TRANSITIVE PERMUTATION GROUPS AND IRREDUCIBLE LINEAR GROUPS

By R. M. BRYANT, L. G. KOVÁCS *and* G. R. ROBINSON[1]

[Received 13 December 1993]

IT was proved by M. F. Newman and the second author that there is a constant c such that each nilpotent transitive permutation group of degree $d \geq 2$ can be generated by $[cd/\sqrt{\log d}]$ elements. Later J. D. Dixon and the second author showed that, for each field $\mathbb{F}$ which has finite degree over its prime subfield, there is a constant $c_{\mathbb{F}}$ such that each finite nilpotent irreducible linear group of degree d over $\mathbb{F}$ can be generated by $[c_{\mathbb{F}}d/\sqrt{\log d}]$ elements. For a finite group G, let $\mathsf{R}(G)$ denote the product of the soluble radical and the generalized Fitting subgroup. Here we extend both results from nilpotent groups to the much wider class of all finite G such that $\mathsf{R}(G) = G$.

The proof easily reduces to dealing with groups that are either soluble or quasinilpotent. The soluble case involves a result of independent interest: there is a constant b such that, given a module of dimension a (over an arbitrary field) for a subgroup of index d in a finite soluble group, each submodule of the induced module can be generated by $[abd/\sqrt{\log d}]$ elements.

One of the steps towards the quasinilpotent case is the following theorem,' which we prove using the classification of finite simple groups. If G is any finite group and n is the composition length of the quotient of the generalized Fitting subgroup of G modulo the Frattini subgroup of $\mathsf{R}(G)$, then G can be generated by $5n$ elements.

1. Introduction

As was proved in [9], there is a number c such that each nilpotent transitive permutation group of degree $d \geq 2$ can be generated by $[cd/\sqrt{\log d}]$ elements. A special case of the first result of the present paper strengthens this by showing that the composition length of the Frattini factor group $G/\Phi(G)$ of such a group G is bounded by $[cd/\sqrt{\log d}]$.

THEOREM 1.1. *If G is a quasinilpotent transitive permutation group of degree $d \geq 2$, then $G/\Phi(\mathsf{F}(G))$ cannot have composition length greater than $cd/\sqrt{\log d}$.*

We use the term *quasinilpotent* in the same sense as Huppert and

[1] The research of the third author was supported by an NSF grant.

Blackburn [7]. As usual, $\mathsf{F}(G)$ denotes the Fitting subgroup of G. Note that $\Phi(\mathsf{F}(G))$, like the Frattini subgroup of any normal subgroup of G, lies in $\Phi(G)$. The number c in Theorem 1.1 is the same as in the theorem of [9].

According to Corollary 1.8 of [5], for each field $\mathbb{F}$ whose degree over its prime subfield is finite, there is a number $c_{\mathbb{F}}$ such that each finite nilpotent irreducible linear group of degree $d \geq 2$ over $\mathbb{F}$ can be generated by $[c_{\mathbb{F}} d/\sqrt{\log d}]$ elements. Our second result yields an improvement of this.

THEOREM 1.2. *To each field $\mathbb{F}$ whose degree over its prime subfield is finite, there is a number $c_{\mathbb{F}}^{\sharp}$ such that if G is a finite quasinilpotent irreducible linear group of degree $d \geq 2$ over $\mathbb{F}$ then $G/\Phi(\mathsf{F}(G))$ cannot have composition length greater than $c_{\mathbb{F}}^{\sharp} d/\sqrt{\log d}$.*

Given that all finite nonabelian simple groups are 2-generator groups (see the survey [4] by Di Martino and Tamburini), it is not hard to see (cf. Wiegold [15]) that a direct product of m simple groups (whether abelian or not) can always be generated by $\max\{m, 2\}$ elements. Since the Frattini quotients of quasinilpotent groups are direct products of this kind, it follows that Theorems 1.1 and 1.2 imply similar bounds for the number of elements required to generate the quasinilpotent group in question.

Indeed, these theorems imply bounds for the number of elements required to generate any finite group G whose generalized Fitting subgroup $\mathsf{F}^*(G)$ admits a faithful transitive or irreducible representation of the relevant kind. Noting that $\Phi(\mathsf{F}(G)) \leq \Phi(\mathsf{R}(G))$, this can be seen from the next theorem, which is the only one here to depend on the classification of finite simple groups.

THEOREM 1.3. *If G is a finite group and $\mathsf{F}^*(G)/\Phi(\mathsf{R}(G))$ has composition length n, then G can be generated by $5n$ elements.*

For terminology, notation and basic facts concerning generalized Fitting subgroups, our reference is § X.13 of [7]; see also the comments at the end of this introduction.

For soluble G, this theorem answers a question of Reinhard Laue [11]. Since there exist (insoluble) groups G with $G > \mathsf{F}^*(G) = \Phi(G)$, one cannot replace $\Phi(\mathsf{R}(G))$ by $\Phi(G)$ in this theorem.

The expression $d/\sqrt{\log d}$ enters our theorems by way of the following result.

THEOREM 1.4. *There is a number b such that if a partially ordered set P of cardinality $d \geq 2$ is a cartesian product of chains then no antichain of P can have cardinality greater than $bd/\sqrt{\log d}$.*

Similar bounds played key roles in [9] and [5]. We are grateful to

Professors Z. Füredi and L. Pyber for pointing out that this result has been known for some time, for example as a consequence of Theorem 4.3.6 in Anderson [2], and accordingly we omit our proof of it. The key application of Theorem 1.4 is the following.

THEOREM 1.5. *Whenever H is a finite soluble group and U is a module of finite dimension a (over an arbitrary field) for a subgroup of index $d \geq 2$, each submodule of the induced module $U\uparrow^H$ can be generated by $[abd/\sqrt{\log d}]$ elements.*

In fact, we use a partial generalization.

COROLLARY 1.6. *Let A be a finite soluble group of composition length a, and H a subgroup in the wreath product $A \operatorname{wr} S_d$ (where $d \geq 2$) with soluble and transitive top projection. Each H-subgroup of the base group B of this wreath product can be generated, as H-group, by $[abd/\sqrt{\log d}]$ elements.*

Here the top projection of H means the image of H in S_d under the obvious homomorphism $A \operatorname{wr} S_d \to S_d$ with kernel B, and the requirement is that this image be soluble and transitive as subgroup of that symmetric group. A subgroup of B normalized by H is termed an H-subgroup; a subset generates it as H-group if it is the smallest H-subgroup to contain that subset. This corollary supersedes the central argument of [9] and provides the step from the easy case of soluble primitive permutation groups to the full generality of the next theorem.

THEOREM 1.7. *There is a number c' such that each soluble transitive permutation group of degree $d \geq 2$ can be generated by $[c'd/\sqrt{\log d}]$ elements.*

Corollary 1.6 is also important in the proof of the final result of this paper, which draws heavily on [5] and on Suprunenko [13] as well.

THEOREM 1.8. *To each field $\mathbb{F}$ whose degree over its prime subfield is finite, there is a number $c'_{\mathbb{F}}$ such that each finite soluble irreducible linear group of degree $d \geq 2$ over $\mathbb{F}$ can be generated by $[c'_{\mathbb{F}}d/\sqrt{\log d}]$ elements.*

These results together imply the following.

COROLLARY 1.9. *Let G be a finite group such that $\mathsf{R}(G) = G$. If G admits a faithful transitive permutation representation of degree $d \geq 2$, then G can be generated by $[\max\{c, c'\}d/\sqrt{\log d}]$ elements. If $\mathbb{F}$ is a field whose degree over its prime subfield is finite, and if G admits a faithful*

irreducible $\mathbb{F}$*-representation of degree* $d \geq 2$, *then* G *can be generated by* $[\max\{c_{\mathbb{F}}^*, c_{\mathbb{F}}'\}d/\sqrt{\log d}]$ *elements.*

All our logarithms are to base 2. Throughout, the symbols c and $c_{\mathbb{F}}$ stand for numbers with the properties cited above from [9] and [5], and d stands for a positive integer. When we say that a group can be generated by s elements, we mean that it can be generated by a subset of cardinality no larger than the integer part $[s]$.

Examples constructed in [9] and [5] show that the bounds discussed (except that in Theorem 1.3) are of the right order even for nilpotent groups, but we have no reason to expect that our methods would be useful in finding optimal constants.

The paper is organized 'linearly', each section giving the proof of one or more of the results stated in this introduction in the order they have appeared here. Some additional comments are left to the last section.

As mentioned above, § X.13 of [7] is our basic reference for quasinilpotent groups, generalized Fitting subgroups, and related matters. In addition, we call a group *quasisimple* if it is perfect and its central factor group is simple. It follows from the results in that section of [7] that any two different quasisimple subnormal subgroups of a finite group G commute elementwise, and that the subgroup $\mathsf{E}(G)$, defined there as the terminal member of the lower central series of the generalized Fitting subgroup $\mathsf{F}^*(G)$, can also be recognized as the product of the quasisimple subnormal subgroups of G. (In [7], the quasisimple subnormal subgroups of G are called the components of $\mathsf{E}(G)$.) The soluble radical of G, which we denote by $\mathsf{S}(G)$, commutes elementwise with $\mathsf{E}(G)$. Further, $\Phi(\mathsf{E}(G)) = \mathsf{S}(\mathsf{E}(G)) = \mathsf{Z}(\mathsf{E}(G))$ and, as $\mathsf{F}^*(G) = \mathsf{E}(G)\mathsf{F}(G)$, we have $\mathsf{R}(G) = \mathsf{E}(G)\mathsf{S}(G)$. These facts will be taken for granted throughout the paper.

We are greatly indebted to Professor Pyber for several discussions and useful suggestions (one of which appears here as Lemma 7.3), for the references [2], [8], [11], and for a preprint of [12].

2. Quasinilpotent transitive groups

In this section we present the proof of Theorem 1.1. It is straightforward to see that the function $x/\sqrt{\log x}$ is monotone increasing when $x > \sqrt{e}$: we shall use this repeatedly, often without reference. The first step is the promised strengthening of the theorem of [9]. This will be based on two simple lemmas.

LEMMA 2.1. *If* $m, n \in \mathbf{Z}$ *and* $m > 1$, $n > 1$, $mn > 8$, *then*

$$\frac{m}{\sqrt{\log m}} + \frac{n}{\sqrt{\log n}} < \frac{mn}{\sqrt{\log mn}}.$$

Proof. Without loss of generality, we may take $m \leq n$. Suppose the claim fails: in view of the monotonicity of $x/\sqrt{\log x}$, then

$$\frac{2n}{\sqrt{\log n}} \geq \frac{mn}{\sqrt{\log mn}} \geq \frac{mn}{\sqrt{(2 \log n)}},$$

so $m \leq 2\sqrt{2}$, $m = 2$, and hence

$$\frac{2}{\sqrt{\log 2}} + \frac{n}{\sqrt{\log n}} \geq \frac{2n}{\sqrt{\log 2n}}.$$

Since $m = 2$ and $mn > 8$, we have $n \geq 5$, and then $\log 2n \leq (3/2) \log n$. Thus

$$2 \geq \left(\frac{2}{\sqrt{(3/2)}} - 1\right) \frac{n}{\sqrt{\log n}}$$

follows. This inequality fails to hold at $n = 5$, so monotonicity implies that it fails whenever $n \geq 5$; we have the contradiction which completes the proof.

For a prime p and a positive integer d, let d_p denote the highest p-power divisor of d. Recall that c denotes a number satisfying the conclusion of the theorem of [9].

LEMMA 2.2. *If F is a nilpotent transitive permutation group of degree d, then $O_p(F)$ has a faithful transitive permutation representation of degree d_p.*

Proof. Since F is nilpotent, $F = O_p(F) \times O_{p'}(F)$, and if K is a point stabilizer in F then $K = (K \cap O_p(F)) \times (K \cap O_{p'}(F))$. It follows that $|O_p(F) : (K \cap O_p(F))| = d_p$ and that $K \cap O_p(F)$ contains no nontrivial normal subgroup of $O_p(F)$.

COROLLARY 2.3. *The Frattini quotient of a nilpotent transitive permutation group of degree $d \geq 2$ has composition length at most $cd/\sqrt{\log d}$.*

Proof. If F is any finite nilpotent group, then $F/\Phi(F) = \prod_p O_p(F)/\Phi(O_p(F))$. Suppose also that F is a transitive permutation group of degree d. Then the product need only be taken over the p such that $d_p > 1$, and for those the theorem of [9] may be applied with the conclusion that the composition length of $O_p(F)/\Phi(O_p(F))$ is at most $cd_p/\sqrt{\log d_p}$: so all we have to add is that $\sum_p d_p/\sqrt{\log d_p} \leq d/\sqrt{\log d}$ follows by repeated application of Lemma 2.1. Not quite, for that lemma is only applicable when $mn > 8$. Here we apply Lemma 2.1 only with coprime m, n, and then this condition is satisfied unless $mn = 6$. The nilpotent transitive groups of degree 6 are all cyclic of order 6, so $2 \leq 6c/\sqrt{\log 6}$ is needed to cover the exception. As the defining property

of c applied to the noncyclic transitive group of degree 4 and order 4 gives that $2 \leq 4c/\sqrt{\log 4}$, the required inequality is certainly available.

Note from the last sentence of this proof that $c \geq 1/\sqrt{2}$.

The remaining task is the quasinilpotent generalization. We shall need a simple observation which may not be well known.

LEMMA 2.4. *If F is a nilpotent normal subgroup and H is a subgroup in a finite quasinilpotent group G, then each perfect subgroup of FH is contained in H.*

Proof. Let $1 = Z_0(FH) \leq Z_1(FH) \leq \cdots$ be the upper central series of FH: it is immediate that $[Z_i(FH)H, Z_i(FH)H] \leq Z_{i-1}(FH)H$ whenever $i \geq 1$. In a finite quasinilpotent group each nilpotent normal subgroup is hypercentral, so F is hypercentral in G and therefore also in FH (although FH need not be quasinilpotent). Thus the chain of subgroups $Z_i(FH)H$ goes from H all the way to FH, each member of the chain containing the derived group of the next. It follows that every perfect subgroup of FH must lie in H.

LEMMA 2.5. *If a transitive permutation group is the direct product of k nonabelian simple groups, then the degree of the group is at least 5^k.*

Proof. We argue by induction on k. The case $k = 1$ being obvious, suppose $k > 1$. Call the group G and write it as $G = R \times S$ with S simple.

A nontrivial permutation which centralizes a transitive group cannot fix any point (for the set of its fixed points is setwise invariant under that transitive group). Hence if a permutation group centralizes a transitive group then all its orbits must be regular. In particular, if S is transitive then all orbits of R are regular. Since $|R| \geq 60^{k-1} > 5^k$, in this case there is nothing left to prove.

Suppose next that S is not transitive. Its orbits form a system of imprimitivity for G, so G permutes the set of these orbits transitively. Denote by T the kernel of this action, and note that T is the direct product of some of the simple direct factors of G (including S). Let m denote the number of simple direct factors of T: of course then $m < k$, and G/T is a direct product of $k - m$ simple groups. By the inductive hypothesis, the number of orbits of S is at least 5^{k-m}. The kernels of the action of T on the various orbits of S are conjugate subnormal subgroups of G: given the structure of G, this means that they must all be the same, and then they must all be trivial. Thus T acts faithfully (and obviously transitively) on any one orbit of S; therefore, by the inductive hypothesis, each orbit of S has length at least 5^m. It follows that the degree of G is at least 5^k, as required.

Proof of Theorem 1.1. In addition to these lemmas, we shall use the

simple fact that if $m > 1$ then $\log m \leq m/\sqrt{\log m}$ (recall that our logarithms are to base 2).

Consider a quasinilpotent group G with a corefree subgroup H of index d, and set $E = \mathsf{E}(G)$, $F = \mathsf{F}(G)$, and $Z = \mathsf{Z}(E) = E \cap F$, noting that $EF = G$. The first point to establish is that $(E \cap FH)/Z$ is corefree in E/Z. Since the minimal normal subgroups of E/Z are the KZ/Z with K a quasisimple normal subgroup, the alternative is that some such K lies in FH: but then by Lemma 2.4 we would have $K \leq H$, contrary to the assumption that H is corefree.

As $G/\Phi(F)$ is an extension of $F/\Phi(F)$ by a group isomorphic to E/Z, what we want to bound is the sum of the composition lengths of these two groups. Set $m = |E:(E \cap FH)|$ and $n = |FH:H|$, and denote by k the number of simple direct factors of E/Z (that is, the composition length of E/Z). Then $d = mn$. From Lemma 2.5, we know that $\log m \geq k \log 5$; of course, $1/\log 5 < 1/\sqrt{2}$, and we noted $1/\sqrt{2} \leq c$ after the proof of Corollary 2.3; so the inequality mentioned at the beginning of this proof yields that if $m > 1$ then $k < cm/\sqrt{\log m}$. On the other hand, $n = |F:(F \cap H)|$; since every normal subgroup of F is normal in G, $F \cap H$ must be corefree in F; hence if $n > 1$ then by Corollary 2.3 the composition length of $F/\Phi(F)$ is at most $cn/\sqrt{\log n}$. If $m = 1$ or $n = 1$ there is nothing left to do; otherwise $m \geq 5$ and $n \geq 2$ so $mn > 8$, and Lemma 2.1 completes the argument.

3. Quasinilpotent linear groups

This section will be taken up by the proof of Theorem 1.2. The plan is to imitate the proof of Theorem 1.1 as closely as is possible (and convenient). The easiest step is the analogue of Lemma 2.5.

LEMMA 3.1. *If a finite group is the product of k quasisimple normal subgroups, then each faithful irreducible linear representation of the group must have degree at least 2^k.*

Proof. If no irreducible representation of the group is faithful, this claim is vacuously true. Otherwise we may take d to be the minimum of the degrees of the faithful irreducible representations of the group over all possible fields, and consider such a representation of degree d. On passing to the algebraic closure of the field, the representation becomes a direct sum of irreducibles which are pairwise Galois-conjugate (see Theorem VII.1.18 and Lemma VII.2.5 in [7]), so each of them must be faithful: the minimality of d therefore guarantees that in fact the representation remains irreducible. Different quasisimple normal subgroups commute elementwise, so over this algebraically closed field the representation is a tensor product of irreducibles of those quasisimple normal

subgroups (Theorem VII.9.14 in [7]); since the representation is faithful for the group, each tensor factor must be faithful for the relevant quasisimple normal subgroup. Thus each tensor factor has degree at least 2, and $d \geq 2^k$.

This is almost a special case of the next lemma, but not quite, because some quasisimple groups have no noncyclic abelian subgroups.

LEMMA 3.2. *Let ρ be a faithful irreducible representation of a group K over an arbitrary field, and suppose that $K = K_1 \cdots K_n$ with subgroups K_i which commute with each other elementwise. Then each restriction $\rho\downarrow_{K_i}$ is a direct sum of copies of a faithful irreducible representation, ρ_i say, of K_i. Moreover, if each of the K_i has at least one noncyclic abelian subgroup, then the multiplicity of ρ_i in $\rho\downarrow_{K_i}$ is at least 2^{n-1}.*

Proof. Suppose that ρ_i is an irreducible constituent of $\rho\downarrow_{K_i}$. Since $K = K_i C_K(K_i)$, Clifford's Theorem tells us that $\rho\downarrow_{K_i}$ is a direct sum of copies of ρ_i, and then it also follows that ρ_i must be faithful.

Because of the symmetry of the assumptions, the second claim will follow once we prove that the multiplicity of ρ_1 in $\rho\downarrow_{K_1}$ is at least 2^{n-1}. For $i = 1, \ldots, n$, let σ_i be an irreducible constituent of $\rho\downarrow_{K_1 \cdots K_i}$; in particular, let $\sigma_1 = \rho_1$, and note that $\sigma_n = \rho$. As in the previous argument, we see that $\rho\downarrow_{K_1 \cdots K_i}$ is a direct sum of copies of σ_i, so if $i < n$ then $\sigma_{i+1}\downarrow_{K_1 \cdots K_i}$ is also a direct sum of copies of σ_i. We claim that $\sigma_{i+1}\downarrow_{K_1 \cdots K_i}$ cannot be irreducible. If it were, then by Schur's Lemma the centralizer of $(K_1 \cdots K_i)\sigma_{i+1}$ in the ambient general linear group (that is, in the codomain of σ_{i+1}) would be the multiplicative group of a skewfield, and so it could have no noncyclic finite abelian subgroup: however, this centralizer contains the isomorphic copy $K_{i+1}\sigma_{i+1}$ of K_{i+1} and therefore does have at least one such subgroup. Differently put, the conclusion is that the multiplicity of σ_i in the restriction of σ_{i+1} is at least 2. It follows by induction on i that the multiplicity of ρ_1 in $\sigma_i\downarrow_{K_1}$ is at least 2^{i-1}.

COROLLARY 3.3. *If $\mathbb{F}$ is any field and X is a subgroup in a group Y such that $XC_Y(X) = Y$ and Y has a faithful irreducible representation of degree at most d over $\mathbb{F}$, then X also has such a representation.*

The case of cyclic groups was trivial in the transitive case but is a problem in the present context: we must prepare for dealing with that. *In the rest of this section, $\mathbb{F}$ will denote a field whose degree over its prime subfield is finite*: that is, $\mathbb{F}$ is either a finite field or a finite degree extension of $\mathbb{Q}$.

LEMMA 3.4. *There is a number $q_{\mathbb{F}}$ such that if a finite cyclic group C has a faithful irreducible representation of degree at most d over $\mathbb{F}$ then $|C| < q_{\mathbb{F}}^d$.*

Proof. The $\mathbb{F}$-linear span of the image of such a representation is an extension field, $\mathbb{E}$ say, of $\mathbb{F}$, with degree at most d, and the multiplicative group of $\mathbb{E}$ contains an isomorphic copy of C. It follows that, when $\mathbb{F}$ is finite, $q_{\mathbb{F}} = |\mathbb{F}|$ will obviously do (and this is best possible). We shall prove that if $|\mathbb{F}:\mathbb{Q}| = m < \infty$ then $q_{\mathbb{F}} = 3m^2$ defines a number with the required properties. As $|\mathbb{E}:\mathbb{Q}| \leq md$, the irreducibility of cyclotomic polynomials over $\mathbb{Q}$ implies that $\varphi(|C|) \leq md$ where φ denotes Euler's function. Using the multiplicative property of φ, one readily sees that if $|C| > 2$ then $|C| \leq (\varphi(|C|))^2 \leq (md)^2 \leq (3m^2)^d$.

It follows from Stirling's formula that there is a positive number s such that $s(n/e)^n < n!$ for every positive integer n.

LEMMA 3.5. *If a finite cyclic group C has a faithful irreducible representation of degree at most $d \geq 2$ over $\mathbb{F}$, then the composition length of the Frattini quotient of C is at most* $(d \log eq_{\mathbb{F}} + |\log s|)/\log d$.

Proof. Write n for the number of different prime divisors of $|C|$. Since the product of n different positive integers is at least $n!$, from Lemma 3.4 we get that $n! \leq |C| < q_{\mathbb{F}}^d$, and so $s(n/e)^n < q_{\mathbb{F}}^d$. With $n = xd$, this yields that $sd^n(x/e)^{xd} < q_{\mathbb{F}}^d$, that is, $d^n < (e/x)^{xd} q_{\mathbb{F}}^d / s$. It is easy to see that $(e/x)^x \leq e$ whenever $x > 0$, so we can conclude that $d^n < (eq_{\mathbb{F}})^d / s$, and therefore $n < (d \log eq_{\mathbb{F}} + |\log s|)/\log d$ as required.

This completes the preparations.

Proof of Theorem 1.2. Let G be a finite irreducible quasinilpotent linear group of degree d over $\mathbb{F}$; set $E = \mathbf{E}(G)$; write H for the product of the $\mathbf{O}_p(G)$ that are cyclic or (possibly generalized) quaternion groups, and K for the product of the other $\mathbf{O}_p(G)$. The composition length of $G/\Phi(\mathbf{F}(G))$ is the sum of the composition lengths of the Frattini quotients of E, H, and K. By Corollary 3.3, each of these groups has a faithful irreducible representation of degree at most d over $\mathbb{F}$. Lemma 3.1 shows that the Frattini quotient of E has composition length at most $\log d$, which obviously cannot exceed $d/\sqrt{\log d}$, while Lemma 3.5 yields that the composition length of the Frattini quotient of H is at most $2 + (d \log eq_{\mathbb{F}} + |\log s|)/\log d$, which cannot exceed $(2 + \log eq_{\mathbb{F}} + |\log s|)d/\sqrt{\log d}$. The proof will be complete, with $c_{\mathbb{F}}^* = 3 + \log eq_{\mathbb{F}} + |\log s| + 2c_{\mathbb{F}}$, if we can show that the composition length of the Frattini quotient of K is at most $2c_{\mathbb{F}} d/\sqrt{\log d}$ (where $c_{\mathbb{F}}$ is as in the Corollary 1.8 of [5] which we quoted in the introduction).

To this end, recall that $x/\sqrt{\log x}$ is monotonic when $x \geq 2$, and note that if $x \geq 4$ then $x/2 \geq \sqrt{x}$ and therefore

$$\frac{x/2}{\sqrt{\log (x/2)}} \leq \frac{x/2}{\sqrt{(\log \sqrt{x})}} = \frac{1}{\sqrt{2}} \frac{x}{\sqrt{\log x}}.$$

Repeated application of this fact yields that

$$\frac{d/2^{r-1}}{\sqrt{\log(d/2^{r-1})}} \leq \left(\frac{1}{\sqrt{2}}\right)^{r-1} \frac{d}{\sqrt{\log d}}$$

as long as $d/2^{r-1} \geq 2$.

Let $K_1, \ldots, K_r$ be the different $O_p(G)$ whose product is K. We know (see Satz III.8.4 in [6]) that each K_i has at least one noncyclic abelian subgroup. In view of Corollary 3.3 (applied with $X = K$, $Y = G$) and the defining property of $c_{\mathfrak{F}}$, we have nothing left to prove if $r \leq 1$, so suppose $r \geq 2$. Then Lemma 3.2 gives that each K_i has a faithful irreducible $\mathfrak{F}$-representation of degree at most $d/2^{r-1}$, so by the previous paragraph and the defining property of $c_{\mathfrak{F}}$ we can conclude that each K_i can be generated by $c_{\mathfrak{F}}\left(\frac{1}{\sqrt{2}}\right)^{r-1} d/\sqrt{\log d}$ elements. Differently put: each $K_i/\Phi(K_i)$ has composition length at most $c_{\mathfrak{F}}\left(\frac{1}{\sqrt{2}}\right)^{r-1} d/\sqrt{\log d}$. It follows that $K/\Phi(K)$ has composition length at most $rc_{\mathfrak{F}}\left(\frac{1}{\sqrt{2}}\right)^{r-1} d/\sqrt{\log d}$. Since $r\left(\frac{1}{\sqrt{2}}\right)^{r-1} \leq 2$ whenever $r \geq 1$, we have proved what we wanted.

4. Groups with small generalized Fitting subgroup

The aim here is the proof of Theorem 1.3. This will be based on the following lemma, which does not depend on the classification of simple groups.

LEMMA 4.1. *In any finite group G,*

$$\mathsf{F}^*(G/\Phi(\mathsf{R}(G))) = \mathsf{F}^*(G)/\Phi(\mathsf{R}(G)).$$

It is an easy corollary that $\mathsf{F}^*(G/N) = \mathsf{F}^*(G)/N$ whenever N is a normal subgroup of G contained in $\Phi(\mathsf{R}(G))$, but we shall not need that here. Any group G such that $G > \mathsf{F}^*(G) = \Phi(G)$ (for example, $G = PSL_2(\mathbb{Z}/5^2\mathbb{Z})$: see Lemma 4.2.2 in Wall [14]) shows that in this lemma, as in Theorem 1.3, one cannot replace $\Phi(\mathsf{R}(G))$ by $\Phi(G)$.

The proof of the lemma needs several preparatory steps. For the rest of this section, we shall write simply $E = \mathsf{E}(G)$, $F = \mathsf{F}(G)$, $F^* = \mathsf{F}^*(G)$, $S = \mathsf{S}(G)$, and $R = \mathsf{R}(G)$.

LEMMA 4.2. *We always have $\Phi(E) = E \cap S$ and $\Phi(R) = \Phi(E)\Phi(S)$.*

Proof. The first statement was already in the comments at the end of the introduction. It is clear that $\Phi(E)\Phi(S) \leq \Phi(R)$, so what is left to show is that $R/\Phi(E)\Phi(S)$ is Frattini-free (that is, has trivial Frattini subgroup). We shall use that all abelian normal subgroups of (finite) Frattini-free groups are complemented, and direct factors and direct products of (finite) Frattini-free groups are always Frattini-free. First, since $[E, S] = 1$, the subgroup $\Phi(E)\Phi(S)/\Phi(S)$ is central in the Frattini-free $S/\Phi(S)$. Its complement is a direct factor, so the complement is Frattini-free, and obviously isomorphic to the quotient $S/\Phi(E)\Phi(S)$. Next, $E\Phi(S)/\Phi(E)\Phi(S)$ is isomorphic to the Frattini-free $E/\Phi(E)$, and $R/\Phi(E)\Phi(S)$ is the direct product of $E\Phi(S)/\Phi(E)\Phi(S)$ and $S/\Phi(E)\Phi(S)$, so $R/\Phi(E)\Phi(S)$ is Frattini-free.

LEMMA 4.3. *If N is a normal subgroup of G contained in $\Phi(E)$, then $\mathsf{E}(G/N) = E/N$.*

Proof. Since all nontrivial homomorphic images of a quasisimple group are quasisimple, $\mathsf{E}(G/N) \geq E/N$. The converse inclusion will follow once we prove that if L is minimal among the subnormal subgroups of G such that LN/N is quasisimple then $L \leq E$. The minimality of L implies that L is perfect. Suppose that E does not contain L. Then E/N is a product of quasisimple subnormal subgroups different from LN/N, so $[LN/N, E/N] = 1$; that is, $[L, E] \leq N$. Since N is central in E, we have $[L, E, E] = 1$; and, as E is perfect, this implies that $[L, E] = 1$. Let $M/(L \cap N) = \mathsf{Z}(L/(L \cap N))$; then $[M, L] \leq L \cap N \leq E$ and so $[M, L, L] = 1$. Since L is perfect, this implies that $M \leq \mathsf{Z}(L)$, whence we see that L is quasisimple and therefore must lie in E. It was assumed that E does not contain L, so we have a contradiction which completes the proof of the lemma.

LEMMA 4.4. *If N is a normal subgroup of G contained in $\Phi(S)$, then $\mathsf{E}(G/N) = EN/N$.*

Proof. As $\mathsf{E}(G/N) \geq EN/N$ is obvious, only the converse inclusion needs proof. Let L be minimal among the subnormal subgroups of G such that LN/N is quasisimple; note that L is perfect. Since

$$[LN/N, S/N] \leq [\mathsf{E}(G/N), \mathsf{S}(G/N)] = 1,$$

we have $[L, S] \leq N$. Choose any prime p and any cyclic p'-subgroup C in L. Set $T = CS$; note that $[C, T] \leq N$, so $CN/N \leq \mathsf{Z}(T/N) \leq \mathsf{F}(T/N) = \mathsf{F}(T)/N$ (because $N \leq \Phi(S) \leq \Phi(T)$), and therefore $C \leq \mathsf{F}(T)$. In particular, C centralizes $\mathsf{O}_p(S)$ which is also $\mathsf{O}_p(G)$. Being a perfect group, L is generated by its cyclic p'-subgroups C, so L itself also centralizes $\mathsf{O}_p(G)$. This holds for all p, so L centralizes F, which of course contains the nilpotent subnormal subgroup $\mathsf{F}(L)$. It follows that $\mathsf{F}(L) = \mathsf{Z}(L)$, so

$L/\mathsf{F}(L)$ has trivial centre. On the other hand, $L/\mathsf{F}(L)$ is a homomorphic image of the quasisimple $L/(L \cap N)$: therefore $L/\mathsf{F}(L)$ is simple. This proves that L is quasisimple, whence $L \leqslant E$ follows.

Proof of Lemma 4.1. By Lemma 4.4 with $N = \Phi(S)$, we have that

$$\mathsf{E}(G/\Phi(S)) = E\Phi(S)/\Phi(S).$$

Of course, $\mathsf{S}(G/\Phi(S)) = S/\Phi(S)$. By Lemma 4.2 and Dedekind's Law,

$$E\Phi(S) \cap S = (E \cap S)\Phi(S) = \Phi(R).$$

Applied to $G/\Phi(S)$ in place of G, the first part of Lemma 4.2 therefore gives that $\Phi(\mathsf{E}(G/\Phi(S))) = \Phi(R)/\Phi(S)$. We may then apply Lemma 4.3 with $\Phi(R)/\Phi(S)$ in the role of N, to get the conclusion that $\mathsf{E}(G/\Phi(R)) = E\Phi(S)/\Phi(R)$. Of course, $\mathsf{F}(G/\Phi(R)) = F/\Phi(R)$, and so the claim of the lemma follows.

LEMMA 4.5. *Let H be a finite group such that $\mathsf{F}^*(H) = \mathsf{F}(H)$, and let $H = N_0 > N_1 > \cdots$ be a chief series of H such that $N_r = \mathsf{F}(H)$ and $N_t = \Phi(\mathsf{S}(H))$. Then $\bigcap_{s=r}^{t-1} \mathsf{C}_H(N_s/N_{s+1}) = \mathsf{F}(H)$.*

Proof. Note that $\mathsf{F}^*(G) = \mathsf{F}(G)$ is equivalent to $\mathsf{E}(G) = 1$. By Lemma 4.4 with H and N_t in place of G and N, we may assume without loss of generality that $N_t = 1$. Since the Fitting subgroup centralizes every chief factor, we assume also that the intersection in question properly contains $\mathsf{F}(H)$, and aim for a contradiction. The part of the chief series above $\mathsf{F}(H)$ may now be modified if necessary to arrange that N_{r-1} is contained in that intersection. Then the elements of N_{r-1} induce inner automorphisms on all factors of this chief series, so by the definition of generalized Fitting subgroup they all lie in $\mathsf{F}^*(H)$. This contradicts that $N_{r-1} > N_r = \mathsf{F}(H) = \mathsf{F}^*(H)$.

We shall use the theorem of [**10**] (which made use of the classification of finite simple groups) through the following result.

LEMMA 4.6. *Let H be a finite group and V a finite semisimple $\mathbb{Z}H$-module. Denote by n the composition length of V as abelian group. Then $H/\mathsf{C}_H(V)$ can be generated by $\frac{3}{2}n$ elements.*

Proof. We use induction on the number of distinct prime divisors p of $|V|$. When there is just one such prime, $H/\mathsf{C}_H(V)$ is a linear group of

dimension n over the relevant prime field, and the claim is the theorem of [10]: we have the initial step. For the inductive step, write V as $P \oplus Q$ with P a p-group and Q a p'-group. By Clifford's Theorem, P is semisimple as $C_H(Q)$-module; so, by the initial step, $\frac{3}{2} \dim P$ suitable elements will generate $C_H(Q)/C_H(V)$. On the other hand, by the inductive hypothesis, $\frac{3}{2}(n - \dim P)$ elements will generate $H/C_H(Q)$.

Now we come to the one point where the classification directly enters our arguments.

LEMMA 4.7. *If the socle of a finite group is the direct product of m nonabelian simple groups, then the group can be generated by $5m$ elements.*

Proof. Let N denote the intersection of the normalizers of the simple direct factors of the socle. This is a normal subgroup, and the quotient is a (not necessarily transitive) permutation group of degree m. Like any subgroup of S_m, this quotient can be generated by $m - 1$ elements. (This result does not depend on the classification and could indeed be older than that, though the earliest reference we know is 'Jerrum's algorithm' in [8].) We noted in the introduction that, since each simple group can be generated by 2 elements, it follows along the lines of Wiegold [15] that any direct product of m simple groups can be generated by $\max\{m, 2\}$ elements. It follows that the socle can be generated by $m + 1$ elements. The quotient of N modulo the socle is a subgroup of the direct product of the outer automorphism groups of m simple groups. From the description of the outer automorphism groups of the simple groups given in the Atlas [3], one can deduce that each subgroup of each such outer automorphism group can be generated by 3 elements; hence each subgroup of the direct product of m such groups can be generated by $3m$ elements.

Proof of Theorem 1.3. By Lemma 4.1, we may assume that $\Phi(R) = 1$. Set $H = C_G(E)$; then $F^*(H) = F(H) = F$, $S(H) = S$, and of course $\Phi(S) = 1$. Choose a chief series $H = N_0 > N_1 > \cdots$ in H through F; let r, t be the indices such that $N_r = F$, $N_t = 1$. Let V be the direct sum of the simple $\mathbb{Z}H$-modules N_s/N_{s+1} with $s = r, \ldots, t - 1$. By Lemma 4.5, $C_H(V) = F$.

Let m denote the number of simple direct factors of the central quotient $E/(E \cap H)$ of E, and n the composition length of F^*. The socle of G/H is isomorphic to $E/(E \cap H)$, so it is a direct product of m nonabelian simple groups. By Lemma 4.7, G/H can therefore be generated by $5m$ elements. The composition length of V as abelian group is $n - m$, so Lemma 4.6 yields that H/F can be generated by $\frac{3}{2}(n - m)$ elements, while of course F itself can be generated by $n - m$ elements. The conclusion is that $5m + \frac{5}{2}(n - m)$ elements will generate G; as $5m + \frac{5}{2}(n - m) \leq 5n$, the proof is complete.

5. Induced modules for soluble groups

We show here how to prove Theorem 1.5 and Corollary 1.6, using Theorem 1.4.

Consider an arbitrary finite soluble group H and a composition series

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_n = H.$$

Each composition factor N_i/N_{i-1} is cyclic of prime order: say,

$$N_i/N_{i-1} = \langle N_{i-1}x_i \rangle \quad \text{and} \quad |N_i/N_{i-1}| = p_i.$$

Each element h of H may then be written as a product of n factors, the ith factor being a power of x_i to an exponent which lies between 0 and $p_i - 1$ (inclusive): say,

$$h = \prod_{i=1}^{n} x_i^{h(i)} \quad \text{with} \quad 0 \leq h(i) < p_i \quad \text{for} \quad i = 1, \ldots, n.$$

Subject to these conditions, the exponents $h(i)$ are uniquely determined by h. We may call $\prod_{i=1}^{n} x_i^{h(i)}$ the *normal form* of h.

In terms of this normal form, we define on H a partial order $\preccurlyeq$ and a full order $\leqslant$, as follows. (It will turn out that $\leqslant$ is a refinement of $\preccurlyeq$, but we shall make no use of that.) Let $h_1 \preccurlyeq h_2$ if $h_1(i) \leq h_2(i)$ for $i = 1, \ldots, n$. It is clear that with respect to this partial order H is poset-isomorphic to the cartesian product of n chains of cardinalities $p_1, \ldots, p_n$, respectively. Let $h_1 < h_2$ if there is a j such that $h_1(j) < h_2(j)$ and $h_1(i) = h_2(i)$ whenever $i > j$. It will be useful for us to note that if $h_1 < h_2$ and j is chosen as above, then to each h_3 in H the element h_3' defined by

$$h_1 h_2^{-1} h_3 = h_3' x_j^{h_1(j) - h_2(j) + h_3(j)} \prod_{i>j} x_i^{h_3(i)} \tag{1}$$

lies in N_{j-1}. This follows because

$$h_3' = \left(\prod_{i<j} x_i^{h_1(i)}\right) x_j^{h_1(j) - h_2(j)} \left(\left(\prod_{i<j} x_i^{h_2(i)}\right)^{-1} \prod_{i<j} x_i^{h_3(i)}\right) x_j^{-(h_1(j) - h_2(j))},$$

each of the three products in this expression is in N_{j-1}, and this subgroup is normalized by x_j.

Given an arbitrary subgroup K in H, let $J = \{i \mid (K \cap N_i)N_{i-1} < N_i\}$. It is easy to see that

$$|(K \cap N_i) : (K \cap N_{i-1})| = \begin{cases} 1 & \text{if } i \in J, \\ p_i & \text{if } i \notin J, \end{cases}$$

and hence $|K| = \prod_{i \notin J} p_i$. Further, set $T = \{h \mid h(i) = 0 \text{ whenever } i \notin J\}$:

generally speaking, this T is not a subgroup, just a subset, and its cardinality $|T|$ is $\prod_{i\in J} p_i$, that is, $|H:K|$. Further, with $X_i = \{x_i^m \mid 0 \leq m < p_i\}$ we have

$$T \cap N_i = (T \cap N_{i-1})X_i \quad \text{whenever } i \in J. \tag{2}$$

Our next aim is to show, by induction on i, that

$$N_i = (K \cap N_i)(T \cap N_i) \quad \text{for } i = 1, \ldots, n. \tag{3}$$

The initial step $i = 1$ is straightforward; for the inductive step, suppose that $1 < i \leq n$. If $i \in J$, use first the inductive hypothesis and then (2) to see that

$$\begin{aligned} N_i = N_{i-1}X_i &= (K \cap N_{i-1})(T \cap N_{i-1})X_i \\ &\subseteq (K \cap N_i)(T \cap N_i) \subseteq N_i. \end{aligned}$$

If $i \notin J$, use the definition of J first and then the inductive hypothesis:

$$\begin{aligned} N_i = (K \cap N_i)N_{i-1} &= (K \cap N_i)(K \cap N_{i-1})(T \cap N_{i-1}) \\ &\subseteq (K \cap N_i)(T \cap N_i) \subseteq N_i. \end{aligned}$$

This completes the proof of (3). With $i = n$, we get $H = KT$; we have already seen that $|T| = |H:K|$; so it follows that T is a complete set of representatives of the right cosets of H modulo K.

Suppose now that $t_1, t_2, t_3 \in T$ with $t_1 < t_2 \leq t_3$. As in (1), we get that

$$t_1 t_2^{-1} t_3 = h x_j^{t_1(j) - t_2(j) + t_3(j)} \prod_{i>j} x_i^{t_3(i)}$$

with j and h such that $t_1(j) < t_2(j)$ and $h \in N_{j-1}$. Note that

$$0 \leq t_1(j) - t_2(j) + t_3(j) < p_j.$$

By (3), we can write $h = kt$ with $k \in K$ and $t \in T \cap N_{j-1}$. Define the element t_4 of H by

$$t_4(i) = \begin{cases} t(i) & \text{if } i < j, \\ t_1(j) - t_2(j) + t_3(j) & \text{if } i = j, \\ t_3(i) & \text{if } i > j: \end{cases}$$

then $t_1 t_2^{-1} t_3 \in K t_4$. Using that $j \in J$ and $t_4(j) < t_3(j)$ because $t_1(j) < t_2(j)$, we see that $t_4 \in T$ and $t_4 < t_3$. It remains to observe that $T = \prod_{i\in J} X_i$ shows T to be, as poset with respect to $\leq$, a cartesian product of chains. What we have proved may be summed up as follows.

LEMMA 5.1. *Let K be a subgroup in a finite soluble group H. Then there is a right transversal T to K in H, with a partial order $\preccurlyeq$ and a full order $\leqslant$, such that whenever $t_1 < t_2 \preccurlyeq t_3$ $(t_1, t_2, t_3 \in T)$ there is a t_4 in T such that $t_4 < t_3$ and $t_1 t_2^{-1} t_3 \in K t_4$. With respect to this partial order, T is a cartesian product of chains.*

With H, K, and T as above, let U be a finite dimensional (right) K-module (over an arbitrary field). Each element v of the induced module $U\uparrow^H$ may then be written as $v = \sum_{t \in T} u(v, t) \otimes t$ with uniquely determined elements $u(v, t)$ in U. For $v \neq 0$, by the 'height' of v we mean the 'largest' element of the set $\{t \in T \mid u(v, t) \neq 0\}$ in terms of the full order $\leqslant$; we write the height of v as $\tau(v)$, and define $\mu(v)$ *as* $u(v, \tau(v))$. Thus $\mu(v) \neq 0$, and $u(v, t) = 0$ whenever $t > \tau(v)$. We shall refer to $\mu(v) \otimes \tau(v)$ as the 'leading summand' of v. The point of the first half of Lemma 5.1 is that if the height of v is t_2 and if $t_2 \preccurlyeq t_3$ then the height of $v t_2^{-1} t_3$ is t_3; indeed, then the leading summand of $v t_2^{-1} t_3$ is $\mu(v) \otimes t_3$. We shall use this to establish a key technical point.

LEMMA 5.2. *Each submodule of $U\uparrow^H$ can be generated by a set V of nonzero elements with the following property: no subset W of V whose image $\tau(W)$ in T is a chain with respect to $\preccurlyeq$ can have more than* $\dim U$ *elements.*

Proof. Set $\dim U = a$, let U' be a submodule of $U\uparrow^H$, and let V be a finite generating set of U' consisting of nonzero elements. Suppose that there are $a + 1$ distinct elements $v_0, \ldots, v_a$ in V such that $\tau(v_0) \preccurlyeq \cdots \preccurlyeq \tau(v_a)$. For $i = 0, \ldots, a$, denote by d_i the dimension of the subspace of U spanned by $\mu(v_0), \ldots, \mu(v_i)$. We must have $d_{j-1} = d_j$ for some j between 1 and a. Then $\mu(v_j)$ is a linear combination of the $\mu(v_i)$ with $i < j$, and the corresponding linear combination of the elements $v_i \tau(v_i)^{-1} \tau(v_j)$ with $i < j$ has the same leading summand as v_j. Consequently, v_j may be either omitted from V or replaced in V by an element with height strictly preceding $\tau(v_j)$ in the full order $\leqslant$, in such a way that the set so obtained from V still generates U'. This procedure can only be repeated finitely many times, and when it is no longer available then the generating set has the required property.

We shall make use of the following direct consequence of a well known theorem of Dilworth (Theorem 3.2.1 in [2]): *if a poset V contains no antichain of cardinality greater than m, nor any chain of cardinality greater than n, then V has at most mn elements.*

Proof of Theorem 1.5. The second half of Lemma 5.1 makes Theorem 1.4 applicable: no antichain in T has cardinality greater than $bd/\sqrt{\log d}$

where $d = |T| = |H:K|$. For each t in T, choose a full order on the set of nonzero elements of $U\uparrow^H$ of height t. Define a partial order on the set of nonzero elements of $U\uparrow^H$ as follows: let $v \prec w$ mean that either $\tau(v) < \tau(w)$ or $\tau(v) = \tau(w)$ and v precedes w in the full order chosen for the elements of height $\tau(v)$. Then τ is a poset homomorphism which maps incomparable elements to incomparable elements, so no antichain of its domain can have cardinality greater than $bd/\sqrt{\log d}$. By Lemma 5.2, each submodule of $U\uparrow^H$ has a generating set V which contains no chain of cardinality greater than $\dim U$. By the consequence of Dilworth's Theorem mentioned above, such a generating set V has at most $(\dim U)bd/\sqrt{\log d}$ elements.

Proof of Corollary 1.6. Clearly we can assume that A is nontrivial. Identify A with one of the coordinate subgroups of the wreath product, and let K be the normalizer $N_H(A)$; note that $|H:K| = d$. Let A_1 be a minimal characteristic subgroup of A, and a_1 the composition length of A_1. This subgroup is normalized by K, and may be viewed as a K-module of dimension a_1 over a finite prime field. The base group B is the direct product of the distinct H-conjugates of A; let B_1 denote the direct product of the distinct H-conjugates of A_1. As H-module, B_1 is generated by the K-submodule A_1, and $\dim B_1 = |H:K| \dim A_1$: this proves (see Corollary 3 on p. 56 of Alperin [1]) that B_1 is (isomorphic to) the H-module induced from the K-module A_1.

We are now ready to prove Corollary 1.6 by induction on a. If $a = a_1$, the claim comes directly from Theorem 1.5, and this can serve as the initial step. If $a > a_1$ and V is an H-subgroup of B, then Theorem 1.5 gives that as H-group $B_1 \cap V$ can be generated by $a_1 bd/\sqrt{\log d}$ elements, while by the inductive hypothesis $(a - a_1)bd/\sqrt{\log d}$ elements will generate the H-group B_1V/B_1. As $V/(B_1 \cap V)$ is H-isomorphic to B_1V/B_1, the claim follows.

6. Soluble transitive groups and irreducible groups

Proof of Theorem 1.7. It is clear that, given b, there exists c' such that

$$x^2 + x \leq c'2^x/\sqrt{x} \quad \text{and} \quad b(x^2 + x)\sqrt{(x+1)} \leq c'(2^x - \sqrt{(x+1)})$$

whenever $x \geq 1$. We prove by induction on d that if c' satisfies these conditions with a number b which has the property asserted in Corollary 1.6, then c' has the property asserted in Theorem 1.7.

The initial step is to show that if G is a soluble primitive permutation group of degree d then it can be generated by the relevant number of elements. Indeed, we claim more, namely that in this case the composition length of G is less than $c'd/\sqrt{\log d}$. Each soluble primitive

permutation group is a subgroup of an affine general linear group over a prime field, so $d = p^n$ with p prime and a point stabilizer in G is a subgroup of $GL(n, p)$. Since $|GL(n, p)| < p^{n^2}$, this implies that

$$\log |G| < (n^2 + n) \log p < (n \log p)^2 + n \log p.$$

Thus $\log |G| < x^2 + x$ where $x = \log d$. The claim then follows from the first defining property of c'.

The inductive step is concerned with imprimitive G. In this case (cf. Theorem 3.3 in Suprunenko's book [**13**]), $d = mn$ with $m \geq 2$, $n \geq 2$, and G is contained in a wreath product $A \operatorname{wr} S_n$ with A a soluble primitive group of degree m, in such a way that the top projection of G is a (soluble) transitive subgroup of S_n. Set $x = \log m$ and $y = \log n$, and denote by a the composition length of A: we know from the preceding paragraph that $a < x^2 + x$. Let B denote the base group of the wreath product, and H a subgroup of G minimal with respect to $(B \cap G)H = G$: then all maximal subgroups of H must contain $B \cap H$, and so $B \cap H$ is contained in the Frattini subgroup of H. On the other hand, $H/(B \cap H)$ is isomorphic to the top projection of G; by the inductive hypothesis, that can be generated by $c'2^y/\sqrt{y}$ elements; therefore, so can H. We know from Corollary 1.6 that $B \cap G$, like any other H-subgroup of B, can be generated as H-group by $ab2^y/\sqrt{y}$ elements.

In combination, these arguments yield that G can certainly be generated by $((x^2 + x)b + c')2^y/\sqrt{y}$ elements, while what we need to prove is that $c'2^{x+y}/\sqrt{(x + y)}$ elements will generate it. Using first that $y \geq 1$ and then the second defining property of c', one gets

$$((x^2 + x)b + c')\sqrt{((x + y)/y)} \leq ((x^2 + x)b + c')\sqrt{(x + 1)} \leq c'2^x,$$

so $((x^2 + x)b + c')2^y/\sqrt{y} \leq c'2^{x+y}/\sqrt{(x + y)}$, and the inductive step is complete.

LEMMA 6.1. *If $\mathbb{F}$ and $q_{\mathbb{F}}$ are as in Lemma* 3.4 *and if G is a finite soluble primitive linear group of degree at most d over $\mathbb{F}$, then G has a cyclic normal subgroup C of order at most $q_{\mathbb{F}}^d$ such that* $\log |G/C| \leq 2 \log d + 4(\log d)^2$.

Proof. This amounts to quoting Suprunenko. Theorem 19.5 in [**13**] yields that if G is a finite soluble primitive linear group of degree at most d (over an arbitrary field $\mathbb{F}$) then G has an abelian normal subgroup C such that $\log |G/C| \leq \log d^2 + (\log d^2)^2$. By Lemma 19.1 of [**13**], this C lies in the multiplicative group of a field extension of degree at most d. By Lemma 3.4, this completes the proof.

Proof of Theorem 1.8. Given b and c', there exists c'' such that

$$c''2^x \geq (4x^2 + 2x + 1)\sqrt{x} \quad \text{and} \quad c''2^x \geq 2\sqrt{x} + ((4x^2 + 2x)b + c')\sqrt{(x + 1)}$$

whenever $x \geqslant 0$. We prove that if c'' satisfies these conditions with a number b which has the property asserted in Corollary 1.6 and a c' which has the property asserted in Theorem 1.7, and if $q_{\mathbb{F}}$ is as in Lemma 3.4, then $c'_{\mathbb{F}} = \frac{2}{\sqrt{3}} b \log q_{\mathbb{F}} + c''$ defines a number with the property asserted in Theorem 1.8.

The first step is to show that if G is a finite soluble primitive linear group of degree d over $\mathbb{F}$ then it can be generated by the relevant number of elements. In view of Lemma 6.1, this is immediate from the first defining property of c''.

The harder second step is concerned with imprimitive G. In this case (see § 15 in [**13**]), $d = mn$ with $m \geqslant 1$, $n \geqslant 2$, and G is contained in a wreath product A wr S_n with A a soluble primitive linear group of degree m over $\mathbb{F}$, in such a way that the top projection of G is a (soluble) transitive subgroup of S_n. Set $x = \log m$ and $y = \log n$: in these terms, what we have to show is that G can be generated by $c'_{\mathbb{F}} 2^{x+y}/\sqrt{(x+y)}$ elements. As in the proof of Theorem 1.7, we take a minimal supplement H for $B \cap G$ in G and argue (this time using Theorem 1.7 itself rather than an inductive hypothesis) that H can be generated by $c' 2^y/\sqrt{y}$ elements. As there, we shall also use that $\sqrt{(x+1)} \geqslant \sqrt{((x+y)/y)}$ (because $y \geqslant 1$).

Consider first the case $3x \leqslant y$: then also $\frac{2}{\sqrt{3}} \geqslant \sqrt{((x+y)/y)}$. By Lemma 6.1, the composition length of A is at most $(\log q_{\mathbb{F}})2^x + 4x^2 + 2x$, and so Corollary 1.6 yields that as H-group $B \cap G$ can be generated by $((\log q_{\mathbb{F}})2^x + 4x^2 + 2x)b2^y/\sqrt{y}$ elements. These facts and the second defining property of c'' readily combine to give what we want.

Finally consider the case $3x > y$: then $2\sqrt{x} > \sqrt{(x+y)}$. By Lemma 6.1, A has a cyclic normal subgroup C of small index. There is a homomorphism from A wr S_n onto (A/C) wr S_n, with kernel a direct product of 2^y copies of C. The intersection of G with that kernel can obviously be generated by 2^y elements. The image of G under that homomorphism can be seen, by an analogue of the argument above, to be generated by $((4x^2 + 2x)b + c')2^y/\sqrt{y}$ elements. Once more it is the second defining property of c'' which is needed to see that the required inequality holds.

7. Concluding remarks

We begin this section with the *proof of Corollary 1.9.* Suppose that $\mathsf{R}(G) = G$: then G is the central product of $\mathsf{E}(G)$ and $\mathsf{S}(G)$. Therefore it follows (cf. Corollary 3.3) from Clifford's Theorem that if G has a faithful irreducible representation of degree at most d over a field $\mathbb{F}$ then so do

$\mathsf{E}(G)$ and $\mathsf{S}(G)$. Similarly, if a transitive permutation representation of G is faithful, then $\mathsf{E}(G)$ and $\mathsf{S}(G)$ are faithful on each of their orbits; thus if G has a faithful transitive permutation representation of degree at most d then so do $\mathsf{E}(G)$ and $\mathsf{S}(G)$. By the first part of Lemma 4.2, $\mathsf{E}(G) \cap \mathsf{S}(G)$ lies in $\Phi(G)$, so it suffices to show that the quotient of G over this intersection can be generated by the asserted number of elements. That quotient is the direct product of a perfect group and a soluble group, and it is well known (cf. Wiegold [15]) that if each of the two direct factors of such a product can be generated by a certain number of elements then so can the product itself.

From our first reference to [15] in the introduction, we see that $\mathsf{E}(G)$ can be generated by $\max\{cd/\sqrt{\log d}, 2\}$ elements in Theorem 1.1, while in Theorem 1.2 it can be generated by $\max\{c_{\mathbb{F}}^{\sharp} d/\sqrt{\log d}, 2\}$ elements. We noted after the proof of Corollary 2.3 that $c \geq 1/\sqrt{2}$, while if $\mathsf{E}(G) \neq 1$ then in the permutation representation case $d \geq 5$; so $cd/\sqrt{\log d} > 2$ whenever this is relevant. On the other hand, each $GL(2, \mathbb{F})$ has noncyclic soluble irreducible subgroups, so we always have $c_{\mathbb{F}}' \geq 1$: therefore $\max\{c_{\mathbb{F}}^{\sharp}, c_{\mathbb{F}}'\} d/\sqrt{\log d} \geq 2$ whenever $d \geq 2$. In view of Theorems 1.7 and 1.8, Corollary 1.9 now follows.

We conclude the paper with two fragments. The first concerns Theorem 1.5. One may well ask whether this is the right kind of result to aim for in general. For example, it is easy to see that if the characteristic of the ground field does not divide the order of H then each submodule of $U\uparrow^H$ can be generated by $\dim U$ elements, and the index $d = |H:K|$ plays no role at all. This shows that we are facing a strictly modular issue: in characteristic p, should we not seek a bound which is independent of the p'-part of the index d? Further encouragement comes from the following (where, as before, d_p stands for the p-part of d).

LEMMA 7.1. *If K is a subgroup of index d in a finite p-soluble group H, and U is a K-module of composition length m over an algebraically closed field of characteristic p, then each submodule of $U\uparrow^H$ can be generated by md_p elements.*

Proof. It is sufficient to prove the claim for simple U. Let V be any simple H-module, and denote by $P(U)$, $P(V)$ the projective covers of U, V, respectively. Note that $\dim P(U) \geq |K|_p$ while $\dim P(V) \leq (\dim V)\,|H|_p$ (because when the restriction of V to a Hall p'-subgroup is induced to H, the result is a projective module which maps onto V), so the Krull-Schmidt multiplicity of $P(U)$ in $P(V)\downarrow_K$ cannot be larger than $(\dim V)d_p$. That multiplicity is $\dim \mathrm{Hom}(P(V)\downarrow_K, U)$, which in turn equals $\dim \mathrm{Hom}(P(V), U\uparrow^H)$ (see Lemma 8.6(2) in [1]): hence (see Exercise

5.2 of [1]) the Jordan-Hölder multiplicity of V in $U\uparrow^H$ cannot exceed $(\dim V)d_p$.

However, a simple example serves as a warning: *even if we restrict attention to 1-dimensional trivial U, no bound in terms of d_p can be better than linear.* Let $H = AGL(1, p^n)$ and $K = 1$, so $d_p = p^n$. Over the complex field, H has $p^n - 1$ linear characters and just one other irreducible character, of degree $p^n - 1$; over an algebraically closed field of characteristic p, there are only the $p^n - 1$ linear characters. The decomposition matrix is an identity matrix augmented by an extra row with all entries 1, whence the Cartan matrix is the sum of the identity matrix and the matrix with all entries 1. The regular H-module is therefore a direct sum of $p^n - 1$ summands each of which has at least one trivial section of dimension 1, so the regular module itself has a trivial section of dimension $p^n - 1$: thus it has a submodule which cannot be generated by fewer than $d_p - 1$ elements.

The example warns against another idea as well. By [9], the regular module for the socle of H has each of its submodules generated by at most $2p^n/\sqrt{n}$ elements; as we have just seen, the regular module for H has submodules needing $p^n - 1$ generators; of course, if $n \geqslant 5$ then $p^n - 1 > 2p^n/\sqrt{n}$. This illustrates that, *even if the group is soluble and the induction is from a normal subgroup whose index is prime to the characteristic, the number of elements required for the generation of submodules may increase.*

For a finite group G such that $\mathsf{F}^*(G)$ admits a faithful transitive permutation representation of degree $d \geqslant 2$, Theorem 1.1 (applied with $\mathsf{F}^*(G)$ in place of G) and Theorem 1.3 yield that G may be generated by $5cd/\sqrt{\log d}$ elements. The second fragment is adapted from our first proof of the existence of a constant which could play the role of $5c$ here. We reproduce it because it does seem to have some independent interest.

LEMMA 7.2. *If G is a finite group and H is a subgroup of index d in G, then G can be generated by $\dfrac{5}{\log 5}\log d$ elements together with a subnormal subgroup contained in H.*

Proof. This only needs proof if $d \geqslant 2$. By Lemma 7.3 below, if H is a maximal subgroup then the intersection of the G-conjugates of H can serve here as the subnormal subgroup. This provides the initial step for a proof by induction on d. For the inductive step, let $H < K < G$, $|G:K| = m$, $|K:H| = n$ (so $\log m + \log n = \log d$), and let S be a subnormal subgroup of G contained in K such that G can be generated by S and $\dfrac{5}{\log 5}\log m$ further elements. Then HS is a subset (though not necessarily

a subgroup) of K with cardinality $|H|\,|S|/|H \cap S|$, whence $|S:(H \cap S)| \leq |K:H| = n < d$, so the inductive hypothesis may be applied once more: S has a subnormal subgroup, T say, which is contained in $H \cap S$ and which together with $\frac{5}{\log 5}\log n$ elements generates S. It follows that G can be generated by the subnormal subgroup T and $\frac{5}{\log 5}\log d$ further elements.

Our superseded proof used a much weaker lemma, with a constant multiple of $\sqrt{d}\,(\log d)^2$ in place of $\frac{5}{\log 5}\log d$, with a similar inductive proof. The initial step for that came from results of Babai and Pyber (see Theorems 2.4 and 2.5 in [**12**]), which together bound the order of a primitive permutation group of degree d that does not contain the alternating group (of that degree). Those results of Babai and Pyber do not depend on the classification of the finite simple groups. Then Professor Pyber pointed out (see p. 201 in [**12**]) that two of our easy lemmas and the theorem of [**10**] (which do depend on the classification) readily yield the following result.

LEMMA 7.3 (cf. [**12**]). *Each primitive permutation group of degree d can be generated by $\frac{5}{\log 5}\log d$ elements.*

Proof. If the socle is a direct product of nonabelian simple groups, this follows from Lemmas 2.5 and 4.7. Otherwise the socle is a self-centralizing minimal normal subgroup of order d, and d is a prime power; say, $d = p^k$. By [**10**], the quotient modulo the socle can be generated by $\frac{3}{2}k$ elements, so the group itself is generated by $1 + \frac{3}{2}k$ elements. If $k \geq 2$ then $1 + \frac{3}{2}k \leq \frac{5}{\log 5}\log p^k$, while if $k = 1$ then the group can be generated by two elements and of course $2 < \frac{5}{\log 5}$.

This seems to be of considerable interest in its own right.

REFERENCES

1. J. L. Alperin, *Local representation theory*, Cambridge University Press, Cambridge, 1986.
2. Ian Anderson, *Combinatorics of finite sets*, Oxford University Press, Oxford, 1987.
3. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.
4. L. Di Martino and M. C. Tamburini, '2-Generation of finite simple groups and some related topics', in *Generators and relations in groups and geometries*, proceedings of the NATO Advanced Study Institute, Castelvecchio Pascoli (Lucca), Italy, April 1–14,

1990, ed. by A. Barlotti et al., Kluwer Academic Publishers, Dordrecht, Boston, 1991, pp. 195–233.
5. J. D. Dixon and L. G. Kovács, 'Generating finite nilpotent irreducible linear groups', *Quart. J. Math. Oxford* (2) 44 (1993), 1–15.
6. B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin–Heidelberg–New York, 1967.
7. B. Huppert and N. Blackburn, *Finite groups II, III*, Springer-Verlag, Berlin–Heidelberg–New York, 1982.
8. Mark Jerrum, 'A compact representation for permutation groups', *J. Algorithms* 7 (1986), 60–78.
9. L. G. Kovács and M. F. Newman, 'Generating transitive permutation groups', *Quart. J. Math. Oxford* (2) 39 (1988), 361–372.
10. L. G. Kovács and Geoffrey R. Robinson, 'Generating finite completely reducible linear groups', *Proc. Amer. Math. Soc.* 112 (1991), 357–364.
11. Reinhard Laue, Zur minimalen Erzeugendenzahl endlicher auflösbarer Gruppen, *Arch. Math.* 35 (1980), 8–14.
12. László Pyber, 'Asymptotic results for permutation groups', in *Groups and Computation*, ed. by Larry Finkelstein and William M. Kantor, DIMACS: Series in Discrete Mathematics and Computer Science 11, Amer. Math. Soc., Providence, 1993, pp. 197–219.
13. D. A. Suprunenko, *Matrix groups*, Translations of mathematical monographs 45, Amer. Math. Soc., Providence, 1976.
14. G. E. Wall, 'A characterisation of $PSL_2(\mathbf{Z}_{p^\lambda})$ and $PGL_2(\mathbf{Z}_{p^\lambda})$', *J. Austral. Math. Soc.* 8 (1968), 523–543.
15. James Wiegold, 'Growth sequences of finite groups III', *J. Austral. Math. Soc. Ser. A* 25 (1978), 142–144.

Department of Mathematics
University of Manchester Institute of Science and Technology
PO Box 88
Manchester M60 1QD, UK

School of Mathematical Sciences
Australian National University
Canberra ACT 0200, Australia

Department of Mathematics
University of Florida
Gainesville FL 32611, USA

Present address:
Department of Mathematics
University of Leicester
Leicester LE1 7RH, UK

Note added in proof. F. Dalla Volta and A. Lucchini have shown that the number 5 can be replaced by 3 in Lemma 4.7: see their forthcoming paper 'Minimal number of generators and composition length of socle in finite groups', *Quart. J. Math. Oxford*, to appear. This yields a similar improvement to Theorem 1.3 (and can be used to improve Lemmas 7.2 and 7.3).