) = b(A_0/G)$. Also, viewing V as a vector space over E, G (and so A_0) certainly act irreducibly. Since $\dim_E(V) < d$ we obtain a contradiction.

So we assume that G (and so A) acts absolutely irreducibly on V.

Suppose that A preserves a field extension structure on V over $\mathbb{F}_{q^e}$ with $e > 1$. Let $A_0 = A \cap \mathrm{GL}_{d/e}(q^e)$ and $G_0 = G \cap A_0$. Let U denote V considered as a vector space over $\mathbb{F}_{q^e}$ (and as an $\mathbb{F}_{q^e}[A_0]$-module). Then A embeds in $\mathrm{GL}_{d/e}(q^e).e$. Let $W = V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^e}$. Now

$$W \cong \oplus_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^e}|\mathbb{F}_q)} U^\sigma$$

as an A_0-module. Then A permutes the U^σ. Moreover, G_0 acts irreducibly on U (or G acts reducibly on W, a contradiction to the fact that V is absolutely irreducible as a G-module). Also, A_0 acts faithfully on U (x trivial on U implies that x is trivial on U^σ for all σ, whence x is trivial on W). Then $b(A/G) = b(A_0/G_0) < (\log n)^{2\log\log n}$ contradicts the minimality of d (noting that $n = |U|$).

Suppose that A acts imprimitively on V – so $V = V_1 \oplus \cdots \oplus V_t$ with $t > 1$ and A permutes the V_i. Note that G must permute the V_i transitively as well since G is irreducible. Let K be the subgroup of A fixing each V_i. Let A_i be the action of $N_A(V_i)$ on V_i and define G_i in an analogous way. By Theorem 2.3, we have $b(A/G) \leq b(A/GK)b(A_1/G_1)$. By Theorem 5.1 (see the next section), $b(A/GK) < t^{\log t}$. Now G_1 must act irreducibly on V_1 (otherwise $K \cap G$ and so G would act reducibly on V) and so by minimality, $b(A_1/G_1) < (\log m)^{2\log\log m}$, where $m = |V_1|$. Note that $n = m^t$. So

$$b(A/G) < t^{\log t}(\log m)^{2\log\log m}.$$

The desired conclusion follows from Lemma 2.4.

The remaining case is that G is absolutely irreducibly on V, A is primitive on V and preserves no field extension structure on V. Let J be a normal subgroup of A. Then J must act homogeneously on V (by the primitivity hypothesis) and moreover, the irreducible constituents for J must be absolutely irreducible (otherwise the center of $\mathrm{End}_J(V)$ is $\mathbb{F}_{q^e}$ for some $e > 1$ and would be normalized by A, whence A preserves a field extension structure on V). Now the result follows by Theorem 4.1. $\qquad\square$

5. Normalizers of transitive and primitive groups – Nonabelian composition factors

We consider the situation $G \lhd A \leq S_n$. We wish to bound $b(A/G)$ when G is transitive and when G is primitive. It is easy to see that even if one is only interested in the primitive case, one needs an answer in the transitive case as well.

We first consider the case when G is merely transitive. We have already used this result in the previous section.

Theorem 5.1. *Let G and A be nontrivial transitive groups with $G \lhd A \leq S_n$. Then $b(A/G) < n^{\log n}$.*

Proof. Suppose the theorem is false and consider a counterexample with n minimal. First suppose that A is primitive.

Let $E := F^*(A)$ be the generalized Fitting subgroup of A. By the Aschbacher-O'Nan-Scott theorem, either E is a minimal normal subgroup or $E = E_1 \times E_2$ with $E_1 \cong E_2$ a direct product of t copies of a simple nonabelian subgroup L of order m.

In the latter case, $n = m^t$, G must contain one of the E_i and by the structure theorem together with Schreier's conjecture, we see that $b(A/G) \leq n(t!)/2 < n^{\log n}$.

In the other cases, G contains E and so we may assume that $G = E$. If E is abelian, then A/G embeds in $\mathrm{GL}_a(p)$ with $n = p^a$ for an integer a and so $b(A/G) \leq |\mathrm{L}_a(p)| < n^{\log n}$. If E is nonabelian and is the product of t copies of a nonabelian simple group L, then either $t \leq 4$ and A/G is solvable or $n \geq 5^t$ and $b(A/G) \leq (t!)/2 < n^{\log n}$.

Suppose that A is not primitive. Let $\{B_1, \ldots, B_t\}$ be an A-invariant partition of the underlying set on which A acts. Let A_i denote the action of the stabilizer of B_i in A on B_i. Then A embeds in $A_i \wr S_t$ and G permutes transitively the subgroups A_i. Let G_i denote the action of the stabilizer of B_i in G on B_i. We apply Theorem 2.3 and induction to conclude that $b(A/G) \leq t^{\log t} b(A_1/G_1) \leq t^{\log t} s^{\log s}$ where $n = st$. Thus, the result holds. $\qquad\square$

The previous and the next theorem imply Theorem 1.4.

Theorem 5.2. *Let G and A be primitive groups with $G \lhd A \leq S_n$ and $n \geq 3$. Then $b(A/G) < (\log n)^{2 \log \log n}$.*

Proof. We consider the various cases in the Aschbacher-O'Nan-Scott theorem.

In all cases, G contains $E := F^*(A)$. The result follows by Theorem 4.2 if E is abelian. So we may assume that E is a direct product of t copies of a nonabelian simple group L of order m. Let K denote the subgroup of A stabilizing all the components of a minimal normal subgroup of A. Clearly K contains E.

Suppose first that $E = E_1 \times E_2$ with $E_1 \cong E_2$ the two minimal normal subgroups of A. In this case $t = 2s$ and $n = |E_1| = m^s$. Then $GK/K \lhd A/K$ are transitive subgroups of S_s and so by Theorem 5.1, $b(A/GK) \leq s^{\log s}$. On the other hand,

K/E is solvable (because it is contained in the direct product of copies of the outer automorphism group of L). Thus, $b(A/G) = b(A/GK) \leq s^{\log s} < (\log n)^{\log \log n}$.

In the remaining cases, E is the unique minimal normal subgroup of A, the groups $GK/K \triangleleft A/K$ are transitive subgroups of S_t and so, as in the previous case, we see that $b(A/G) \leq t^{\log t}$. It follows by the Aschbacher-O'Nan-Scott theorem that $n \geq 5^t$ and so $t^{\log t} < (\log n)^{\log \log n}$. $\qquad\square$

6. p-SOLVABLE COMPOSITION FACTORS OF PRIMITIVE GROUPS

If G is a finite group, define $a(G)$ to be the product of the orders of all the abelian (i.e. cyclic) simple composition factors of G in a composition series for G. The bounds we will give in this section for $a(G)$ extend naturally to results about $a_p(G)$ defined to be the product of the orders of all composition factors of G which are either p-groups or p'-groups for a given prime p. Clearly $a(G) \leq a_p(G)$ for any prime p and, by the Odd Order Theorem, $a_2(G) = a(G)$.

It is easy to see that $a_p(G)$ (and $a(G)$) is bounded by the order of some p-solvable (solvable) subgroup $S \leq G$ (e.g., this follows from Theorem 6.4 below). By a theorem of Dixon [D] this implies (see also Dixon-Mortimer [DM]) that $a(G)$ is at most $24^{(n-1)/3}$ for any subgroup G of S_n. We state the following more general result.

Proposition 6.1. *Let $G \leq \mathrm{S}_n$. The product of the orders of all composition factors of G which are not isomorphic to alternating groups of degrees larger than $d \geq 4$ is at most $d!^{(n-1)/(d-1)}$. In particular, $a_2(G)$ and $a_3(G)$ are at most $24^{(n-1)/3}$ and $a_p(G) \leq (p-1)!^{(n-1)/(p-2)}$ for $p \geq 5$.*

Proof. The first statement follows from [M, Corollary 1.5] by using the argument implicit in the proofs of Theorem 14.2 and Lemma 14.1. $\qquad\square$

Recall that a subgroup I is *intravariant* in a group G if for all automorphisms α of G, the subgroup I^α is G-conjugate to I.

Lemma 6.2. *Let G be a finite group and let $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1$ be a normal series with each $G_i \triangleleft G$. Let $\overline{G_i} = G_{i-1}/G_i$. Let p be a fixed prime. Suppose for each i that I_i is an intravariant p'-subgroup of $\overline{G_i}$. Then G has a p'-subgroup H such that $|H| \geq \prod_{i=1}^{r} |I_i|$.*

Proof. This is a special case of [Su, Theorem 5.3.17]. $\qquad\square$

We also need a consequence [LP, Lemma 2.9] of the classification theorem of finite simple groups.

Lemma 6.3. *Let G be a nonabelian finite simple group and p a prime. Then G has a solvable intravariant p'-subgroup I such that $2|\mathrm{Out}(G)|_p \leq |I|$.*

Now we prove a useful reduction result.

Theorem 6.4. *Let G be a finite group and p a prime. Then $a_p(G) \leq |S|$ for some p-solvable subgroup S of G.*

Proof. We may assume that the largest normal p-solvable subgroup of G is trivial.

The socle L of G is a direct product $L = L_1 \times \cdots \times L_t$ of nonabelian simple groups L_i and G is embedded in $\mathrm{Aut}(L)$. Denote the kernel of the action of G on the set of subgroups L_i by K. Then G/K is a permutation group of degree t and $|G/K|_p \leq 2^t$.

Let $I_1, \ldots, I_t$ be solvable intravariant p'-subgroups of maximal orders in the groups $L_1, \ldots, L_t$. Since K/L is isomorphic to a subgroup of $\prod_{i=1}^{t} \mathrm{Out}(L_i)$, using Lemma 6.3 we see that $|I_1||I_2| \cdots |I_t| \geq 2^t |K/L|_p \geq |G/L|_p$.

It is easy to see that the subgroup $I = I_1 I_2 \cdots I_t$ is intravariant in L.

Consider now a normal series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} = L$ such that the groups G_i/L form a chief series of G/L. Every p'-factor G_j/G_{j+1} can be considered as an intravariant p'-subgroup of itself. Applying Lemma 6.2 we see that G has a p'-subgroup S whose order is greater or equal to the product of the orders of these p'-factors and $|G/L|_p$. Therefore we have $|S| \geq a_p(G)$ as required. $\qquad\square$

Combining Theorem 6.4 with well-known results of Pálfy [Pá] and Wolf [W] one obtains sharp bounds for $a(X)$ for irreducible linear groups and primitive permutation groups X. Using [HM] we extend these results even further. In the next three results $c_1 = \log_9(48 \cdot 24^{1/3})$ which is close to 2.24399.

Theorem 6.5. *If A is a finite group acting faithfully and completely reducibly on a finite vector space of size n in characteristic p, then $a(A) \leq a_p(A) \leq 24^{-1/3} n^{c_1}$.*

Proof. By Theorem 6.4 we know that there is a p-solvable subgroup S of A such that $a_p(A) \leq |S|$. Moreover, by the construction implicit in the proof of Theorem 6.4, we may assume that $O_p(S) = 1$ (since $O_p(A) = 1$). Thus S can be viewed as a finite group acting faithfully and completely reducibly on a vector space of size n. By [HM, Theorem 1.2] we have $|S| \leq 24^{-1/3} n^{c_1}$. $\qquad\square$

Corollary 6.6. *Let $1 \neq G \lhd A \leq \mathrm{S}_n$ with A primitive. Let p be a prime dividing n. Then $a(A/G) \leq a_p(A/G) \leq 24^{-1/3} n^{c_1}$.*

Proof. We use the Aschbacher-O'Nan-Scott Theorem. The affine case follows from Theorem 6.5 by noting that $|G|$ may be taken to be n. So assume that $F^*(A)$ is nonabelian and it is the direct product of t copies of a nonabelian simple group L. By our choice of p the group L (and thus $F^*(A)$) is not p-solvable.

If $F^*(A)$ is the unique minimal normal subgroup of A, then $n \geq m^t$ for some divisor m of $|L|$ which is at least the minimal degree of a permutation representation for L. In this case $a_p(A) \leq |\mathrm{Out}(L)|^t a_p(T)$ where T is a transitive permutation group on t letters. By [AG2, Lemma 2.7 (i)] we have $|\mathrm{Out}(L)| \leq (2/3)m$, and by Proposition 6.1 we have $a_p(T) \leq n$ (since m can be chosen such that $m \geq p$). These give $a_p(A) < (2/3)n^2$. This is less than $24^{-1/3} n^{c_1}$ unless $n \leq 15$ (and thus $t = 1$). If $n \leq 15$, then $a_p(A)$ is at most $|\mathrm{Out}(L)| < m = n < 24^{-1/3} n^{c_1}$.

Finally assume that $F^*(A)$ is the direct product of two minimal normal subgroups of A. In this case $n = l^{t/2}$ where $l = |L| \geq 60$. Again by [AG2, Lemma

2.7 (i)] and Proposition 6.1 we find that $a_p(A) \leq (2/3)n^2 < 24^{-1/3}n^{c_1}$ for $n \geq 60$ (since $l^{1/2} \geq p$). $\qquad \square$

This immediately implies the following sharp result (which extends the main result of [Pá] and [W]).

Corollary 6.7. *If A is a primitive permutation group of degree n and p is a prime divisor of n, then $a(A) \leq a_p(A) \leq 24^{-1/3}n^{1+c_1}$.*

This proves a part of Theorem 1.5.

7. BASIC RESULTS ON ABELIAN COMPOSITION FACTORS

Our earlier results on nonabelian composition factors in wreath products do not help in considering abelian composition factors. We use different methods for studying abelian composition factors.

The following lemma and its consequences will be crucial in proving Theorem 1.1 on the indices of primitive groups in their normalizers.

If V is a G-module over a field, let $t_G(V)$ denote the smallest number r such that every submodule of V can be generated by r elements.

Lemma 7.1. *Let $H < G$ with $|G : H| = t > 1$. Let W be an H-module over an arbitrary field and let $V = W_H^G$ be the induced module. Then we have the following.*

1) $t_G(V) \leq \frac{1}{2} \dim V$.
2) If $t \neq 2^n$ for any integer n, then $t_G(V) \leq \frac{1}{3} \dim V$.
3) If $H \triangleleft G$ and $G/H \cong C_2^n$, then $t_G(V) \leq c_n \dim V$ where $c_n = \frac{1}{2^n}\binom{n}{\lfloor n/2 \rfloor}$.
4) If $t = 2^n$ for an integer n, then $t_G(V) \leq \frac{3}{8} \dim V$, unless H is normal in G and $G/H \cong C_2$ or C_2^2. Moreover $t_G(V) \leq \frac{5}{16} \dim V$ for $t \geq 32$.

Proof. First we prove 1) and 2). By extension of scalars, we may assume that the ground field k is algebraically closed. Let p be the largest prime dividing t and let S be a Sylow p-subgroup of G.

Consider the restricted module V_S. By the Mackey decomposition, this is a direct sum of induced modules of the form $(W^g)_{H^g \cap S}^S$ with $g \in G$. Now p divides t, so $H^g \cap S$ is a proper subgroup of S for all $g \in G$. If we manage to show the proposed bounds for $t_S(V_S)$ then we are finished since $t_G(V) \leq t_S(V_S)$. Since t_S is subadditive with respective to a direct sum decomposition of V_S, it is sufficient to bound $t_S((W^g)_{H^g \cap S}^S)$ for a given $g \in G$. But this means that we may assume that $S = G$ and $H^g = H$.

Now let $c \in G$ be an element which does not lie in any conjugate of H and let $C = \langle c \rangle$. Then, as above, $C \cap H^g$ is proper in C for all $g \in G$, so by restricting V to C we may assume that G is a nontrivial cyclic p-group.

We can also assume that W is irreducible. Since H is cyclic, W is 1-dimensional and the induced module V consists of a single Jordan block, thus it can be generated by one element. That is, $t_G(V) = 1 \leq \frac{1}{p} \dim V \leq \frac{1}{2} \dim V$ as required.

Now if $t \neq 2^n$, then $p > 2$ and 2) follows.

Now we turn to the proof of 3) and 4). If $t = 2^n$, then let P be the permutation representation of G on the set of left cosets of H and let T be a Sylow 2-subgroup of G, the image of S in the permutation representation P. Then T is transitive and so the restricted module V_S is simply the induced module $W_{S \cap H}^S$, by the Mackey decomposition.

Instead of V and W, we will consider the restricted modules V_S and $W_{S \cap H}$. If $\mathrm{char}(k) \neq 2$, then V_S is semisimple and $t_G(V) \leq t_S(V) \leq \dim W$ holds. So we can assume that $\mathrm{char}(k) = 2$. Then we can assume that $W_{S \cap H}$ is irreducible, so the action of $S \cap H$ on $W_{S \cap H}$ is trivial, i.e., $W_{S \cap H}$ is the trivial 1-dimensional module. (For this notice that a composition series of $W_{S \cap H}$ corresponds naturally to a series of $\dim W$ submodules of V. For any submodule A of V we can view the intersection of A with the members of the previous series. We obtain the claim after summing dimensions corresponding to factor modules of A and by noticing that c_n can be viewed as a constant.) Then V_S is isomorphic to the regular representation module of C_2^n. Now using [KN, 3.2] we see that $t_G(V) \leq t_S(V) \leq c_n \dim V$, as required.

In proving 4), we need the following.

Claim. Let D be the permutational wreath product of a regular elementary abelian 2-group R and C_2. If g is an element of order 4 in D, then the cycle decomposition of g consists of 4-cycles.

To see this, write g in the form $g = (a, b)\tau$ where (a, b) is an element of the base group $R_1 \times R_2$ (here R_1 and R_2 are naturally identified with R) and τ is the involution in the top group. Then $g^2 = (a, b)\tau(a, b)\tau = (ab, ba)$. Since $g^2 \neq 1$, we see that ab and $ba = (ab)^{-1}$ are both different from the identity, hence they are fixed point free involutions and so is g^2 which implies the claim.

Now we will prove 4).

If T itself is not isomorphic to the regular action of C_2^n, then we prove that $t_S(V) \leq \frac{1}{4} \dim V$ from which 4) follows. We argue by induction. Let B_1, B_2 be a T-invariant partition. Let K be the stabiliser of the partition. Since K has index 2 in T, K acts as a transitive group K_i on B_i so using the inductive hypothesis, we are done unless K_1 (or equivalently, K_2) is isomorphic to the regular action of C_2^{n-1}. Then T embeds into the wreath product $K_1 \wr C_2$. Now T has an element g of order 4, otherwise T would be regular elementary abelian. By our claim, the cycle decomposition of g consists of 4-cycles. Now using the preimage of g in G we see that $t_G(V) \leq \frac{1}{4} \dim V$.

If T is isomorphic to C_2^n then our claim follows from 3). $\qquad\square$

Lemma 7.1 is used in the following result.

Lemma 7.2. *Let $X_1, \ldots, X_t$ be finite groups, X their direct product, and let G be an automorphism group of X which permutes the factors transitively. Let $K \leq X$ be a G-invariant subgroup, such that for each projection π_i of X onto X_i we have $\pi_i(K) \lhd\lhd X_i$. Set $J = [G, K]$ (and note that J is normal in K and G-invariant). Then $a(K/J) \leq (a(X_1))^{t/2}$. If $t \neq 2, 4$ then $a(K/J) \leq (a(X_1))^{3t/8}$ and if $t \geq 17$ then $a(K/J) \leq (a(X_1))^{t/3}$.*

Proof. Let Y_1 be a minimal characteristic subgroup of X_1 and let $Y = Y_1 \times \ldots \times Y_t$ where Y_i are the images of Y_1 under G. Note that

$$a(K/J) = a(K/J(K \cap Y))a((K \cap Y)J/J) = a(KY/JY)a((K \cap Y)/(J \cap Y)).$$

So by induction on the length of a characteristic series in X_1, we might assume that X_i is characteristically simple.

If X_i is elementary abelian, then X is an induced module and the result follows by Lemma 7.1. Suppose that X_i is a direct product of isomorphic copies of a nonabelian simple group. Since $\pi_i(K) \lhd\lhd X_i$, the same is true for each $\pi_i(K)$, whence K is also a direct product of copies of a nonabelian simple group. Since $J \lhd K$, K/J also has the same form, whence $a(K/J) = 1$.

If $t \neq 2, 4$ or $t \geq 17$, the same argument applies (using the stronger conclusions in Lemma 7.1). $\qquad\square$

We will use Lemma 7.2 in the above form, however in one case we will need a refined version.

Lemma 7.3. *Use the notations and assumptions of Lemma 7.2. Let $t = 4$ and for each i with $1 \leq i \leq t$ suppose that $X_i = \mathrm{GL}_2(3)$. Then $a(K/J) \leq 16^2 \cdot 3$.*

Proof. In the notation of Lemma 7.1 we have $t_G(V) \leq \frac{1}{2} \dim V$ in general, and $t_G(V) \leq \frac{1}{4} \dim V$ for $t = 4$ and $\mathrm{char}(k) = 3$. Since $|\mathrm{GL}_2(3)| = 16 \cdot 3$, the proof of Lemma 7.2 gives $a(K/J) \leq 16^{t/2} \cdot 3^{t/4} = 16^2 \cdot 3$. $\qquad\square$

We will need the following explicit exponential estimate.

Theorem 7.4. *Let $G \lhd A \leq \mathrm{S}_n$ with G transitive. Then $a(A/G) \leq 6^{n/4}$.*

Proof. If A is primitive, then our statement follows from Corollary 6.6 for $n \geq 12$ and from [GAP] for $n \leq 11$.

If A is not primitive, then choose a non-trivial partition $\{B_1, \ldots, B_t\}$ that is A-invariant with $1 < t < n$ maximal. Denote by A_1 the action of the stabilizer of B_1 in A on B_1 and denote by K the stabilizer of the partition in A. Write $n = st$. Then

$$a(A/G) \leq a(A/KG)a(K/G \cap K) \leq a(A/KG)a(K/[G, K]).$$

First suppose that t is different from 2 and 4. Then induction and Lemma 7.2 yield $a(A/G) \leq 6^{t/4} \cdot a(A_1)^{3t/8}$. By Proposition 6.1, $a(A_1) \leq 24^{(s-1)/3}$ and so

$$a(A/G) \leq 6^{t/4} \cdot 24^{(s-1)t/8} < 6^{t/4} \cdot 6^{(s-1)t/4} = 6^{st/4} = 6^{n/4}.$$

Now let $t = 2$ or $t = 4$. Then by [M, Corollary 1.4] we see that $a(A_1) \leq 6^{(s-1)/2}$, unless $s = 4$. This and the previous argument using Lemma 7.2 give the desired conclusion unless the set of prime divisors of $|A|$ is $\{2, 3\}$ and $n = 8$ or $n = 16$. But even in this case [GAP] gives the result. $\qquad\square$

An asymptotically better version of Lemma 7.1 has been obtained by Lucchini, Menegazzo and Morigi [LMM1]. The constant in their result has been evaluated by Tracey [T, Corollary 4.2].

Lemma 7.5. *Let $H < G$ with $|G : H| = t > 1$. Let W be an H-module and let $V = W_H^G$ be the induced module. Then $t_G(V) < 4\frac{t}{\sqrt{\log t}} \dim W$.*

Combining this lemma with other ideas above one can easily prove the following.

Theorem 7.6. *Let G and A be transitive permutation groups of degree $n > 1$ with $G \lhd A$. Then $a(A/G) \leq 4^{n/\sqrt{\log n}}$.*

Proof. We use the bound, the notation and the argument of Theorem 7.4. By the $6^{n/4}$ bound we see that we may assume that $n > 512$. Also, by Corollary 6.6, it is easy to see that we may assume that A is an imprimitive transitive group. Let t and s be as in the proof of Theorem 7.4. By use of Lemma 7.2 and Corollary 6.7, the result follows for $s \geq 32$ as in the proof of Theorem 7.4. If $6 \leq s < 32$, then we obtain the result using the fact that $t > 16$. Finally, if $2 \leq s \leq 5$, then $t > 100$ and the bound follows. $\square$

As pointed out in the Introduction, Theorems 7.6 and 5.1 imply Theorem 1.7.

We will also use various bounds for the orders of outer automorphism groups of simple groups.

Lemma 7.7. *Let S be a nonabelian finite simple group and suppose that S has a nontrivial permutation representation of degree n. Then $|\mathrm{Out}(S)| \leq 2 \log n$ or $S = \mathrm{L}_d(q)$ with $d > 2$ or $S = \mathrm{P}\Omega_8^+(3^e)$ with e an integer, and $|\mathrm{Out}(S)| \leq 3 \log n$. In all cases we have $|\mathrm{Out}(S)| \leq 2\sqrt{n}$. Moreover, $|\mathrm{Out}(S)| \leq \sqrt{n}$ unless $S = \mathrm{A}_6$, $\mathrm{L}_2(27)$, $\mathrm{L}_3(4)$ or $\mathrm{L}_3(16)$.*

Proof. We refer the reader to Chapter 5 of [KL] for detailed information about these degrees of permutation representations and outer automorphism groups.

In most cases we will see in fact that $|\mathrm{Out}(S)| \leq \log n \leq \sqrt{n}$ holds.

If S is sporadic, the Tits group, or an alternating group of degree other than 6, then $|\mathrm{Out}(S)| \leq 2$ and $n > 4$. Also, $|\mathrm{Out}(\mathrm{A}_6)| = 4 \leq 2 \log 6$.

So assume that S is a simple group of Lie type in characteristic p and is not an alternating group.

Suppose that $S = \mathrm{L}_2(q)$ for some power q of p. So $q > 5$ and $q \neq 9$. The smallest permutation representation is at least q and is generically $q + 1$. Also, the outer automorphism group has size $(2, q-1) \log_p q$ which is less than $\log n$ if $p = 2$ or $p \geq 5$ and is at most $2 \log n$ if $p = 3$. If $p = 3$ and $q > 9$ then $|\mathrm{Out}(S)| = 2 \log_3 q \leq \sqrt{q+1}$ unless $q = 27$.

Next consider the case that $S = \mathrm{L}_d(q), d > 2$. We may exclude $\mathrm{L}_3(2) = \mathrm{L}_2(7)$ and $\mathrm{L}_4(2) = \mathrm{A}_8$. The order of the outer automorphism group is $2(d, q-1) \log_p q$ and the smallest permutation representation is of degree $(q^d - 1)/(q - 1)$.

So $\log((q^d - 1)/(q - 1)) > (d - 1) \log q \geq 2(d, q-1) \log_p q$ unless one of the following holds.

1. $d | (q - 1)$ and $(d - 1)/2d \leq \log_p q / \log q = \log_p 2$. In this case $p \leq 7$. If $p = 7$, then $d = 3$, and if $p = 5$, then $d \leq 7$. We have

$$|\mathrm{Out}(S)| = \log_p(q^{2d}) < \log(n^{2d/(d-1)}) = 2d \log n/(d-1) \leq 3 \log n.$$

Also, note that if $d|(q-1)$, then $\log_p(q^{2d}) < ((q^d-1)/(q-1))^{1/2}$ unless $d=3$ and $q=4$ or $q=16$.

2. $(d, q-1) = d/2$ and $(d-1)/d \leq \log_p 2$. In this case $p = 2$. Also $d/2$ must be odd, whence $d \geq 6$. Thus $|\mathrm{Out}(S)| = \log(q^d) \leq (1 + 2/d)\log n \leq (4/3)\log n$. Note also that $(4/3)\log n < \sqrt{n}$ since $d \geq 6$ and $q \geq 4$.

Next consider $U_d(q)$ with $d \geq 3$. We exclude $U_3(2)$ (which is solvable).

Then the outer automorphism group has order $2(d, q+1)\log_p q$.

If $d = 3$, then the smallest permutation degree is $q^3 + 1$ (aside from $q = 5$, where it is 50). If $p > 3$, we see that $\log n$ dominates $|\mathrm{Out}(S)|$ unless $q = 5$. If $p = 3$, then $|\mathrm{Out}(S)| = 2\log_3 q$ and the result holds.

Finally, if $p = 2$ and $q > 2$ is an odd power of 2, then $|\mathrm{Out}(S)| = 6\log q$ and $n > q^3$, whence $|\mathrm{Out}(S)| < 2\log n$.

If $d = 4$, then the smallest permutation degree is $(q+1)(q^3+1)$. We see that $|\mathrm{Out}(S)| = 2(4, q+1)\log_p q$ which is less than $\log n$ unless $p = 3$ when it is at most $2\log n$.

If $d \geq 5$, then the smallest permutation representation has degree roughly q^{2d-3} and we see that $|\mathrm{Out}(S)| \leq \log n$ if $p \geq 5$ and at most $2\log n$ in any case. In all cases we have $|\mathrm{Out}(S)| \leq \sqrt{n}$.

Suppose that $S = \mathrm{P}\Omega_8^+(q)$, q odd. In this case $|\mathrm{Out}(S)| = 24\log_p q$ and the smallest permutation degree is $(q^4+1)(q^2+q+1)$. If $p \geq 5$, then we see that $|\mathrm{Out}(S)| \leq 2\log n$. If $p = 3$, then $|\mathrm{Out}(S)| \leq 3\log n$ and in any case $|\mathrm{Out}(S)|$ is at most $\sqrt{n}$.

In all other cases, $|\mathrm{Out}(S)| \leq 8\log q$ and we see that $|\mathrm{Out}(S)| < \log n$. This completes the proof. $\qquad\square$

We remark that the above lemma may be considered as a sharper version of the observation [AG2] that if $S \neq A_6$, then $2|\mathrm{Out}(S)| < n$.

A handy consequence of the lemma is that for all nonabelian finite simple groups S we have $|\mathrm{Out}(S)| \leq \sqrt[4]{|S|}$ unless $S = L_3(4)$. This follows from the known fact that the minimal degree of a permutation representation of S is less than $\sqrt{|S|}$, when $|\mathrm{Out}(S)| \leq \sqrt{n}$, and directly in the remaining cases.

We end this section with a result about dimensions versus outer automorphism groups for simple groups.

Lemma 7.8. *Let S be a nonabelian simple section of $\mathrm{SL}_n(p)$ where p is a prime. Then $|\mathrm{Out}(S)| \leq 4n$.*

Proof. For sporadic and alternating groups the result is obvious.

Suppose that S is a group in $\mathrm{Lie}(p')$ over $\mathbb{F}_r$ of (untwisted) rank ℓ. By [LP, Lemma 3.1] in this case we have $n \geq \min\{R_p(S), r^\ell\}$ where $R_p(S)$ is the minimal degree of a projective representation of S in characteristic p. Using the lower bounds of Landazuri and Seitz for $R_p(S)$ (slightly corrected in [KL, Table 5.3A])

and [KL, Table 5.1A], where values of $|\mathrm{Out}(S)|$ are given, the result follows by easy inspection.

Suppose now that S is a group in $\mathrm{Lie}(p)$. If the order of S is divisible by a primitive prime divisor of $p^m - 1$ then clearly $n \geq m$ holds. A list of the largest such numbers m is given in [KL, Table 5.2C]. Using this we see that in all cases $4m \geq |\mathrm{Out}(S)|$ holds. This completes the proof. $\qquad\square$

8. Transitive subnormal subgroups

In this section we prove an amusing variant of Theorem 1.7 for subnormal transitive subgroups by an elementary argument.

Theorem 1.8. *Let* $G \vartriangleleft\vartriangleleft A \leq \mathrm{S}_n$. *If* G *is transitive, then* $|A : G| \leq 5^{n-1}$.

Proof. Consider a counterexample with n minimal.

Let $\{B_1, \ldots, B_t\}$ be an A-invariant partition, which consists of blocks of minimal size $k > 1$ (if A is primitive, then we take $k = n$). Denote by H_i the action of the stabilizer of B_i in A on B_i. Denote by K the kernel of the action of A on the set of blocks and by K_i the action of K on B_i.

We claim that $|K : G \cap K| \leq 5^{n-t}$.

By the minimality of k the group H_1 is primitive.

If $k \leq 7$, then $|H_1| \leq |\mathrm{S}_k| \leq 5^{k-1}$. Furthermore if $k \geq 8$ and H_1 does not contain the alternating group A_k, then, by a theorem of Praeger and Saxl [PS], we have $|H_1| \leq 4^k \leq 5^{k-1}$. This implies that if $k \leq 7$, or if $k \geq 8$ and H_1 does not contain the alternating group A_k, then $|K : G \cap K| \leq |K| \leq |H_1|^t \leq 5^{n-t}$. Thus we may assume that $k \geq 8$ and that $\mathrm{A}_k \leq H_1$.

Since $K_1 \vartriangleleft H_1$, we must have $K_1 = 1, \mathrm{A}_k$ or S_k.

If $K_1 = 1$ then $K = 1$.

We may assume that K is a subdirect product of symmetric or alternating groups of degree k. Hence the derived subgroup K' is a subdirect product of alternating groups of degree k and we have $|K : K'| \leq 2^t$. Now A_k is nonabelian and simple, so the set $\{B_1, \ldots, B_t\}$ has a partition such that K' acts diagonally on the set of blocks which belong to one part of the partition and K' is the direct product of these diagonal subgroups. This partition of the set of blocks is clearly A-invariant and it follows that A acts transitively on the set of factors of the direct product, hence K' is a minimal normal subgroup of A.

Let $G = N_l \vartriangleleft N_{l-1} \vartriangleleft \cdots \vartriangleleft N_1 = A$ be a normal series of length l between G and A. Let j be the largest index with $K' \subseteq N_j$.

If $j = l$, i.e., G contains K', then $|K : G \cap K| \leq |K : K'| \leq 2^t < 5^{n-t}$.

Otherwise $N_{j+1} \cap K'$ is normal in N_j and it is properly contained in K'. Since N_j is transitive, we see that in fact K' is a minimal normal subgroup in N_j (and not just in A). Hence $N_{j+1} \cap K' = 1$, thus K' centralizes N_{j+1}. Now N_{j+1} is transitive, hence its centralizer is semiregular. However K' acts on B_1 as A_k which is impossible.

This completes the proof of the claim.

Now the permutation group GK/K is transitive on t points and it is subnormal in A/K, so we have $|A : GK| = |A/K : GK/K| \leq 5^{t-1}$. Using the claim we see that

$$|A : G| = |A : GK| |GK : G| = |A : GK| |K : G \cap K| \leq 5^{n-1}.$$

Thus the result holds. $\square$

Using the classification theorem via improved versions [KW], [M] of the Praeger-Saxl result one can improve the above bound. For example the second author [M] shows that a primitive group H of degree k not containing A_k has order $|H| < c^k$ where $c = 2.6$. This easily implies the bound $|H| \leq 3^{k-1}$. Substituting this bound in the above proof we obtain that $|A : G| \leq 3^{n-1}$. It would be interesting to see whether in fact $|A : G| \leq 2^n$ holds. This would be essentially best possible, since if n is a power of 2, then the Sylow 2-subgroup P of S_n contains a regular elementary abelian 2-subgroup of index $2^n/2n$ (which is necessarily subnormal in P). Note also that by use of [M, Corollary 1.4] the bound $|A : G| \leq 2^{n-1}$ holds in case A is primitive, unless $n = 8$, $A = \mathrm{AGL}_3(2)$, and G is regular.

In later sections we will need an improvement (relying on the classification theorem) of the previous bound in a special case.

Theorem 8.1. *Let $G \lhd A \leq S_n$. If G is transitive, then $|A : G| \leq 168^{(n-1)/7}$.*

Proof. We may use the notations and the argument of Theorem 1.8. For this purpose consider a counterexample with n minimal. For convenience set $c = 168^{1/7}$.

By the remark after the previous theorem, A cannot be a primitive permutation group. Thus $t \geq 2$ and $1 < k < n$.

We may also assume that $|H_1| > c^{k-1}$. Furthermore, H_1 not only does not contain A_k for $k \geq 8$, by the proof of Theorem 1.8, but it cannot contain A_k even for $k = 5$, 6, and 7. (For $k = 6$ we have $|K : K'| \leq 4^t$, but this is also sufficient for our purposes.) Taking this a step forward we also see that H_1 cannot be any of the groups appearing in (ii), (iii) and (iv) of [M, Corollary 1.4]. We conclude that case (i) of [M, Corollary 1.4] holds. Using the bound $|H_1| > c^{k-1}$, we may exclude two more groups from the list. Thus H_1 must be $\mathrm{AGL}_1(5)$ for $k = 5$, $\mathrm{AGL}_3(2)$ for $k = 8$, $\mathrm{AGL}_2(3)$ for $k = 9$, or $\mathrm{AGL}_4(2)$ for $k = 16$.

As in the proof of Theorem 1.8, we get

$$|A : G| = |A : GK| |GK : G| = |A : GK| |K : G \cap K| \leq c^{t-1} |K : G \cap K|.$$

But $|K : G \cap K| \leq b(H_1)(a(H_1))^{t/2} \leq |H_1|^{t/2} \leq c^{n-t}$, where the first inequality follows from Theorems 2.3 and 7.2 and the second inequality from the fact that $t \geq 2$. $\square$

9. Normalizers of primitive groups – Abelian composition factors

We consider the situation $G \lhd A \leq S_n$, G primitive and want to bound $a(A/G)$. We first consider the case when the socle of G is abelian. To deal with this case, we need the following result on primitive linear groups.

Theorem 9.1. *Let V be a finite vector space of order $n = p^b$ defined over a field of prime order p. Let B be a subgroup of $\mathrm{GL}(V) = \mathrm{GL}_b(p)$ which acts primitively (and irreducibly) on V. Let F be a maximal field such that B embeds in $\Gamma L_F(V)$. Let $|F| = p^f$ and let $d = \dim_F V$ (so $d = b/f$). Then one of the following holds.*

(1) $d = 1$ and $a(B) \le (n-1)f \le (n-1)\log n$; or
(2) $d > 1$ and $a(B) < n$ for $n > 3^{16}$.

Furthermore $a(B) < n^2/6^{1/2}$ unless $n = 9$ and $B = \mathrm{GL}_2(3)$.

Proof. Every normal subgroup of a primitive linear subgroup of $\mathrm{GL}(V)$ acts homogeneously on V. In particular, any abelian subgroup normalized by B acts homogeneously and so is cyclic by Schur's Lemma. Let C be the subgroup of nonzero elements in F (viewing F as a subring of $\mathrm{End}(V)$). Note that C is normalized by B and, for $d = 1$, contains the centralizer of B. We may replace B by BC and so assume that $C \le B$.

Let $E = \mathrm{End}_B(V)$ with $q = |E|$. The algebra generated by C is F and $|F| = q^e$ for some integer e.

Let B_0 be the centralizer of C in B. Note that C is the center of B_0. We claim that B_0 acts irreducibly on V considered as a vector space over F. For let U denote V as a B_0-module over F. Then $V' := V \otimes_E F \cong \oplus U^\sigma$, where the sum is over the elements of $\mathrm{Gal}(F \mid E)$. Since B acts absolutely irreducibly on V (over E), B acts irreducibly on V'. Note that B/B_0 acts regularly on the set $\{U^\sigma\}$ and so B_0 must act irreducibly on each U^σ and so, in particular, on U as claimed.

Note that $a(B) = a(B_0)e$ for B/B_0 is cyclic of order e.

Let R be a normal subgroup of B contained in B_0 minimal with respect to not being contained in C. If none exists, then $B_0 = C$, $d = 1$ and B' is cyclic and the first conclusion allowed holds. So assume that this is not the case. Let W be an irreducible $F[R]$-submodule of V, which, as an $F[R]$-module, is a direct sum of copies of W. Let $F' = \mathrm{End}_R(W)$.

We claim that $F' = F$. The center of the centralizer of R in $\mathrm{GL}(V)$ is the group of units of F'. This is normalized by B and so by the choice of C must just be C, whence $F = F'$. Let d_R denote $\dim_F W$.

Notice that R cannot be abelian. For if R is abelian, then so is RC. But then RC is cyclic by Schur's Lemma and so $RC = C$ by our choice of C. This is a contradiction since we chose R not to be contained in C. (By this same argument we also see that every characteristic abelian subgroup of B_0 is central and contained in C.)

So there are two possibilities for R.

1. R is of symplectic type with $R/Z(R)$ of order r^{2a} for some prime r and integer a. Since $Z(R) \le C$, it follows that $r | q^e - 1$ and $d_R = r^a$. By [LMM2, Lemma 1.7] in this case $R/Z(R)$ is a completely reducible $\mathbb{F}_r B_0$-module under conjugation.

2. R is the central product of t isomorphic quasisimple groups $Q_i, 1 \le i \le t$. Since R acts homogeneously on V and since $F' = F$, it follows that W is of the form

$W_1 \otimes \cdots \otimes W_t$ where W_i is absolutely irreducible over F (and the tensor product is taken over F). Thus $d_R = (\dim_F W_1)^t$.

Choose a maximal collection of non-cyclic subgroups described above which pairwise commute. Denote these by $J_1, \ldots, J_m$. Let $J = J_1 \cdots J_m$ be the central product of these subgroups.

We next claim that $C_{B_0}(J) = C$. Suppose not. By the maximality condition, any B-normal subgroup of $C_{B_0}(J)$ minimal with respect to not being contained in C is one of the J_i. However, J_i is nonabelian and so is not contained in $C_{B_0}(J)$.

In particular B_0/C embeds in the direct product of the automorphism groups of the $J_i/Z(J_i)$. Since J is the central product of the J_i, J acts homogeneously and F is a splitting field for the irreducible constituents for each J_i, it follows that $d = \dim_F V \geq \prod d_i$ where $d_i = d_{J_i}$.

Thus, $a(B) \leq f(p^f - 1) \prod e_i$, where the e_i are defined as follows.

If J_i is of symplectic type with $J_i/Z(J_i)$ of order $r_i^{2\ a_i}$, then if B_i denotes the (completely reducible) action of B_0 on $J_i/Z(J_i)$, we have $a(B_i) \leq (r_i^{2a_i})^{2.25}$ by Theorem 6.5. In this case we set $e_i = r_i^{6.5a_i}$.

If $J_i/Z(J_i) = L_1 \times \cdots \times L_t \neq 1$ for non-abelian simple groups L_i, then if S_i denotes the action of B_0 permuting the L_j, we have $a(S_i) \leq 24^{(t-1)/3}$ by Proposition 6.1. In this case we set $e_i = |\mathrm{Out}(L_1)|^t 24^{(t-1)/3}$. Using Lemma 7.8 we see that

$$e_i \leq 4^t\ d_{J_i} \cdot f^t \cdot 24^{(t-1)/3} \leq (d_{J_i})^{4.53} f^{[\log d_{J_i}]}.$$

Altogether we see that $a(B) \leq p^f \cdot f^{1+[\log d]} \cdot d^{6.5}$. On the other hand $n = p^{fd}$.

From this, by a tedious calculation, it follows that $a(B) < n$ whenever $n \geq 2^{40}$ (for $d > 1$). With more calculations it is possible to show that $a(B) < n$ whenever $n > 3^{16}$ and $d > 1$.

Finally, consider the last statement of the theorem. By similar calculations as before, it follows that $a(B) < n^2/6^{1/2}$ whenever $n \geq 2^{16}$ (even if $d = 1$). So assume that $n < 2^{16}$ and also that $d > 1$.

If $p^f = 2$ then no J_i is a group of symplectic type and so a closer look at our previous estimates yields $a(B) < n^2/6^{1/2}$ and $a(B) < n$ (if $d > 1$).

Let $p^f = 3$. Then $d \leq 10$, a J_i can be a group of symplectic type, but, in this case, we must have $r_i = 2$. Using this observation, a simple calculation gives $a(B) < n^2/6^{1/2}$ whenever $n > 81$.

Let $p^f = 4$. Then $d \leq 7$, a J_i can be a group of symplectic type, but, in this case, we must have $r_i = 3$ and $a_i = 1$. Using the fact that $|\mathrm{Sp}_2(3)| = 24$, the exponent 6.5 in the above estimate can be improved in this special case and we get $a(B) < n^2/6^{1/2}$ whenever $n > 64$. The same bound holds even in case $d = 1$ and $n > 64$.

Let $p^f \geq 5$. Here $d \leq 6$ and a very similar argument yields the desired bound.

Thus we only need to check the last statement of the theorem for $n \leq 81$. This was done by GAP [GAP]. $\qquad\square$

Theorem 9.2. *Let $G \lhd A \leq \mathrm{GL}(V)$ with $|V| = p^f = n$. Assume that G acts irreducibly on V. Then either A is metacyclic and $|A/G| < n$ or $a(A/G) < n$ for $n > 3^{16}$.*

Proof. Consider a counterexample with n minimal.

If A acts primitively on V, then, by Theorem 9.1, either $a(A) < n$, or A' is cyclic, A embeds in $\Gamma\mathrm{L}_1(p^f)$ and $|A| = a(A) < nf$.

Consider the latter case. Since G acts irreducibly on V over the prime field, it follows that $|G| \geq f$ (a group of order less than f will not have an irreducible module of dimension f). Thus $|A/G| < n$.

So we may assume that A acts imprimitively.

So $V = V_1 \oplus \cdots \oplus V_t$ with $t > 1$ and A permutes the V_i. Note that since G is irreducible, G must permute the V_i transitively as well. We may assume that this is done in such a way that V_1 has minimal dimension over $\mathbb{F}_p$. Set $m = |V_1|$. Since $t > 1$ and since A is irreducible on V, we have $m > 2$.

Let K be the subgroup of A fixing each V_i. Let A_i be the image of $N_A(V_i)$ acting on V_i and define G_i similarly. Since V_1 is minimal, it follows that A_1 acts primitively on V_1.

Now $a(A/G) \leq a(A/GK)a(K/(G \cap K))$. By Theorem 7.4, $a(A/GK) \leq 6^{t/4}$. By Lemma 7.2 and Theorem 9.1, $a(K/(G \cap K)) \leq a(A_1)^{t/2} < (m^2/6^{1/2})^{t/2}$ unless m is 9 and $A_1 = \mathrm{GL}_2(3)$. Thus, if $m \neq 9$, we have $a(A/G) < 6^{t/4}(m^2/6^{1/2})^{t/2} = n$.

Assume now that $m = 9$ and $A_1 = \mathrm{GL}_2(3)$.

By the restriction $n > 3^{16}$, we have $t \neq 2$, 4. Then Lemma 7.2 implies that $a(K/(G \cap K)) \leq a(A_1)^{3t/8} = 48^{3t/8}$. Hence $a(A/G) \leq \left(6^{1/4}48^{3/8}\right)^t < m^t = n$. $\square$

Theorem 9.3. *Let G and A be primitive permutation groups of degree n with $G \lhd A$. Then $a(A/G) < n$ for $n > 3^{16}$.*

Proof. We consider the various cases in the Aschbacher-O'Nan-Scott Theorem.

In all cases, G contains $E := F^*(A)$. The result follows by Theorem 9.2 if E is abelian. So we may assume that E is a direct product of t copies of a nonabelian simple group L of order l. Let K denote the subgroup of A stabilizing all the components.

Suppose first that $E = E_1 \times E_2$ with $E_1 \cong E_2$ the two minimal normal subgroups of A. In this case $t = 2s$ for some integer s and $n = |E_1| = l^s$. Then the groups $GK/K \lhd A/K$ can be considered as transitive subgroups of S_s and so by Theorem 7.4, $a(A/GK) \leq 6^{s/4}$. By Lemma 7.2, $a(GK/G) = a(K/G \cap K) \leq |\mathrm{Out}(L)|^s$. Hence $a(A/G) \leq n^{1/4} \cdot 6^{s/4}$ unless $L = \mathrm{L}_3(4)$ by a remark after Lemma 7.7. This is certainly less than n since $l \geq 60$. The same follows for $L = \mathrm{L}_3(4)$ by direct computation.

In the remaining cases, E is the unique minimal normal subgroup of A, the groups $GK/K \lhd A/K$ are transitive subgroups of S_t and so as in the previous case, we see that $a(A/GK) \leq 6^{t/4}$. Here $n \geq m^t$ where m is at least the minimal degree

of a nontrivial permutation representation of L. By Lemmas 7.2 and 7.7 it follows that $a(GK/G) \leq |\mathrm{Out}(L)|^{t/2} \leq (2\sqrt{m})^{t/2}$. Hence $a(A/G) \leq n^{1/4} \cdot 2^{t/2} \cdot 6^{t/4}$ which is less than n if $m \geq 5$. $\qquad\square$

10. NORMALIZERS OF PRIMITIVE GROUPS – SIZES

We continue to consider the situation $G \lhd A \leq \mathrm{S}_n$, G primitive and want to bound $|A/G|$. We first consider the case when the socle of G is abelian. To deal with this case, we need the following result on primitive linear groups.

Theorem 10.1. *Let V be a finite vector space of order $n = p^b$ defined over a field of prime order p. Let A be a subgroup of $\mathrm{GL}(V) = \mathrm{GL}_b(p)$ which acts primitively (and irreducibly) on V. Let F be a maximal field such that A embeds in $\Gamma\mathrm{L}_F(V)$. Let G be a normal subgroup of A which acts irreducibly on V. Let $|F| = p^f$ and let $d = \dim_F V$ (so $d = b/f$). Then $a(A)b(A/G) < f \cdot p^f \cdot d^{2\log d + 3}$.*

Proof. We use the description of the structure of A found in the proof of Theorem 9.1 (where this group was denoted by B). By the fourth paragraph of the proof of Theorem 4.1 we see that G contains every non-solvable normal subgroup of A which is minimal with respect to being non-central. From this the result easily follows. $\qquad\square$

We note here that, with little modification and in case $J \neq 1$, the proof of Theorem 4.1 essentially bounds $|A|/(b(G)|J|) = (a(A)b(A/G))/|J|$, where J is the product of all *solvable* normal subgroups of A (satisfying the conditions of Theorem 4.1) which are minimal with respect to being non-central. We also note that $(\log n)^{2\log\log n}$ is close to $d^{2\log d}$. However the argument in Theorem 9.1 is to be used together with Lemma 7.8 but excluding Theorem 6.5.

We continue with a simple lemma.

Lemma 10.2. *Let us use the notations and assumptions of the statement of Theorem 10.1. Put $A_0 = A \cap \mathrm{GL}_F(V)$. Suppose that A has a unique normal subgroup J contained in A_0 which is minimal subject to being not contained in the multiplicative group C of F viewed as a subset of $\mathrm{End}(V)$. If $|A/G| \geq n$, then $J \leq G$.*

Proof. Let the multiplicative group of the field $K = \mathrm{End}_G(V)$ be L.

We may assume that G is not cyclic. Indeed, otherwise $|A| < |L| \cdot |G| < n \cdot |G|$ since A acts on G by conjugation with kernel contained in L.

By the facts that G is not cyclic and a Singer cycle is self centralizing, we must have $df \geq 2$ and $|K| \leq p^{df/r}$ where r is the smallest prime factor of df.

We may also assume that G is metacyclic. Indeed, $G_0 = G \cap A_0$ is normal in A, is contained in A_0, thus it may be assumed that $G_0 \leq C$ is cyclic and thus G is metacyclic.

By considering the action of A_0 on G, we see that $|A_0| \leq |L| \cdot |G|$ since the kernel of the action is $L \cap A_0$, $G_0 \leq Z(A_0)$, and G/G_0 is cyclic. From this we have $|A/G| \leq f \cdot |L| < f \cdot p^{df/r} \leq p^{df} = n$. $\qquad\square$

We next present two useful bounds for $|A/G|$ in terms of n.

Lemma 10.3. *Let n, A and G be as in Theorem 10.1. Then we have the following.*

(1) $|A/G| < n$ for $n > 3^{16}$;
(2) $a(A)b(A/G) < n^2/6^{1/2}$ unless $n = 9$ and $A = \mathrm{GL}_2(3)$.

Proof. In case A/G is solvable, this follows from Theorems 9.2 and 9.1. Thus we may assume that A/G is not solvable. An easy computation using Theorem 10.1 shows that $|A/G| < n$ for $n \geq 2^{136}$ and $a(A)b(A/G) < n^2/6^{1/2}$ for $n \geq 2^{34}$. It is easy to see by the structure of a primitive linear group (see Theorem 9.1), that if $p^f = 2$ (where p and f are as in Theorem 10.1) and A/G is not solvable, then $n \geq 2^{243}$. Thus we may also assume that $p^f \geq 3$ (and $d \geq 4$, where d is as in Theorem 10.1).

Now straightforward calculations using Theorem 10.1 give $|A/G| < n$ for $n \geq 3^{54}$ and $a(A)b(A/G) < n^2/6^{1/2}$ for $n \geq 3^{14}$.

Let us adopt the notations and assumptions of the proof of Theorem 9.1 (with B replaced by A and B_0 replaced by A_0).

Assume that $p^f = 3$. Then we may assume that $16 < d \leq 53$ and $d \leq 13$ in the respective cases. A J_i can be a group of symplectic type, but, in this case, we must have $r_i = 2$. As in Example 3.3 the normalizer N_i in $\mathrm{GL}_{2^{a_i}}(3)$ of such a J_i satisfies $N_i/(J_i Z) \cong \mathrm{O}_{2a_i}^\epsilon(2)$ where Z is the group of scalars. (This is because $|Z(J_i)|$ must be 2 since it divides $p^f - 1$.) A straightforward computation using the structure of A (and G) gives the result.

We only comment on the bound (1) in case $n = 3^{32}$ and when the product J of all normal subgroups of A contained in A_0 which are not contained in the multiplicative group, C of F viewed as a subset of $\mathrm{End}(V)$, is solvable. When J is itself a normal subgroup of A contained in A_0 which is minimal subject to being not contained in C (a unique such), then $J \leq G$, by Lemma 10.2, and so we find that $|A/G| < n$. Otherwise, if J is a product of more than one J_i, then $|A| < n$ by the fact that the index of a proper subgroup in $\mathrm{O}_{10}^\epsilon(2)$, apart from the simple subgroup $\mathrm{SO}_{10}^\epsilon(2)$ whose index is 2, is at least 495.

Assume that $p^f = 4$. Then $13 \leq d \leq 42$ and $d \leq 11$ in the respective cases. A J_i can be a group of symplectic type, but, in this case, we must have $r_i = 3$. We are assuming that A/G is not solvable. As a result, for (2), only the case $d = 9$ has to be checked. The bound in (1) is slightly more complicated to establish (but true).

To finish the proof of (2) we may assume that $p^f \geq 5$. Then $4 \leq d \leq 9$. Using this information and Theorem 10.1 we see that $a(A)b(A/G) < f \cdot p^f \cdot d^{2 \log d + 3} < n^2/6^{1/2}$. Thus from now on we only consider (1).

Let $p^f = 5$. Then we may assume that $11 \leq d \leq 36$. In fact, by use of Theorem 10.1 we may assume that $d \leq 29$. With a computation similar to the ones above it is possible to deduce (1) in this special case.

We only comment on the case $n = 5^{16}$ and when the product J of all normal subgroups of A contained in A_0 which are minimal subject to being not contained in C is solvable. When J is itself a normal subgroup of A contained in A_0 which

is minimal subject to being not contained in C (a unique such), then $J \leq G$, by Lemma 10.2, and so we find that $|A/G| < n$. Otherwise, if J is a product of more than one J_i, then $|A| < n$ by the fact that the subgroups $\mathrm{Sp}_6(2) \times \mathrm{Sp}_2(2)$ and $\mathrm{Sp}_4(2) \times \mathrm{Sp}_4(2)$ of $\mathrm{Sp}_8(2)$ are relatively small.

Let $p^f = 7$. We may assume that $10 \leq d \leq 17$ (by use of Theorem 10.1). A straightforward computation gives the result.

Similarly, if $p^f = 8$, 9 or 11, then we may assume that d satisfies $9 \leq d \leq 16$, $9 \leq d \leq 15$ or $8 \leq d \leq 11$ in the respective cases. Straightforward computations give the result.

Let $p^f = 13$. We may assume that $d = 7$, 8 or 9. A straightforward computation gives the result except when $d = 8$ and A does not contain a non-solvable normal subgroup which is minimal subject to being not contained in C. In this latter case we may proceed as in the case $n = 5^{16}$ described above.

Let $p^f = 16$. We may assume that $d = 7$ or $d = 8$. In this case there is nothing to do since we are assuming that A/G is non-solvable.

Let $p^f = 17$. We may assume that $d = 7$ and so there is nothing to do.

Let $p^f = 19$. We may assume that $d = 6$. However there is nothing to do since A/G is non-solvable.

By $p^f \geq 23$ and Theorem 10.1, we have $d = 4$ or $d = 5$. Both these cases can easily be handled using the assumption that $n > 3^{16}$.

This finishes the proof of the lemma. $\square$

Theorem 10.4. *Let* $G \lhd A \leq \mathrm{GL}(V)$ *with* $|V| = p^d = n$. *Assume that* G *acts irreducibly on* V. *Then* $|A/G| < n$ *for* $n > 3^{16}$.

Proof. By Lemma 10.3 we may assume that A acts imprimitively on V. By Theorem 9.2 we may also assume that A/G is not solvable.

We may proceed almost as in the relevant paragraph of Theorem 4.2. We may decompose V in the form $V = V_1 \oplus \cdots \oplus V_t$ with $t > 1$ maximal such that A permutes the V_i. Note that G must permute the V_i transitively as well since G is irreducible. Let K be the subgroup of A fixing each V_i. Let A_i be the action of $N_A(V_i)$ on V_i and define G_i similarly.

Now G_1 must act irreducibly on V_1 and so by Theorem 10.1 we have the inequality $a(A_1)b(A_1/G_1) < f_1 \cdot p^{f_1} \cdot d_1^{2 \log d_1 + 3}$, where $m = |V_1| = p^{f_1 d_1}$ for certain integers f_1 and d_1. Note that $n = m^t$.

By Theorem 2.3, we have

$$|A/G| = a(A/G)b(A/G) \leq a(A/GK)b(A/GK) \cdot a(K/(G \cap K))b(A_1/G_1).$$

We have $b(A/GK) < t^{\log t}$ by Theorem 5.1. We also have $a(A/GK) \leq 6^{t/4}$ by Theorem 7.4. Thus Lemma 7.2, Theorem 9.1, and Theorem 4.2 give

$$|A/G| \leq 6^{t/4} \cdot t^{\log t} \cdot a(A_1)^{t/2} \cdot b(A_1/G_1) < 6^{t/4} \cdot t^{\log t} \cdot (m^2/6^{1/2})^{t/2} \cdot (\log m)^{2 \log \log m},$$

provided that $m \neq 9$. However we can improve this bound by use of the inequality

$$a(A_1)^{t/2} b(A_1/G_1) \leq f(m)^{t/2} (a(A_1) b(A_1/G_1)) / f(m),$$

where $f(m)$ is any upper bound for $a(A_1)$. For example if $m \neq 9$ then we get

$$|A/G| < 6^{t/4} \cdot t^{\log t} \cdot (m^2/6^{1/2})^{t/2} \cdot (a(A_1) b(A_1/G_1)) / (m^2/6^{1/2}).$$

First it will be convenient to deal with the case when $t = 2$ or $t = 4$. Then $m \neq 9$. Since $b(A/GK) = 1$, the previous inequality shows that we are done unless $b(A_1/G_1) \neq 1$. On the other hand, if $b(A_1/G_1) \neq 1$, then Lemma 10.3 gives

$$a(A_1) b(A_1/G_1) < m^2/6^{1/2},$$

provided that $m \neq 9$.

Now let t be different from 2 and 4 but at most 16.

Assume first that $m \neq 4$. By Lemma 7.2 and Theorem 8.1,

$$|A/G| < 168^{(t-1)/7} \cdot (m^{8/3}/168^{8/21})^{3t/8} \cdot (a(A_1) b(A_1/G_1)) / (m^{8/3}/168^{8/21}) <$$

$$< m^t \cdot (a(A_1) b(A_1/G_1)) / (m^{8/3}/168^{8/21}) \cdot 168^{-1/7}$$

(since $m^{8/3}/168^{8/21} > m^2/6^{1/2} > a(A_1)$ for $m \geq 5$ (and m different from 9), and $m^{8/3}/168^{8/21} > a(A_1)$ for $m = 3$ and $m = 9$). Again, we are finished if $b(A_1/G_1) = 1$. Assume that $b(A_1/G_1) \neq 1$. If $m = 81$ then we can use GAP [GAP] to arrive to a conclusion. Otherwise it is easy to see that $m \geq 625$. Since $d_1 \geq 4$, we certainly have

$$a(A_1) b(A_1/G_1) < f_1 \cdot p^{f_1} \cdot d_1^{2 \log d_1 + 3} < m^{8/3}/168^{8/21}$$

for $m \geq 625$, unless possibly if $p^f = 2$ or $p^f = 3$. If $p^f = 2$, then $d_1 \geq 3^5$, by the structure of A_1, and so the previous inequality holds. We also have the previous inequality in case $p^f = 3$ since we may assume by the structure of A_1 that $d_1 \geq 8$.

If $m = 4$ then Lemma 7.2 and Theorem 8.1 give us $|A/G| \leq 168^{(t-1)/7} \cdot 6^{3t/8}$. This is not necessarily less than 4^t, however it is for $t \leq 16$.

Now let $t \geq 17$.

By Lemma 7.2 and Theorem 8.1,

$$|A/G| < 168^{(t-1)/7} \cdot (m^3/168^{3/7})^{t/3} \cdot (a(A_1) b(A_1/G_1)) / (m^3/168^{3/7}) <$$

$$< m^t \cdot (a(A_1) b(A_1/G_1)) / (m^3/168^{3/7}) \cdot 168^{-1/7}$$

(since $m^3/168^{3/7} > m^2/6^{1/2}$ when $m \geq 4$, and $m^3/168^{3/7} > a(A_1)$ for $m = 3$ and $m = 9$). We may assume that $b(A_1/G_1) \neq 1$. Then $m = 81$ or $m \geq 625$ by the structure of A_1. If $m = 81$ then we have $a(A_1) b(A_1/G_1) < m^3/168^{3/7}$ by use of GAP [GAP]. If $m \geq 625$ then we arrive to a conclusion by use of three paragraphs up, noting that $m^{8/3}/168^{8/21} < m^3/168^{3/7}$ for $m \geq 3$. $\square$

Theorem 10.5. *Let G and A be permutation groups with $G \lhd A \leq S_n$. Suppose that G is primitive and $|A/G| \geq n$. Then A and G are affine primitive permutation groups and $n \leq 3^{16}$.*

Proof. If A is an affine primitive permutation group then the result follows from Theorem 10.4. Otherwise we may mimic the proof of Theorem 9.3 by noting that we must replace $6^{s/4}$ by $168^{s/7}$ and $6^{t/4}$ by $168^{t/7}$ in the respective cases (due to Schreier's conjecture and Theorem 8.1). $\qquad\square$

11. Small linear groups

In this section we will finish the proof of the first half of Theorem 1.1.

Let G and A be permutation groups with $G \lhd A \le S_n$. Suppose that G is primitive and $|A/G| \ge n$. We must show that the pair $(n, A/G)$ is one of the eleven exceptions in Theorem 1.1.

By Theorem 10.5 it is sufficient to consider affine primitive permutation groups of degrees at most 3^{16}.

Let V be a finite vector space of size n with $n \le 3^{16}$. Opposed to the notation of the statement of the theorem, let G and A be groups such that $G \lhd A \le \mathrm{GL}(V)$. Assume that G (and thus A) acts irreducibly on V. We must classify all possibilities for which $|A/G| \ge n$.

Let us first assume that A acts primitively on V. We use the notations and assumptions of Theorem 9.1 and its proof (with B replaced by A and B_0 replaced by A_0). We put $n = p^b$ for a prime p and integer b with the property that A is a subgroup of $\mathrm{GL}(V) = \mathrm{GL}_b(p)$ acting primitively (and irreducibly) on V. Let F be a maximal field such that A embeds in $\Gamma L_F(V)$. Let $|F| = p^f$ and let $d = \dim_F V$ (so $d = b/f$). Let the multiplicative group of F, viewed as a subset of $\mathrm{End}(V)$, be denoted by C.

If $d = 1$ then Theorem 9.2 gives $|A/G| < n$. Thus assume that $d > 1$.

As in the proof of Theorem 9.1, let J be the product of all normal subgroups of A contained in A_0 which are minimal subject to not being contained in C.

Assume that d is a prime. Then, by the proof of Theorem 9.1, J itself is a normal subgroup of A contained in A_0 which is minimal subject to not being contained in C. Moreover J is either a quasisimple group or is a group of symplectic type with $|J/Z(J)| = d^2$. In both of these cases we must have $J \le G$, by Lemma 10.2.

Assume that J is a quasisimple group. By Lemma 7.8 (and the proof of Theorem 9.1), we have $|A/G| \le 4(p^f - 1)df^2$. This is less than p^{df} for $d \ge 5$. Assume that $d = 2$. If A_5 is a factor group of J, then $|A/G| \le 2f(p^f - 1) < p^{2f}$. Otherwise, by Dickson's theorem on subgroups of $\mathrm{GL}_2(p^f)$, we have $|A/G| \le 2f^2(p^f - 1) < p^{2f}$ if p is odd, and $|A/G| \le f^2(p^f - 1) < p^{2f}$ if $p = 2$. Now assume that $d = 3$. Then, by information from [KL], we find that $|A/G| \le 6f^2(p^f - 1)$. This is smaller than p^{3f} unless $p = f = 2$. If $d = 3$ and $p = f = 2$, then, by [GAP], we get the desired estimate $|A/G| \le 4f(p^f - 1) = 24 < 64 = n$.

Let J be a group of symplectic type with $|J/Z(J)| = d^2$ where d is a prime. Then $|A/G| \le |\mathrm{Sp}_2(d)|f(p^f - 1) < d^3 f(p^f - 1) < n$ for $d \ge 5$, and also for $d = 3$ and $p^f > 4$. If $d = 3$ and $p^f = 4$, then $|A/G| \le d^3 f = 54 < 64$. Let $d = 2$. It is then easy to see that $|A/G| \le 6f((p^f - 1)/2) < p^{2f}$ since $p > 2$.

From now on we assume that d is not a prime and larger than 1.

In this paragraph let $p^f = 2$. By the structure of A described in the proof of Theorem 9.1 we know that all normal subgroups of A contained in A_0 and minimal with respect to being not contained in C are non-solvable. Moreover J has at most two non-abelian simple composition factors, since $d \leq 25$. By this, we immediately see, as in the proof of Theorem 9.1, that $|A/G| \leq 32d$. This is less than 2^d unless $d \leq 8$. If $d = 6$ or 8, then $|A/G| \leq 4d < 2^d$. For $d = 4$ the result follows by [GAP].

From now on we assume that $p^f > 2$.

In this paragraph we deal with the cases when $d = 6$, 10, 14, or 15. In these cases d is a product of two primes r_1 and r_2. First suppose that J is not solvable. If A has no solvable normal subgroup contained in A_0 which is minimal with respect to being noncentral, then it is easy to see that $|A/G| \leq f(p^f - 1) \cdot 4^2 f^2 d < p^{fd}$ since $p^f > 2$. Otherwise we get $|A/G| \leq f^2(p^f - 1) \cdot 4r_1 \cdot r_2{}^5$ (for a certain choice of r_1 and r_2). This is always less than p^{df} unless $d = 6$ and $p^f = 3$ or 4. If $d = 6$ and $p^f = 3$, then in the previous bound we must have $r_2 = 2$ and thus $|A/G| < n$. If $d = 6$ and $p^f = 4$, then we must have $r_1 = 2$ and $r_2 = 3$. In this special case we can modify our bound to $|A/G| \leq f(p^f - 1) \cdot 2 \cdot 3^5 = 12 \cdot 3^5 < 4^6 = n$. Thus we may assume that J is solvable. In this case d divides $p^f - 1$, and since $n \leq 3^{16}$, we are left to consider only the case $d = 6$ and $p^f = 7$ or 13 when $|A| < n$.

We are left to consider the cases when $d = 4$, 8, 9, 12, or 16.

Let $d = 4$.

First assume that J is solvable and it is the unique normal subgroup of A contained in A_0 which is minimal subject to being not contained in C. By Lemma 10.2 we may assume that $J \leq G$. For $p^f \geq 7$ we can bound $|A/G|$ by $f((q^f - 1)/2)|\mathrm{Sp}_4(2)| = 360f(q^f - 1) < p^{4f}$. We are left to consider the cases when $p^f = 3$ and $p^f = 5$. If $p^f = 3$, $d = 4$ and $|A/G| \geq 81$, then $(n, A/G) = (3^4, \mathrm{O}_4^-(2))$, while if $p^f = 5$, $d = 4$ and $|A/G| \geq 625$, then $(n, A/G) = (5^4, \mathrm{Sp}_4(2))$. Now assume that J is solvable and it is the product of two normal subgroups, say J_1 and J_2 of A contained in A_0 which are minimal subject to being not contained in C. If $f = 1$ then G contains one (if not both) of these normal subgroups, say J_1. Furthermore, since J_1 is not irreducible on V, the irreducible group G properly contains J_1. Thus $|A/G| \leq 4 \cdot 36 \cdot ((p^f - 1)/2) \cdot (1/2) = 36(p - 1) < p^4$. We may now assume that $f \geq 2$ (and also that p is odd). In this case we only use the fact that $|G| \geq 4$ to conclude that $|A/G| \leq f(p^f - 1)16 \cdot 36 \cdot (1/4) = 144f(p^f - 1)$. We already know from the same paragraph that this is less than p^{4f} for $p^f \geq 9$.

Secondly assume that A has no solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. In this case J has at most two non-abelian composition factors and so $|A/G| \leq f^3(p^f - 1) \cdot 4^3 \cdot 2 = 128f^3(p^f - 1)$, by the second half of the proof of Theorem 9.1. From this we get $|A/G| < p^{4f}$ unless possibly if $p^f = 3$, 4, 8, 9 or 16. When J has a unique non-abelian composition factor, then we may sharpen our bound to $|A/G| \leq 16f^2(p^f - 1)$, and this is smaller than p^{4f} for the remaining five values of p^f. Thus J has exactly two non-abelian composition factors. In this case we can apply Dickson's theorem on subgroups of $\mathrm{GL}_2(p^f)$ to refine our bound on $|A/G|$ even further. This is $8f^3(p^f - 1)$ which is smaller than p^{4f} for the remaining five values of p^f.

Thirdly there are two normal subgroups of A contained in A_0 which are minimal subject to not being contained in C. One is J_1, a symplectic 2-group, and one is J_2, a quasisimple group. In this case we have $|A/G| \leq f(p^f - 1) \cdot 2f \cdot 24 = 48f^2(p^f - 1)$. This is less than p^{4f} where $p > 2$, unless $p^f = 3$. But $p^f = 3$ cannot occur in this case since $J_2 \leq \mathrm{GL}_2(3)$ is solvable.

From now on let d be 8, 9, 12 or 16.

In this paragraph suppose that A has no solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. In this case the number, say r of non-abelian composition factors of J is at most 4. If $r = 4$ then $d = 16$ and so $p^f = 3$. In this case it is easy to see that $|A/G| \leq 98304f^5(p^f - 1) < 3^{16}$. Let $r = 3$. Then $d = 8$ or $d \geq 12$. In the first case we can use Dickson's theorem to conclude that a quasisimple subgroup Q of $\mathrm{GL}_2(p^f)$ satisfies $|\mathrm{Out}(S/Z(S))| \leq 2f$. This implies that $|A/G| \leq 48f^4(p^f - 1) < p^{8f}$. In case $d \geq 12$ we can use our usual bound $|A/G| \leq f^4(p^f - 1) \cdot 4^3 \cdot 16 \cdot 6 = 6144f^4(p^f - 1) < p^{12f}$. Finally let $r \leq 2$. Then $|A/G| \leq 512f^3(p^f - 1)$. This is less than p^{fd} for $d \geq 8$ (and $p^f > 2$).

In the remaining cases A has a solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. This implies that the greatest common divisor of d and $p^f - 1$ is larger than 1. This, the above, and the fact that $n \leq 3^{16}$ imply that the only cases to deal with are the following: $d = 8$ and $p^f = 3$, 5, 7, 9; $d = 9$ and $p^f = 4$, 7; $d = 12$ and $p^f = 3$, 4; and $d = 16$ and $p^f = 3$.

Let $d = 8$. We may assume that A has a solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. First suppose that J is not solvable. Then J has one or two non-abelian composition factors. Such a composition factor can be considered as a subgroup of $\mathrm{L}_2(p^f)$ or of $\mathrm{L}_4(p^f)$. In the first case we must have $p^f \geq 5$. Suppose J has exactly one non-abelian composition factor. If this is a subgroup of $\mathrm{L}_2(p^f)$, then, by Dickson's theorem, we have the estimate $|A/G| \leq f(p^f - 1) \cdot 2f \cdot |\mathrm{Sp}_4(2)| \cdot 2^4 < p^{8f}$ for $p^f \geq 5$. If this is considered as a subgroups of $\mathrm{L}_4(p^f)$, then $|A/G| \leq f(p^f - 1) \cdot 16f \cdot |\mathrm{Sp}_2(2)| \cdot 4 < p^{8f}$. Finally, if J has exactly two non-abelian composition factors, then these must be subgroups of $\mathrm{L}_2(p^f)$, and we have $|A/G| \leq f(p^f - 1) \cdot (2f)^2 \cdot 2 \cdot |\mathrm{Sp}_2(2)| \cdot 4 < p^{8f}$ for $p^f \geq 5$. Thus we may assume that J is solvable. First assume that $p^f = 9$. If A has more than one normal subgroup contained in A_0 which is minimal subject to not being contained in C, then $|A| \leq 2 \cdot 8 \cdot |\mathrm{Sp}_4(2)||\mathrm{Sp}_2(2)| \cdot 2^6 < 9^8$. Otherwise we may assume that $J \leq G$, by Lemma 10.2, and so $|A/G| \leq 2 \cdot 8 \cdot |\mathrm{Sp}_6(2)| < 9^8$. We may now assume that $p^f = 3$, 5, or 7. In all of these cases $A_0 = A$. First suppose that A has more than one normal subgroup which is minimal subject to not being contained in C. If $p^f \neq 3$, then $|A/G| \leq 16 \cdot 3 \cdot |\mathrm{Sp}_4(2)||\mathrm{Sp}_2(2)| < p^{8f}$. Let $p^f = 3$. If $|G| \geq 16$, then $|A/G| \leq 8 \cdot |\mathrm{O}_4^-(2)||\mathrm{O}_2^-(2)| < 3^8$. Otherwise $|G \cap J| = 8$ and in fact $|G| = 8$. But such a group G cannot act irreducibly on V. We conclude that J is the unique normal subgroup of A which is minimal subject to not being contained in C. Thus $J \leq G$. If $p^f = 7$, then $|A/G| \leq |\mathrm{O}_6^-(2)| < 7^8$. Let $p^f = 5$. Assume that A is the full normalizer of J in $\mathrm{GL}(V)$. If $G = J$, then $(n, A/G) = (5^8, \mathrm{Sp}_6(2))$. Otherwise, since $A/J \cong \mathrm{Sp}_6(2)$ is simple, $G = A$. Thus we may assume that A/J is a proper subgroup of $\mathrm{Sp}_6(2)$. By [DM, pp. 319], we have $|A/G| \leq |A/J| \leq |\mathrm{Sp}_6(2)|/28 < 5^8$. We remain with the case $p^f = 3$. If $G = J$ and $J \leq A$ has index at most 2 in the full normalizer of J in $\mathrm{GL}(V)$, then

$|A/G| > n$ and $(n, A/G) = (3^8, \mathrm{O}_6^-(2))$, $(3^8, \mathrm{SO}_6^-(2))$, $(3^8, \mathrm{O}_6^+(2))$ or $(3^8, \mathrm{SO}_6^+(2))$. Suppose now that $J \leq A$ has index larger than 2 in the full normalizer of J in $\mathrm{GL}(V)$. Since $\mathrm{SO}_6^+(2) \cong \mathrm{A}_8$ and $\mathrm{SO}_6^-(2) \cong \mathrm{U}_4(2)$ are simple groups with minimal index of a proper subgroup 8 and 27 respectively (for the latter see [DM, pp. 317]), we immediately get $|A/G| \leq |A/J| < 3^8$ in the remaining cases.

Let $d = 9$. We may assume that A has a solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. If J is non-solvable, then, by the structure of A (and G), $|A/G| \leq f(p^f - 1) \cdot 4 \cdot 3f \cdot 3^2 \cdot |\mathrm{Sp}_2(3)| < p^{9f}$. Thus J is solvable. If $p^f = 7$ then an easy computation yields $|A| \leq 6 \cdot 81 \cdot |\mathrm{Sp}_4(3)| < 7^9$. We assume that $p^f = 4$. Now J is the product of one or two normal subgroups of A not contained in C. If one, then we may assume by Lemma 10.2 that $J \leq G$. In this case we get $|A/G| \leq 2 \cdot |\mathrm{Sp}_4(3)| < 4^9$. In the other case we get $|A| \leq 6 \cdot 81 \cdot |\mathrm{Sp}_2(3)|^2$. Since $|G| > 2$, we see that $|A/G| < 4^9$.

Let $d = 12$. We may again assume that A has a solvable normal subgroup contained in A_0 which is minimal subject to not being contained in C. We may also assume that J is not solvable since p^f is 3 or 4. If J has one non-abelian composition factor, then $|A/G| \leq f(p^f - 1) \cdot 4 \cdot 6f \cdot 16 \cdot |\mathrm{O}_4^-(2)| = f^2(p^f - 1) \cdot 46080 < p^{12f}$ for both $p^f = 3$ and $p^f = 4$. Finally, if J has two non-abelian composition factors, then $|A/G| \leq f(p^f - 1) \cdot 4^2 \cdot 4 \cdot f^2 \cdot 2 \cdot 9 \cdot |\mathrm{Sp}_2(3)| = f^3(p^f - 1) \cdot 27648 < p^{12f}$ for both $p^f = 3$ and $p^f = 4$.

Let $d = 16$. Then $p^f = 3$ and $A_0 = A$. From the above we may assume that A has a solvable normal subgroup which is minimal subject to not being contained in C. Assume first that J is not solvable. Since $\mathrm{GL}_2(3)$ is solvable and 3 does not divide 16, we know that J has a unique non-abelian composition factor and this can be considered as a subgroup of $\mathrm{L}_4(3)$. From this we arrive to a conclusion by $|A/G| \leq f(p^f - 1) \cdot 4 \cdot (4f) \cdot |\mathrm{O}_4^-(2)| \cdot 2^4 < 3^{16}$. Thus we may assume that J is solvable. First assume that A contains more than one normal subgroup which is minimal subject to not being contained in C. In this case $|A/G|$ is at most $2^6 \cdot |\mathrm{O}_6^-(2)||\mathrm{O}_2^-(2)| < 3^{16}$. Thus we may assume that J is the unique normal subgroup of A which is minimal subject to not being contained in C. This implies that $J \leq G$. If $G = J$ and $J \leq A$ has index at most 2 in the full normalizer of J in $\mathrm{GL}(V)$, then $|A/G| > n$ and $(n, A/G)$ is $(3^{16}, \mathrm{O}_8^-(2))$, $(3^{16}, \mathrm{SO}_8^-(2))$, $(3^{16}, \mathrm{O}_8^+(2))$ or $(3^{16}, \mathrm{SO}_8^+(2))$. Now $\mathrm{SO}_8^\epsilon(2)$ are simple groups with the property that every proper subgroup has index at least 119 (see [DM, pp. 319–320]). This implies that if $J \leq A$ has index larger than 2 in the full normalizer of J in $\mathrm{GL}(V)$, then $|A/G| \leq |A/J| < 3^{16}$.

We may now assume that A acts imprimitively on V. By the proofs of Theorems 9.2 and 10.4 we see that we may assume, in the notations of these proofs, that $m = 9$ and $t = 2$ or $t = 4$. In these cases $n = 3^4$ or $n = 3^8$. If $n = 3^4$, then [GAP] gives $|A/G| < n$. So assume that the second case holds. The group A is clearly solvable and so by Lemmas 7.3 and 7.4 we have $|A/G| \leq 6 \cdot 16^2 \cdot 3$. This is less than 3^8.

This completes the proof of the first half of Theorem 1.1.

12. Normalizers and outer automorphism groups of primitive groups

In this section we prove Theorem 1.2.

Let G be a primitive permutation group of degree n. Assume first that the generalized Fitting subgroup $E = F^*(G)$ of G is nonabelian. By [R, Lemma 1.1] $\mathrm{Aut}(G)$ has a natural embedding into $\mathrm{Aut}(E)$ and it acts transitively on the components of E (this is also true if G has two minimal normal subgroups). The bound follows as in the proof of the bound for $|A/G|$.

So suppose that $F^*(G) = V$ is abelian. If V is central, then n is a prime, G is cyclic and $\mathrm{Out}(G)$ is cyclic of order $n - 1$. So assume that $Z(G) = 1$. In this case the centralizer of G in S_n is 1.

Lemma 12.1. *Let G be a primitive affine permutation group of degree n and H a point stabilizer. Let $V = F(G) = F^*(G)$. Then $|\mathrm{Aut}(G) : N_{\mathrm{S}_n}(G)| = |H^1(H, V)|$.*

Proof. Let N be the normalizer of G in S_n, then N embeds into $A = \mathrm{Aut}(G)$. Moreover an element $\varphi \in A$ is in N exactly when the image of a point stabilizer H of G under φ is also a point stabilizer [DM, 4.2B].

It is easy to see that A acts transitively on the complements of V hence it acts transitively on the G-conjugacy classes of such complements. It follows that $|A : N|$ equals the number of G-conjugacy classes of complements, that is, $|H^1(H, V)|$. □

Assume first that $H^1(H, V) = \{0\}$. Then $\mathrm{Out}(G) \cong N_{\mathrm{S}_n}(G)/G$. In this case we may apply Theorem 1.1. We see that if A is a permutation group of degree n and G is a primitive normal subgroup in A, then $|A/G| < n$ unless one of eleven cases holds. From these eleven exceptional pairs, (A, G), the group A is the full normalizer of G in S_n in exactly seven cases. These pairs give rise to the seven exceptions in the statement of Theorem 1.2. In order to characterize the seven groups G, the reader is referred to Example 3.3 and the paragraph that follows it.

From now on we assume that $H^1(H, V) \neq \{0\}$. So $G = VH$ with H acting faithfully and irreducibly on V. We must show that if $|\mathrm{Out}(G)| \geq n$, then (8) holds (in the statement of Theorem 1.2).

We first point out the following result in [AG1, 2.7 (c)]. See also [G1].

Lemma 12.2. *Suppose that H is a finite group acting irreducibly and faithfully on V with $H^1(H, V) \neq 0$. Then H has a unique minimal normal subgroup N of the form $L_1 \times \cdots \times L_t$ with $L_i \cong L$ a nonabelian simple group. Set $L_{i'} = C_N(L_i)$ (the product of all the other L_j). Moreover, $V = \oplus_i V_i$ where $V_i = [L_i, V] = C_V(L_{i'})$ and $|H^1(H, V)| \leq |H^1(L_1, W)|$, where W is any nontrivial irreducible L_i-submodule of V_1.*

Now we obtain bounds on the size of outer automorphism groups for such groups.

First an example. Let $q = 2^e, e > 1$ and $H = \mathrm{L}_2(q)$. Let V be the natural module for H (i.e. 2-dimensional over F_q). Consider $G = V.\mathrm{L}_2(q)$ acting on V. Then G is primitive and $|\mathrm{Out}(G)| = |H^1(H, V)||N_{\mathrm{S}_n}(G) : G| = q(q-1)e < (n \log n)/2$ but $|\mathrm{Out}(G)| > n$ and indeed has order roughly $(n \log n)/2$. We now show that this is the only example with $|\mathrm{Out}(G)| \geq n$. That will complete the proof of Theorem 1.2.

Theorem 12.3. *Let G be a primitive affine permutation group of degree n. Let $V = F(G) = F^*(G)$ and $H \neq 1$ a point stabilizer. Assume that $H^1(H, V) \neq \{0\}$. Then either $|\mathrm{Out}(G)| < n$ or $n = q^2$ with $q = 2^e, e > 1$ and $H = \mathrm{L}_2(q)$.*

Proof. We use the lemma above and write $V = \oplus V_i$ where $V_i = [L_i, V]$. Let N be the normalizer of L_1. Then N preserves V_1 and indeed N is precisely the stabilizer of V_1. Since H is irreducible on V, N is irreducible on V_1. Let $E = \mathrm{End}_H(V)$. So E is a field of size q. By Frobenius reciprocity, $E \cong \mathrm{End}_N(V_1)$. Let $d = \dim_E V_1$ and $h_1 = |H^1(H, V)|$.

So $H^1(H, V)$ embeds in $H^1(L_1, U_1)$ where U_1 is an L_1-submodule of V_1. Now we know that $|\mathrm{Out}(G)| \leq (q-1)h_1|N_J(H)/H|$ where $J = \mathrm{Aut}(\mathrm{L}) \wr \mathrm{S_t}$.

Suppose that $t = 1$. Then $F^*(H) = L$ and $|\mathrm{Out}(G)| \leq (q-1)h_1|\mathrm{Out}(L)|$. We first consider some special cases.

If $d = 2$, then (since we are assuming that $h_1 > 1$), $h_1 = q$. This implies (see [GH]) that $L = \mathrm{L}_2(q)$ with $q = 2^e > 2$. Moreover, the equality on h_1 implies that $H = L$ and we are as in the example above.

Suppose that $d = 3$. Then also by the main result in [GH], it follows that $h_1 = q$. So $|\mathrm{Out}(G)| < q(q-1)\sqrt{(q^3-1)/(q-1)} < q^3$ unless possibly $L = \mathrm{A}_6$, $\mathrm{L}_2(27)$, $\mathrm{L}_3(4)$ or $\mathrm{L}_3(16)$ (see Lemma 7.7). In these exceptional cases $|\mathrm{Out}(L)|$ has order $4, 6, 12$ or 24 respectively and the result holds unless possibly $q < |\mathrm{Out}(L)|$. This easily rules out the first two cases (there are no 3-dimensional representations over a field of size $q < |\mathrm{Out}(L)|$ cf. [JLPW]). For the latter two groups, there are no 3-dimensional representations (only projective representations).

So assume that $d \geq 4$.

Suppose that $|H^1(H, V)| < |V|^{1/2}$. Since (by construction), V is an irreducible $\mathbb{F}_q[H]$-module, $|H^1(H, V)| \leq q^{(d/2)-1}$ if d is even and $|H^1(H, V)| \leq q^{(d-1)/2}$ if d is odd.

In this case, the same argument as above applies. We only need to deal with the four groups as above and only for representations where $|\mathrm{Out}(L)|$ is larger than $\sqrt{(q^d-1)/(q-1)}$. From [JLPW] we see that the only possibility is that $L = \mathrm{A}_6$ and $q = 2$, $d = 4$. In that case, $|H^1(H, V)| \leq 2$ and we still have the result.

The remaining case is when $|H^1(H, V)| = |V|^{1/2}$. This can only occur for $d = 2$ except if $H = \mathrm{A}_6$, $q = 3$ and $d = 4$ [GH]. So $n = 81$. In that case, we see that $|\mathrm{Out}(G)| \leq 9 \cdot 2 \cdot 4 = 72$ and the result still holds.

Now suppose that $t > 1$ and $n = q^{dt}$ where $d = \dim_E V_1$. Then we have $|N_J(H)/H| \leq |\mathrm{Out}(L)|^{t/2}b_t$ where b_t is the analogous bound for transitive groups of degree t. Thus by [GH], $|\mathrm{Out}(G)| \leq (q-1)q^{d/2}|\mathrm{Out}(L)|^{t/2}b_t$. By Theorem 5.1 and Theorem 7.4, we have $b_t \leq 2^t \cdot t^{\log t}$ and it is easy to see that if $t \leq 7$ then in fact $b_t \leq 2^t$ holds. Unless $L = \mathrm{A}_6$ (which we assume) we have $|\mathrm{Out}(L)| < q^d/(2(q-1))$ by [AG2, Lemma 2.7].

Assuming first that $q \neq 2$ we see that $|\mathrm{Out}(G)| < q^{d((t/2)+1)}t^{\log t}$. It is also clear that (since $\mathrm{L}_2(3)$ is solvable) in this case we have $q^d \geq 16$ and $|\mathrm{Out}(G)| < q^{dt}$ follows for $t \geq 8$ (and even for $t \leq 7$ by the observation a few lines above).

Finally let $q = 2$. Then we see that $|\mathrm{Out}(G)| \leq 2^{(d+t+dt)/2} \cdot t^{\log t}$. If $d \geq 4$ and $t \geq 8$, then this is less than 2^{dt}. Otherwise $L = \mathrm{L}_3(2)$ and in this case for $t \geq 8$ we have $|\mathrm{Out}(G)| \leq 2 \cdot 2^{t/2} \cdot 2^t \cdot t^{\log t} < 2^{3t}$. If $t \leq 7$, then $|\mathrm{Out}(G)| < 2^{dt}$ follows,

using $b_t \leq 2^t$ and Lemma 7.7, in all cases, except when $L = \mathrm{A}_6 = \mathrm{L}_2(9)$. Finally, if $L = \mathrm{A}_6 = \mathrm{L}_2(9)$, then $d \geq 6$ and $|\mathrm{Out}(G)| < 2^{dt}$ follows easily. $\square$

This completes the proof of Theorem 1.2.

13. p-SOLVABLE COMPOSITION FACTORS AND OUTER AUTOMORPHISM GROUPS

The purpose of this section is to complete the proof of Theorem 1.5.

Fix a prime p. Throughout this section we put c to be $24^{1/3}$ if $p \leq 3$ and $(p-1)!^{1/(p-2)}$ if $p \geq 5$.

The first result concerns transitive permutation groups.

Theorem 13.1. *Let $G \lhd A \leq \mathrm{S}_n$ be transitive permutation groups of degree n. Let p be a prime. Then $a_p(G)|A/G| \leq c^{n-1}$.*

Proof. We prove the result by induction on n.

First let A be a primitive permutation group. If A contains A_n, then the bound is clear. Otherwise we have $|A| \leq 24^{(n-1)/3}$ by [M].

Now let A be an imprimitive permutation group. Let $\{B_1, \ldots, B_t\}$ be an A-invariant partition of the underlying set on which A acts, with $1 < t < n$. Let A_1 denote the action of the stabilizer of B_i in A on B_i. Then A embeds in $A_i \wr \mathrm{S}_t$ and G permutes transitively the subgroups A_i. Let G_i denote the action of the stabilizer of B_i in G on B_i. By Theorem 2.3 we have $b(A/G) \leq b(A/GK)b(A_1/G_1)$ where K denotes the kernel of the action of A on $\{B_1, \ldots, B_t\}$.

In order to bound $a_p(G)$ we first set $s = |B_1|$, that is $n = st$. We have

$$a_p(G) = a_p(G/K \cap G) \cdot a_p(K \cap G) \leq a_p(GK/K) \cdot a_p(K \cap G).$$

Let N be the kernel of the action of K on B_1. We have

$$a_p(K \cap G) \cdot a(K/(K \cap G)) \leq a_p((K \cap G)N) \cdot a(K/(K \cap G)N) =$$

$$= a_p((K \cap G)N/N) \cdot a_p(N) \cdot a(K/(K \cap G)N) \leq a_p(G_1) \cdot a(A_1/G_1) \cdot a_p(N).$$

We are now in position to bound $a_p(G) \cdot |A/G| = a_p(G) \cdot a(A/G) \cdot b(A/G)$. We have

$$a_p(G) \cdot |A/G| \leq a_p(GK/K) \cdot |A/GK| \cdot a_p(K \cap G) \cdot a(K/(K \cap G)) \cdot b(A_1/G_1) \leq$$

$$\leq (a_p(GK/K) \cdot |A/GK|) \cdot (a_p(G_1) \cdot |A_1/G_1|) \cdot a_p(N).$$

By induction (noting that GK/K and G_1 are transitive on $\{B_1, \ldots, B_t\}$ and B_1 respectively), we have $a_p(GK/K) \cdot |A/GK| \leq c^{t-1}$ and $a_p(G_1) \cdot |A_1/G_1| \leq c^{s-1}$. Moreover by repeated use of Proposition 6.1, we see that $a_p(N) \leq c^{(s-1)(t-1)}$. These give $a_p(G)|A/G| \leq c^{t-1}c^{s-1}c^{(s-1)(t-1)} = c^{n-1}$. $\square$

We next need a lemma which depends on the existence of regular orbits under certain coprime actions.

Lemma 13.2. *Let A be a primitive linear subgroup of $\Gamma L_d(p^f)$ for a prime p and integers f and d with d as small as possible. Put $A_0 = GL_d(p^f) \cap A$. Let J_0 be the product of all normal subgroups of A contained in A_0 which are nonsolvable, have orders coprime to p, and are minimal with respect to being noncentral in A_0. Then either $p^f = 7$, $d = 4$ or 5, and $b(J_0) = |PSp_4(3)|$, or $b(J_0) < p^{fd}$.*

Proof. The group J_0 is a central product of quasisimple groups $J_1, \ldots, J_r$ for some r. Since $J_0 \lhd A$ and A is primitive, J_0 acts homogeneously on the underlying vector space. Let W be an irreducible J_0-submodule. As in the proof of Theorem 4.1, we may use [KL, Lemma 5.5.5, page 205 and Lemma 2.10.1, pages 47-48] to write W in the form $W_1 \otimes \cdots \otimes W_r$ where for each i the J_i-module W_i (defined over a possibly larger field) is irreducible.

Assume first that $r = 1$. If J_0 has a regular orbit on W, then the result is clear. If J_0 does not have a regular orbit on W, then [Sc, Theorem 7.2.a] says that (J_0, W) is a permutation pair in the sense of [Sc, Example 5.1.a] or (J_0, W) is listed in the table on [Sc, Page 112]. In all these exceptional cases we have $|J_0/Z(J_0)| < |W|$ unless W is a 4 or 5 dimensional module over the field of size 7 and $J_0/Z(J_0) \cong PSp_4(3)$. Moreover $|J_0/Z(J_0)| < p^{fd}$ or $|W| = p^{fd}$ and one of the previous exceptional cases holds.

Assume that $r > 1$. For each i we have $b(J_i) < |W_i|$ or $|W_i| = 7^4$ or 7^5 and $b(J_i) < |W_i|^{1.31}$. From these it follows that $b(J_0) < |W| \leq p^{fd}$. $\qquad\square$

The next lemma may be viewed as a sharper version of Theorem 6.5 under the assumption that $p \geq 7$.

Lemma 13.3. *Let G be a finite group acting faithfully and completely reducibly on a finite vector space V in characteristic p. Then $a_p(G) \leq |V|^{c_1}/c$.*

Proof. By Theorem 6.5, we may assume that $p \geq 5$. By [HM, Theorem 1.1], the strong base size of a p-solvable finite group S acting completely reducibly and faithfully on a vector space of size n over a field of characteristic $p \geq 5$ is at most 2. Thus $|S| < n^2/(p-1)$. By the proof of Theorem 6.5 we then have $a_p(G) \leq |V|^2/(p-1) \leq |V|^{c_1}/c$. $\qquad\square$

Theorem 13.1 is used in the proof of the following result which could be compared with Theorem 6.5.

Theorem 13.4. *Let $G \lhd A \leq GL(V)$ be linear groups acting irreducibly on a finite vector space V of size n and characteristic p. Then $a_p(G)|A/G| \leq 24^{-1/3}n^{c_1}$.*

Proof. We prove the result by induction on n.

Assume that A acts primitively on V. If $a_p(G) = a(G)$, then the result follows from part (2) of Lemma 10.3. In fact, in our argument to show Theorem 1.1 we naturally took G to be as small as possible and our calculations actually gave $|A/(G \cap Z(A)J)| < n$ apart from the eleven exceptions listed in Theorem 1.1 (when $a_p(G) = a(G)$). Here, as usual, J denotes the central product of all normal subgroups of A contained in A_0 (where $A_0 = GL_d(p^f) \cap A$ and d is smallest with $A \leq \Gamma L_d(p^f)$ and $n = p^f$) subject to being noncentral. Thus we are finished if

the product of the orders of the nonabelian composition factors of J which are p'-groups is at most $24^{-1/3}n^{c_1-1}$. Let J_0 be as in Lemma 13.2. By Lemma 13.2 we have $b(J_0) \leq 24^{-1/3}n^{c_1-1}$ unless $n \leq 81$ or $p^f = 7$ and $d = 4$ or 5. It can be checked by GAP [GAP] that the bound holds in case $n \leq 81$. Thus assume that $p^f = 7$ and $d = 4$ or 5 with $|b(J_0)| = |\mathrm{PSp}_4(3)|$. Then A is a $7'$-group by [Sc, Theorem 7.2.a] and so $a_7(G)|A/G| = |A| \leq 24^{-1/3}n^{c_1}$ by [HM, Theorem 1.2].

Assume that A acts (irreducibly and) imprimitively on V. Let $V = V_1 \oplus \cdots \oplus V_t$ be a direct sum decomposition of the vector space V such that $1 < t$ and A (and so G) acts transitively on the set $\{V_1, \ldots V_t\}$. Set $m = |V_1|$. Let K be the kernel of the action of A on $\{V_1, \ldots V_t\}$ and let A_1 and G_1 be the action of $N_A(V_1)$ and $N_G(V_1)$ on V_1 respectively. As in the proof of Theorem 13.1, we have

$$a_p(G) \cdot |A/G| \leq (a_p(GK/K) \cdot |A/GK|) \cdot (a_p(G_1) \cdot |A_1/G_1|) \cdot a_p(N),$$

where, in this case, N denotes the kernel of the action of K on V_1. Since the groups $GK/K \lhd A/K$ can be viewed as transitive permutation groups acting on t points, Theorem 13.1 gives $a_p(GK/K)|A/GK| \leq c^{t-1}$. In the proof of Theorem 4.2 it was noted that G_1 must act irreducibly on V_1. Thus, by the induction hypothesis, $a_p(G_1)|A_1/G_1| \leq 24^{-1/3}m^{c_1}$. Since N is subnormal in the irreducible group A, it must be completely reducible. By repeated use of Lemma 13.3 we have $a_p(N) \leq m^{c_1(t-1)}/c^{t-1}$. Applying these three estimates to the displayed inequality above, we get $a_p(G) \cdot |A/G| \leq c^{t-1} \cdot (24^{-1/3}m^{c_1}) \cdot (m^{c_1(t-1)}/c^{t-1}) = 24^{-1/3}n^{c_1}$. $\square$

We are now in the position to complete the proof of Theorem 1.5 in the special case that G is an affine primitive permutation group.

Theorem 13.5. *Let G be an affine primitive permutation group of degree n, a power of a prime p. Then $a_p(G)|\mathrm{Out}(G)| \leq 24^{-1/3}n^{1+c_1}$.*

Proof. Let H be a point stabilizer in G. We may assume that $H \neq 1$. Clearly H acts irreducibly and faithfully on a vector space V of size n. If $H^1(H,V) = \{0\}$, then Theorem 13.4 gives the result, by Lemma 12.1. So assume that $H^1(H,V) \neq \{0\}$. By Lemma 12.2, $F^*(H) = L_1 \times \cdots \times L_t$ where $L_i \cong L$ are nonabelian simple groups viewed as subgroups of $\mathrm{GL}(V_i)$ where the V_i are vector spaces with $V = \oplus_{i=1}^t V_i$. For each i put $|V_i| = p^d$ for a prime p and integer d. (See Lemma 12.2 and the proof of Theorem 12.3.)

If $n = q^2$ with $q = 2^e$ for an integer $e > 1$ and $H = \mathrm{L}_2(q)$, then, by Section 12, $a_2(G)|\mathrm{Out}(G)| < (n^2 \log n)/2 < 24^{-1/3}n^{1+c_1}$. Thus, by Theorem 12.3, we may assume that $|\mathrm{Out}(G)| < n$.

Assume first that L is not p-solvable. By Lemma 7.8 and Proposition 6.1, we have the estimate $a_p(H) \leq (4d)^t c^{t-1}$ where c is as in the beginning of this section, depending on p. For $d = 2$ and $p \geq 5$, $d = 3$ and $p \geq 3$, or $d = 4$ and $p \geq 3$, or $d \geq 5$ we have $(4d)^t c^{t-1} \leq 24^{-1/3}p^{dt(c_1-1)}$ giving the desired bound for $a_p(H)$ and thus for $a_p(G)|\mathrm{Out}(G)|$ in these cases. The only exceptions are $d = 3$ and $p = 2$, and $d = 4$ and $p = 2$. However in these cases in the previous two estimates we may replace $4d$, we obtained from Lemma 7.8, by 1 and 4 respectively. Thus we may assume that L is p-solvable (and $p \geq 3$).

Let A be the full normalizer of G in S_n. Assume that $p \geq 5$ and that A/G is not p-solvable. By Schreier's conjecture and the proof of Theorem 5.1 we must then have $t \geq 8$. By the proof of Lemma 13.3 we have $a_p(A) \leq n^3/4$. Thus, by the main result of [GH], Lemma 12.2 and Theorem 5.1, we have the estimate $a_p(G)|\mathrm{Out}(G)| \leq (n^3/4) \cdot t^{\log t} \cdot p^{d/2}$. Furthermore, by the proof of Theorem 12.3, we may also assume that $d \geq 3$ as well as $t \geq 8$. Under these conditions it easily follows that $(n^3/4) \cdot t^{\log t} \cdot p^{d/2} < 24^{-1/3}n^{1+c_1}$. Assume now that $p \geq 5$ and A/G is p-solvable. Then we must bound $a_p(A)|H^1(H,V)| \leq (n^3/4) \cdot p^{d/2}$. Using Lemma 7.8 this is smaller than the desired estimate unless $t \leq 2$. Using Lemma 13.2 we can deduce the result if $t \leq 2$ and $d \geq 4$. By the proof of Theorem 12.3 we cannot have $d = 2$ since $H^1(H,V) \neq \{0\}$ and $p \neq 2$. Thus $t \leq 2$ and $d = 3$. We then have by the proof of Lemma 13.3 that $a_p(A)|H^1(H,V)| \leq (n^3/(p-1)) \cdot p$ which is, for $n \geq 343$, less than $24^{-1/3}n^{1+c_1}$. This forces $p = 5$, $d = 3$ and $t = 1$ with $|L|$ not divisible by 5. GAP [GAP] shows that there is no such possibility.

We are left to consider the case when $p = 3$ and L is 3-solvable, that is, a Suzuki group. In this case $F^*(H)$ has a regular orbit on V by [Sc, Theorem 7.2.a]. We also have $1 < |H^1(H,V)| \leq n^{1/14}$ by [H, Table 2] and so we may assume by Lemma 12.2 that $d \geq 14$. By these, Proposition 6.1 and a remark after Lemma 7.7, $a_3(A)|H^1(H,V)| < n^3 < 24^{-1/3}n^{1+c_1}$ for $n \geq 3^{14}$. We may thus assume that $a_3(G)|\mathrm{Out}(G)| > a_3(A)|H^1(H,V)|$. Then $t \geq 8$ as in the previous paragraph and so $a_3(G)|\mathrm{Out}(G)| < n^3 \cdot t^{\log t} \cdot p^{d/14} < 24^{-1/3}n^{1+c_1}$ whenever $n \geq 3^{8 \cdot 14}$. □

Finally we finish the proof of Theorem 1.5. By Theorem 13.5 we may assume that G is a primitive permutation group of degree n with nonabelian socle E which is isomorphic to a direct product of t copies of a nonabelian simple group L. By Theorem 1.2 we know that $|\mathrm{Out}(G)| < n$ in this case and so it is sufficient to show $a_p(G) \leq 24^{-1/3}n^{c_1}$ for every prime divisor p of n. This follows from the proof of Corollary 6.6.

14. On the central chief factors of a primitive group

In this section Theorem 1.6 is proved.

For a finite group X let $c(X)$ denote the product of the orders of the central chief factors in a chief series for X. By a generalization of the Jordan-Hölder theorem, $c(X)$ is independent from the choice of the chief series for X. Clearly, $c(X) \leq c(X/N)c(N)$ for any normal subgroup N of X. The following technical lemma is not necessary but it makes our argument easier to understand.

Lemma 14.1. *Let $X = X_1 \times \cdots \times X_t$ be the direct product of finite groups X_i. Let Y be a subgroup of X such that Y projects onto every factor X_i. Then $c(Y)$ is at most $c(X) = \prod_{i=1}^{t} c(X_i)$.*

Proof. We prove the result by induction on t. In case $t = 1$ we have $Y = X$ and the result follows. Assume that $t > 1$. Write X in the form $X_1 \times X'$ where X' is the direct product of all but the first factor of X. Let N be the kernel of the projection of Y onto X_1. Then $N \lhd Y$ and $c(Y)$ is equal to $c(Y/N) = c(X_1)$ times the product, denoted by $c_Y(N)$, of the orders of the central chief factors of Y which are contained in N. Let Y' be the projection of Y into X'. Now N embeds naturally

in X' and $N \triangleleft Y'$. Observe that a chief factor of Y contained in N is central in Y if and only if it is central in Y'. From this we get $c_Y(N) = c_{Y'}(N) \leq c(Y')$. By our induction hypothesis, we get $c(Y') \leq c(X') = \prod_{i=2}^{t} c(X_i)$. $\qquad\square$

Our first result generalizes a theorem of Dixon [D] stating that a nilpotent permutation group of degree n has order at most 2^{n-1}.

Theorem 14.2. *For a permutation group G of finite degree n we have $c(G) \leq 2^{n-1}$.*

Proof. Let G act on a set Ω of size n. We prove our bound using induction on n.

If G is a cyclic group generated by an n-cycle, then $c(G) = n \leq 2^{n-1}$. Assume that G is a noncyclic primitive permutation group. Then the socle of G does not contain any central chief factor of G. If $n = 3$, 4, or 5, then inspection shows that $c(G)$ is at most 2, 3 and 4 in the respective cases. Otherwise if $n \geq 6$, then Corollary 6.6 gives $c(G) \leq 24^{-1/3} n^{c_1} < 2^{n-1}$.

Let G be an imprimitive transitive group acting on Ω. Let Σ be a system of nontrivial, proper blocks each of size k and let K be the kernel of the action of G on Σ. By Lemma 14.1 and induction, we have $c(K) \leq (2^{k-1})^{n/k}$. Thus, again by induction, we get $c(G) \leq c(G/K)c(K) \leq 2^{(n/k)-1} \cdot 2^{n-(n/k)} = 2^{n-1}$.

Finally suppose that G acts intransitively on Ω. Let Δ be a G-orbit in Ω of size k. Let K be the kernel of the action of G on Δ. By induction we have $c(G/K) \leq 2^{k-1}$ and $c(K) \leq 2^{n-k-1}$. Thus $c(G) \leq c(G/K)c(K) < 2^{n-1}$. $\qquad\square$

In the next theorem c_2 denotes the constant $\log_9 32$ which is close to 1.57732.

Theorem 14.3. *Let G be a finite group acting faithfully and completely reducibly on a finite vector space V. Then $c(G) \leq |V|^{c_2}/2$.*

Proof. Let us prove the result by induction on $n = |V|$.

Suppose that G acts irreducibly and primitively on V. First let G be a subgroup of $\Gamma L_1(p^f)$ where $n = p^f$ for a prime p and integer f. Since $p^f - 1 < n^{c_2}/2$, we may assume that $|G| > p^f - 1$. Set $G_0 = G \cap GL_1(p^f) < G$. If G_0 contains a cyclic (irreducible) subgroup of prime order q where q is a Zsigmondy prime, then $c(G) \leq f((p^f - 1)/q) < p^f - 1 < n^{c_2}/2$ since such a cyclic subgroup cannot be central in $G > G_0$ and $q \geq f + 1$. Otherwise Zsigmondy's theorem implies that $f = 2$ or $p^f = 2^6$. In both of these cases we either have $c(G) \leq |G| < n^{c_2}/2$ or $G = \Gamma L_1(p^f)$ and $c(G) = |G|$. If $G = \Gamma L_1(p^2)$, then $|G| \leq n^{c_2}/2$ unless $p = 2$ or 3 when $c(G) = 2$ and 16 respectively, with our proposed bound being sharp in the latter case. Thus we may assume that $G = \Gamma L_1(2^6)$. But in this case $c(G) < |G|$.

Let us continue to assume that G acts irreducibly and primitively on V. Let us use the notation of Theorem 9.1 with B replaced with G. By the previous paragraph we may assume that $d > 1$. By Theorem 9.1 we may also assume that $n \leq 3^{16}$. Let G_0 be B_0 in the notation of the proof of Theorem 9.1. Let J be the product of all normal subgroups of G contained in G_0 which are minimal with respect to not being contained in C.

Assume that J is a central product of quasisimple finite groups. Let $p^f = 2$. By the proof of Theorem 9.1 we may assume in this case that $16 \leq d \leq 25$, and so that

J is the direct product of at most two quasisimple groups. Then $c(G)$ is at most $a(G) \leq 32d < 2^{16} \leq n$. Let $p^f \geq 3$. Then $d \leq 16$ and J is the central product of at most three quasisimple groups. In this case $c(G) \leq a(G) \leq 384f^4d(p^f - 1)$. This is less than $p^{c_2fd}/2$ unless $d \leq 7$. Assume that $d \leq 7$. If J is a central product of two quasisimple groups, then, by Dickson's theorem, $a(G) \leq 32f^3(p^f - 1) < n^{c_2}/2$, if J acts on a vector space of dimension 4, and $a(G) \leq 96f^3(p^f - 1) < n^{c_2}/2$ if J acts on a vector space of dimension 6. Assume that J is a single quasisimple group. If $d = 2$, then Dickson's theorem gives $a(G) \leq 2f^2(p^f - 1) < n^{c_2}/2$. If $3 \leq d \leq 7$, then $a(G) \leq 4f^2d(p^f - 1)$ which is again smaller than $n^{c_2}/2$.

Assume that J is solvable. Then $c(G) \leq c(G/G_0)c(G_0/Z(G_0))c(Z(G_0))$ which is at most $f(p^f - 1)c(G_0/Z(G_0))$. The group $G_0/Z(G_0)$ is isomorphic to an affine linear group HW acting on a vector space of size $|W| = d^2$ with W a completely reducible H-module. By induction it is easy to see that $c(HW) \leq |W|^{c_2}/2$. Thus $c(G) \leq f(p^f - 1)(d^{2c_2}/2)$ which is at most $n^{c_2}/2$.

Assume now that $J = J_1 \circ J_2$ where J_1 is a normal subgroup of G that is a central product of quasisimple groups and J_2 is a solvable noncentral normal subgroup of G. Let $d_1 \geq 2$ and $d_2 \geq 2$ be the dimensions of the vector spaces (over the field of size p^f) on which J_1 and J_2 act naturally. So $d_1d_2 \mid d$. The group $G_0/Z(G_0)$ may be viewed in a natural way as a subgroup Y of a certain direct product $X_1 \times X_2$ such that Y projects onto both X_1 and X_2 where X_1 was treated two paragraphs up and X_2 one paragraph up as $G_0/Z(G_0)$, where it was shown that $f(p^f - 1)c(X_i) \leq p^{fd_ic_2}/2$ for $i = 1$ and 2. By Lemma 14.1 we have $c(G) \leq f(p^f - 1)c(X_1)c(X_2) < p^{fdc_2}/2$.

Assume that G acts irreducibly and imprimitively on V. Suppose G preserves a direct sum decomposition $V_1 \oplus \cdots \oplus V_t$ of the vector space V with $t > 1$ maximal. Let K be the kernel of the transitive permutation action of G on $\{V_1, \ldots, V_t\}$. Observe that the action of K on every V_i is completely reducible since such a projection of K can be viewed as a normal subgroup in the primitive action of $N_G(V_i)$. Thus by Theorem 14.2, Lemma 14.1 and induction, we have

$$c(G) \leq c(G/K)c(K) \leq 2^{t-1} \cdot |V_1|^{c_2t}/2^t = |V|^{c_2}/2.$$

Finally assume that G acts reducibly on V which may be considered as $U \oplus W$ where U and W are nontrivial G-submodules of V. If K denotes the kernel of the action of G on U, then G/K and K act faithfully and completely reducibly on U and W respectively. By induction $c(G) \leq c(G/K)c(K) \leq (|U|^{c_2}/2)(|W|^{c_2}/2) < n^{c_2}/2$. This finishes the proof of the theorem. □

We are now in the position to prove Theorem 1.6. By Theorem 14.3 we are finished in case G is an affine primitive permutation group. If G is not an affine primitive permutation group, then, as in the last two paragraphs of the previous section, $c(G)$ can be bounded using Theorem 14.2 and the two remarks that follow Lemma 7.7. In both of these cases we get $c(G) < n^{3/2}/2$.

15. Asymptotics

In this section the second half of Theorem 1.1 and Theorem 1.3 are proved.

Let G be a primitive permutation group of degree n and let A be the full normalizer of G in S_n. Assume that A is not an (affine) subgroup of $A\Gamma L_1(q)$ for a prime power q equal to n. We will show that for $n \geq 2^{14000}$ we have $|A/G| < n^{1/2} \log n$.

Assume first that A is an affine primitive permutation group. Then so is G. In fact we may change notation and assume that A and G are linear groups acting irreducibly on a finite vector space V of size n with $G \lhd A$. First assume that A acts primitively on V. Let us use the notation of Theorem 10.1. By assumption, we have $d \geq 2$. If $d = 2$ then, by the structure of A, we have that $|A/G|$ is at most $(3/2)(\sqrt{n} - 1)\log_3 n < n^{1/2} \log n$ if A is solvable and $|A/G| < n^{1/2} \log n$ if A is nonsolvable (using Dickson's theorem). If $d \geq 3$, then, by Theorem 10.1,

$$|A/G| < n^{1/3} \cdot (\log n) \cdot d^{2 \log d + 3} \leq n^{1/3} (\log n)^{2 \log \log n + 4} < n^{1/2}$$

for $n \geq 2^{8192}$.

Assume now that A acts imprimitively on V and that it preserves a direct sum decomposition $V_1 \oplus \cdots \oplus V_t$ of V where $t > 1$ is as large as possible. Let K denote the kernel of the (transitive) action of A on $\{V_1, \ldots, V_t\}$. As in the proof of Theorem 9.2, let A_1 be the action of $N_A(V_1)$ on V_1. The group A_1 acts primitively and irreducibly on V_1. By Theorem 9.1, we have $a(A_1) < m \log m$ for $m = |V_1| > 3^{16}$. In the notation of Lemma 7.2 for $t \geq 2^{729}$ we have $a(K/J) \leq (a(X_1))^{t/3c_1}$, by use of Lemma 7.5, where c_1 is as in Theorem 1.5. From this and by the proof of Theorem 9.2 together with part (2) of Lemma 10.3 and Theorem 1.7, for $t \geq 2^{729}$ we get

$$|A/G| \leq |A/GK| \cdot (a(A_1)b(A_1/G_1))^{t/3c_1} \leq 16^{t/\sqrt{\log t}} \cdot n^{1/3} < n^{1/2}.$$

Otherwise, if t is bounded (is at most 2^{729}) but $t \neq 2, 4$, then, again by the proof of Theorem 9.2 and by Lemma 7.2 and Theorems 1.7 and 4.2, we have, for $n \geq 2^{8192}$,

$$|A/G| \leq |A/GK| \cdot b(A_1/G_1) \cdot (a(A_1))^{3t/8} \leq 16^{t/\sqrt{\log t}} \cdot (\log m)^{2 \log \log m} \cdot n^{7/16} < n^{1/2}.$$

If $t = 2$ and $m \geq 2^{2048}$, then $|A/G| \leq b(A_1/G_1)a(A_1) < m \log m < n^{1/2} \log n$.

Let $t = 4$. Then $|A/G| \leq 6 \cdot b(A_1/G_1) \cdot (a(A_1))^2$. Using the notation d (for A_1) as in Theorem 10.1, by the argument above, we see that for $d \geq 2$ and $m \geq 2^{2048}$ we have $b(A_1/G_1) \cdot a(A_1) < 16 \cdot m^{1/2} \log m$. This gives $|A/G| < n^{1/2} \log n$ for $n \geq 2^{8192}$ under the assumption that $d \geq 2$. Thus assume that $d = 1$. Here we use the observation made in Lemma 7.3. Write $a(A_1) = |A_1|$ in the form $2^\ell r$ where r is odd and ℓ is an integer. Then we have $|A/G| \leq 6 \cdot 2^{2\ell} \cdot r$. From this the result follows if $|A_1| < 6m$. Otherwise, by Zsigmondy's theorem, $2^\ell < m$. Now $|A_1| < m \log_q m$ where q is the size of the field over which A_1 and A are defined. From this $2^{2\ell} \cdot r < m^2 \log_q m$ giving $|A/G| < n^{1/2} \log n$ unless $q = 2$. If $q = 2$, then $2^\ell \leq \log m$, and so $|A/G| < 6 \cdot m(\log m)^2 < n^{1/2} \log n$ for $m \geq 2^{2048}$.

Assume that A is a primitive permutation group which is not of affine type. In this case we use the notations, assumptions and the argument in the last two paragraphs of Section 9. However, we use Theorem 1.7. If A has two minimal normal subgroups, then we have

$$|A/G| = a(A/G)b(A/G) < n^{1/3} \cdot 4^{s/\sqrt{\log s}} \cdot (\log n)^{2 \log \log n} < n^{1/2}$$

for $n \geq 2^{8192}$, if $s \neq 1$, and also when $s = 1$. Finally assume that A has a unique minimal normal subgroup. We first claim that we may assume that $t \geq 512$. If

$|\mathrm{Out}(L)| \leq \sqrt{m}$ and $t \leq 512$, then $|A/G| \leq n^{1/4} \cdot 16^{t/\sqrt{\log t}} < n^{1/2}$. If $|\mathrm{Out}(L)|$ is larger than $\sqrt{m}$, then L is one of the exceptions in Lemma 7.7 and so $t \geq 512$ by use of $n \geq 2^{14000}$. If $t \geq 512$, then, for $n \geq 2^{14000}$, we have

$$|A/G| \leq |\mathrm{Out}(L)|^{1/3t} \cdot 4^{t/\sqrt{\log t}} \cdot t^{\log t} < n^{1/2} \log n.$$

This proves the second half of Theorem 1.1.

So far we showed Theorem 1.3 in case $|\mathrm{Out}(G)| = |A/G|$. In fact by the same calculation as in the previous paragraph we established Theorem 1.3 in case G is not of affine type. Thus assume that G is of affine type and $H^1(H, V) \neq 0$ where V is the minimal normal subgroup of G and $H \neq 1$ is a point stabilizer in G. Let us use the notation and assumptions of the proof of Theorem 12.3.

Let us first assume that $t > 1$ and $|\mathrm{Out}(G)| \leq (q-1)q^{[d/2]}|\mathrm{Out}(L)|^{t/2}b_t$ with $d \geq 2$ where $b_t \leq 4^{t/\sqrt{\log t}} \cdot t^{\log t}$, by Theorem 1.7 and $|\mathrm{Out}(L)| \leq 4(\log n)/t$, by Lemma 7.8. Here $n = q^{dt}$. Thus $|\mathrm{Out}(G)| < q^{[d/2]+1} \cdot (4(\log n)/t)^{t/2} \cdot 4^{t/\sqrt{\log t}} \cdot t^{\log t}$. If $d \geq 3$ or $t \geq 3$, then this is less than $n^{1/2} \log n$ for $n \geq 2^{14000}$. Finally, if $d = 2$ and $t = 2$, then $|\mathrm{Out}(G)| < n^{1/2} \log n$ since $|\mathrm{Out}(L)| \leq \log n$ by use of Dickson's theorem on subgroups L of $\mathrm{GL}_2(q)$.

Finally assume that in the proof of Theorem 12.3 we have $t = 1$, that is, H is an almost simple group with socle L. Then $|\mathrm{Out}(G)| \leq (q-1)|H^1(L, W)||\mathrm{Out}(L)|$ where W is a nontrivial irreducible L-module of size dividing n and defined over a field of size q. By Lemma 7.8, $|\mathrm{Out}(L)| \leq 4 \log n$.

By the main result of [GH], we have $|\mathrm{Out}(G)| \leq 4(q-1)|W|^{1/2} \log n$. Assume first that $|W| < n$. If $\dim W \geq 3$, then $|\mathrm{Out}(G)| \leq 4 \cdot n^{5/12} \log n$, which is less than $n^{1/2} \log n$ for $n \geq 2^{14000}$. If $\dim W = 2$, then $|\mathrm{Out}(G)| < n^{1/2}|\mathrm{Out}(L)|$ which is less than $n^{1/2} \log n$ by using Dickson's theorem once again. Thus assume that $|W| = n = q^d$. Furthermore, as observed in the proof of Theorem 12.3, we may assume that $d \geq 3$ (otherwise G is a member of the infinite sequence of examples in Theorem 1.2). Then, by [GH], it is easy to see that $|\mathrm{Out}(G)| < 2 \cdot n^{3/4}$, at least for $n \geq 2^{14000}$. (In this previous bound the factor 2 comes from the fact that the full normalizer in $\mathrm{GL}_4(q)$ of A_6 acting on the fully deleted permutation module of dimension 4 in characteristic 3 over the field of size q has size $(q-1)|\mathrm{S}_6|$ since the dimension of the fixed point space of a 3-cycle in A_6 is different from the dimension of the fixed point space of an element in A_6 which is the product of two 3-cycles.) This proves the first statement of Theorem 1.3.

If L is an alternating group of degree at least 7, a sporadic simple group or the Tits group, then $\dim(H^1(L, W)) \leq (1/4) \dim(W)$ by [GK, Corollary 3] and [GH]. Thus in these cases we have $|\mathrm{Out}(G)| < 2 \cdot n^{1/2} \leq n^{1/2} \log n$. If L is a simple group of exceptional type, then $\dim(H^1(L, W)) \leq (1/3) \dim(W)$ by [H], thus if $d \geq 7$ then $|\mathrm{Out}(G)| < 4 \cdot n^{3/7} \log n < n^{1/2} \log n$ for $n \geq 2^{14000}$. Otherwise $d = 6$ and $L = \mathrm{G}_2(r)$ with r even or $4 \leq d \leq 6$ and L is a Suzuki group (by [KL, Table 5.3.A] and [KL, Table 5.4.C]). However in these cases $\dim(H^1(L, W)) \leq 1$, by [H], and so $|\mathrm{Out}(G)| < n^{1/2} \log n$. We may now assume that L is a classical simple group.

Since we are assuming that the dimension of the natural module for L is at least 7, we see from [KL, Table 5.4.C] and [KL, Table 5.3.A] that $d \geq 7$. By [H] we also

have $\dim(H^1(L,W)) \leq (1/3)\dim(W)$. Thus $|\mathrm{Out}(G)| < 4 \cdot n^{3/7} \log n < n^{1/2} \log n$ for $n \geq 2^{14000}$.

This completes the proof of Theorem 1.3.

References

[A]   M. Aschbacher, Finite group theory. Second edition. Cambridge Studies in Advanced Mathematics, 10. Cambridge University Press, Cambridge, 2000.

[AG1] M. Aschbacher and R. M. Guralnick, Some applications of the first cohomology group. *J. Algebra* **90** (1984), 446–460.

[AG2] M. Aschbacher and R. M. Guralnick, Abelian quotients of primitive groups. *Proc. Amer. Math. Soc.* **107** (1989), 89–95.

[D]   J. D. Dixon, The Fitting subgroup of a linear solvable group. *J. Austral. Math. Soc.* **7** (1967), 417–424.

[DM]   J. D. Dixon and B. Mortimer, Permutation groups, Graduate Texts in Math. 163, Springer-Verlag, New York, 1996.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.5*, 2014, (http://www.gap-system.org).

[G1]   R. M. Guralnick, Generation of simple groups. *J. Algebra* **103** (1986), 381–401.

[G2]   R. M. Guralnick, Cyclic quotients of transitive groups. *J. Algebra* **234** (2000), 507–532.

[GH]   R. M. Guralnick and C. Hoffman, The first cohomology group and generation of simple groups, in Proc. Conf. Groups and Geometries (Siena, 1996), Trends in Mathematics, Birkhäuser, Basel 1998, pp. 81–89.

[GK]   R. M. Guralnick and W. Kimmerle, On the cohomology of alternating and symmetric groups and decomposition of relation modules. *J. Pure Appl. Algebra* **69** (1990), no. 2, 135–140.

[HM]   Z. Halasi and A. Maróti, The minimal base size for a *p*-solvable linear group, to appear in *Proc. Amer. Math. Soc.*

[H]   C. Hoffman, On the cohomology of the finite Chevalley groups. *J. Algebra* **226** (2000), no. 2, 649–689.

[GS]   R. M. Guralnick and K. Stevenson, Prescribing ramification. Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 387–406, *Proc. Sympos. Pure Math.*, **70**, Amer. Math. Soc., Providence, RI, 2002.

[JLPW] C. Jansen, K. Lux, R. Parker and R. Wilson, An Atlas of Brauer characters, Oxford Univ. Press, Oxford 1995.

[KL]   P. B. Kleidman and M. W. Liebeck, The subgroup structure of the finite classical groups, LMS Lecture Note Ser. 129, Cambridge Univ. Press, Cambridge 1990.

[KW]   P. B. Kleidman and D. B. Wales, The projective characters of the symmetric groups that remain irreducible on subgroups. *J. Algebra* **138** (1991), 440–478.

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

[LP]   M. W. Liebeck and L. Pyber, Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra* **198** (1997), 538–562.

[LMM1] A. Lucchini, F. Menegazzo and M. Morigi, Asymptotic results for transitive permutation groups. *Bull. Lond. Math. Soc.* **32** (2000), 191–195.

[LMM2] A. Lucchini, F. Menegazzo and M. Morigi, On the number of generators and composition length of finite linear groups. *J. Algebra* **243** (2001), 427–447.

[M]   A. Maróti, On the orders of primitive groups. *J. Algebra* **258** (2002), 631–640.

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

[PS]   C. E. Praeger and J. Saxl, On the order of primitive permutation groups. *Bull. Lond. Math. Soc.* **12** (1980), 303–308.

[Py]   L. Pyber, Asymptotic results for permutation groups, Groups and computation, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 11 (ed. L. Finkelstein and W. M. Kantor) Amer. Math. Soc. Providence RI 1993, pp. 197–219.

[R]   J. S. Rose, Automorphism groups of groups with trivial centre. *Proc. Lond. Math. Soc.* (3) **31** (1975), 167–193.

[Sc] P. Schmid, The solution of the $k(GV)$ problem. ICP Advanced Texts in Mathematics, 4. Imperial College Press, London, 2007.

[Su] M. Suzuki, Group Theory II, Springer-Verlag, New York, 1986.

[T]   G. M. Tracey, Minimal generation of transitive permutation groups. ArXiv: 1504.07506.

[W]   T. R. Wolf, Solvable and nilpotent subgroups of $GL(n, q^m)$. *Canad. J. Math.* **34** (1982), 1097–1111.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-1113, USA

E-mail address: guralnic@math.usc.edu

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, REÁLTANODA UTCA 13-15, H-1053, BUDAPEST, HUNGARY

E-mail address: maroti.attila@renyi.mta.hu

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, REÁLTANODA UTCA 13-15, H-1053, BUDAPEST, HUNGARY

E-mail address: pyber.laszlo@renyi.mta.hu