ISRAEL JOURNAL OF MATHEMATICS **137** (2003), 265–284

ENUMERATING FINITE GROUPS WITHOUT ABELIAN COMPOSITION FACTORS

BY

BENJAMIN KLOPSCH

Mathematisches Institut, Heinrich-Heine-Universität
Düsseldorf, Germany
e-mail: klopsch@math.uni-duesseldorf.de

ABSTRACT

Let Σ denote the class of all *non-abelian* finite simple groups. We are concerned with enumerating poly-Σ groups, that is finite groups without abelian composition factors. For any natural number n let $\mathbf{g}_\Sigma(n)$ denote the number of (isomorphism classes of) poly-Σ groups of order at most n. We determine the growth rate of the sequence $\mathbf{g}_\Sigma(n)$, $n \in \mathbb{N}$.

Similarly, for any $S \in \Sigma$ we give estimates for the numbers $\widehat{\mathbf{g}}_S(k)$ of poly-S groups of composition length at most k, as k tends to infinity. This initiates an investigation somewhat complementary to the "classical" enumeration of finite p-groups by Higman [6] and Sims [15].

Our ancillary results include upper bounds for the minimal number of generators and for the number of (equivalence classes of) permutation actions of any given poly-Σ group.

1. Introduction

1.1. MOTIVATION AND MAIN RESULTS. The problem of determining the numbers $\mathbf{f}(n)$ of (isomorphism classes of) groups of order n is as old as Cayley's introduction of the abstract group concept. In 1895 Hölder [8] established a beautiful formula which yields $\mathbf{f}(n)$ for all square-free n. In contrast, it is now considered unlikely that an equally explicit formula can be found if n is allowed to take prime power values; cf. [13, Section 2]. Modern computer algorithms determine $\mathbf{f}(n)$ successfully in the range $1 \leq n \leq 2000$; see [2].

Received September 30, 2002

The asymptotic behaviour of the arithmetic function $\mathbf{f}(n)$, $n \in \mathbb{N}$, and certain variants — enumerating only groups of some restricted type — came under investigation in the early 1960s. For any given prime p, Higman and Sims determined the asymptotic growth rate of the sequence $\mathbf{f}(p^k)$, $k \in \mathbb{N}$, thus estimating the number of p-groups of any given order: their results in [6] and [15] show that

$$p^{\frac{2}{27}k^3 - O(k^2)} \leq \mathbf{f}(p^k) \leq p^{\frac{2}{27}k^3 + O(k^{8/3})} \quad \text{as } k \to \infty. \tag{1.1}$$

Since then there has been a steady interest in the subject, especially, after the classification of finite simple groups (CFSG) made the general enumeration problem much more treatable [11, 4, 9, 7]. Indeed, in 1993 Pyber [12] succeeded in showing that $\mathbf{f}(n) \leq n^{(2/27+o(1))\mu(n)^2}$ as n tends to infinity, where $\mu(n)$ denotes the exponent of the highest prime power dividing n.

For every $n \in \mathbb{N}$ let $\mathbf{g}(n)$ denote the number of (isomorphism classes of) groups of order at most n. For every $n \in \mathbb{N}$ the interval $[n/2, n]$ contains a power of 2, and thus Pyber's result combined with (1.1) yields

$$n^{(\frac{2}{27} - o(1))(\log_2 n)^2} \leq \mathbf{g}(n) \leq n^{(\frac{2}{27} + o(1))(\log_2 n)^2} \quad \text{as } n \to \infty.$$

The purpose of this paper is to consider a restricted enumeration problem which in a way complements the "classical" situation studied by Higman and Sims. Let Σ denote the class of all **non-abelian** finite simple groups. For every $n \in \mathbb{N}$ let $\mathbf{g}_\Sigma(n)$ denote the number of (isomorphism classes of) poly-Σ groups of order at most n, and for every $S \in \Sigma$ and $k \in \mathbb{N}$ let $\widehat{\mathbf{g}}_S(k)$ denote the number of (isomorphism classes of) poly-S groups of composition length at most k.* Thus we propose to count groups which are far from soluble, or in the above parlance: far from poly-abelian.

Intuitively, it is clear that $\mathbf{g}_\Sigma(n)$ grows much slower than $\mathbf{g}(n)$ as n tends to infinity; cf. [4]. But what is the precise growth rate of the sequence $\mathbf{g}_\Sigma(n)$, $n \in \mathbb{N}$? And, given $S \in \Sigma$, what is the growth rate of $\widehat{\mathbf{g}}_S(k)$ as k tends to infinity? In view of the successful enumeration of finite p-groups by Higman and Sims these questions appear very natural. Our main results are

THEOREM A (Enumeration of poly-Σ groups): *There exist constants $B, C \in \mathbb{R}_{>0}$ such that for all $n \in \mathbb{N}$,*

$$n^{B \log_2 \log_2 n} \leq \mathbf{g}_\Sigma(n) \leq n^{C \log_2 \log_2 n}.$$

* If Γ is any class of groups, then a poly-Γ group is a group G which allows a finite subnormal series $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$ such that each factor G_i/G_{i-1} is isomorphic to some group in Γ. If $\Gamma = \{H\}$ contains a single element, we also speak of poly-H instead of poly-Γ groups. A poly-Σ group is just a finite group without abelian composition factors.

THEOREM B (Enumeration of poly-S groups): *For every non-abelian finite simple group S there exist constants $B, C \in \mathbb{R}_{>0}$ such that for all $k \in \mathbb{N}$,*

$$k^{Bk} \leq \widehat{\mathbf{g}}_S(k) \leq k^{Ck}.$$

Our methods allow us to bound the constants appearing in Theorems A and B quite explicitly — e.g. one may take $C = 53$ in Theorem A — but most likely this is not optimal. Thus one feels compelled to ask the following intriguing

Question: Let $S \in \Sigma$. Does there exist a constant $C = C(S) \in \mathbb{R}_{>0}$ such that $\widehat{\mathbf{g}}_S(k) = k^{Ck+o(k)}$? If so, how does its value depend on S?

As far as I know this is completely open, even for alternating groups. As indicated above, the analogous problem for finite p-groups has positive solution and the constant involved depends uniformly on the prime p; see (1.1).

1.2. DETAILED DISCUSSION AND ANCILLARY RESULTS. Clearly, for every $S \in \Sigma$ and all $k \in \mathbb{N}$ we have $\widehat{\mathbf{g}}_S(k) \leq \mathbf{g}_\Sigma(|S|^k)$. So the lower bound in Theorem A can be derived from the lower bound in Theorem B; conversely, the upper bound in Theorem A yields the upper bound in Theorem B.

At first sight the lower bound in Theorem B may come as a surprise, because groups without abelian composition factors are known to have a very rigid structure. For instance, if $S \in \Sigma$ is such that $\mathrm{Aut}(S)$ splits over $\mathrm{Inn}(S)$, then every poly-S group can be written as an iterated twisted wreath product of several copies of S; see [1]. Nevertheless we are able to manufacture sufficiently many poly-S groups of socle length just two.

The proof of the upper bound in Theorem A has two main ingredients. Using recursive methods we construct small generating sets for poly-Σ groups. Writing $d(G)$ for the minimal number of generators of a finite group G and $\mathrm{com}(G)$ for its composition length, we show

PROPOSITION 1.1: *Every non-trivial finite group G without abelian composition factors satisfies*

$$d(G) \leq 3 \log_2 \mathrm{com}(G) + 2.$$

This can be regarded as a first step towards generalizing results of Wiegold and others on growth sequences of finite simple groups: given $S \in \Sigma$, there are rather precise estimates for the generating numbers $d(S^k)$, $k \in \mathbb{N}$; e.g., see [10]. A much more elementary observation shows that every poly-Σ group can be generated by a single conjugacy class of elements; see Proposition 4.3.

Proposition 1.1 and a rather crude, but often-used argument (based on the fact that every poly-Σ group embeds into the automorphism group of its socle;

e.g., see [11, 4]) already ensure the existence of a constant $C \in \mathbb{R}_{>0}$ such that for all $n \in \mathbb{N}$ we have $\mathbf{g}_\Sigma(n) \leq n^{C(\log_2 \log_2 n)^2}$. The sharper estimate provided in Theorem A requires a new ingredient, namely information about the number of permutation actions of a given poly-Σ group.

PROPOSITION 1.2: *There exists a constant $C \in \mathbb{R}_{>1}$ such that for all $n \in \mathbb{N}$ every non-trivial finite group G without abelian composition factors admits (up to equivalence) at most $C^{n(\log_2 \mathrm{com}(G)+\log_2 n)}$ permutation representations of degree n. In fact, one may take $C = 2^{24}$.*

It is not difficult to bound the number of normal subgroups of a poly-Σ group. This leads to the following interesting consequence.

COROLLARY 1.3: *There exists a constant $C \in \mathbb{R}_{>1}$ such that for all $n \in \mathbb{N}$ every finite group G without abelian composition factors admits (up to equivalence) at most $C^{n \log_2 n}$ faithful permutation representations of degree n. In fact, one may take $C = 2^{48}$.*

These bounds for the number of permutation representations of poly-Σ groups are somewhat reminiscent of similar estimates which have been established for groups with "restricted sections"; e.g., see [3, Theorem 1.2]. But in fact there is little common ground, because in our setting **all** non-abelian finite simple groups are allowed as composition factors, and hence the powerful Babai–Cameron–Pálfy restrictions simply do not apply. Another noteworthy difference is that our approach relies much less on consequences of CFSG.

All our results are true for finite groups whose composition factors belong to the list of "known" simple groups, and we only require the following consequences of CFSG: the validity of Schreier's conjecture, the fact that finite simple groups are two-generated, and — for the upper bounds in Theorems A and B — the fact that there are at most two non-isomorphic finite simple groups of any prescribed order (actually a suitable weaker bound would be enough).

1.3. ORGANIZATION OF THE PAPER AND NOTATION. Section 2 provides basic estimates for the socle size and socle length of a poly-Σ group. In Section 3 we bound the minimal number of generators required by a poly-Σ group and thus establish Proposition 1.1. Section 4 contains two results about the normal subgroups of a poly-Σ group. In Section 5 we study permutation representations of poly-Σ groups and verify Proposition 1.2. The proof of Theorems A and B appears in Sections 6 (upper bound) and 7 (lower bound).

Our notation is mostly standard. For every $x \in \mathbb{R}_{>0}$ we write $\log x := \log_2 x$ for brevity. If necessary, the reader can look up the definitons of

Σ, $\mathbf{g}_\Sigma(n)$, $\hat{\mathbf{g}}_S(n)$, $d(G)$, com(G), poly-Σ, poly-S group	in Section 1;
soc(G), soc$_i(G)$, sol(G)	in Section 2;
anything related to socle types $\mathbf{M}$	in Section 6.

2. The socle series of a poly-Σ group

Let G be a finite group. The characteristic subgroup soc$(G) \leq G$ generated by all the minimal normal subgroups of G is called the **socle** of G. More generally, the **socle series**

$$1 = \mathrm{soc}_0(G) \leq \mathrm{soc}_1(G) \leq \cdots \leq G$$

of G is defined recursively as follows: $\mathrm{soc}_0(G) := 1$, and for every $i \in \mathbb{N}$ the i-th term $\mathrm{soc}_i(G)$ is to satisfy the condition $\mathrm{soc}(G/\mathrm{soc}_{i-1}(G)) = \mathrm{soc}_i(G)/\mathrm{soc}_{i-1}(G)$. The **socle length** of G is $\mathrm{sol}(G) := \min\{i \in \mathbb{N}_0 |\ \mathrm{soc}_i(G) = G\}$.

Suppose that G is poly-Σ. As explained in the introduction, this just means that G is a finite group without abelian composition factors. Then its socle is the direct product of non-abelian simple groups, say

$$M := \mathrm{soc}(G) \cong S_1^{n_1} \times \cdots \times S_r^{n_r}, \quad S_i \in \Sigma \text{ for } i \in \{1, 2, \ldots, r\},$$

where $S_i \cong S_j$ if and only if $i = j$. The centralizer $C_G(M)$ is normal in G, but M has trivial center. So $C_G(M) = 1$, and G acts faithfully on M by conjugation. It is easily seen that

$$\mathrm{Aut}(M) \cong \prod_{i=1}^{r} \mathrm{Aut}(S_i) \wr \mathrm{Sym}(n_i),$$

where all wreath products are formed with respect to the natural permutation actions.

A consequence of CFSG is the validity of Schreier's conjecture: the outer automorphism group of every finite simple group is soluble. This fact implies that

$$G/M \hookrightarrow \mathrm{Sym}(n_1) \times \cdots \times \mathrm{Sym}(n_r) \hookrightarrow \mathrm{Sym}(n)$$

where $n = \sum_{i=1}^{r} n_i = \mathrm{com}(M)$.

LEMMA 2.1: *Let A be a direct product of finitely many elementary abelian groups, and let $|A| = p_1^{e_1} \cdots p_r^{e_r}$ be the prime power factorization of $|A|$. Then A embeds into the symmetric group* Sym(n) *if and only if $n \geq \sum_{i=1}^{r} e_i p_i$.*

Proof: This follows by induction on the number of orbits, using the fact that a transitive permutation group which is abelian acts regularly. ∎

LEMMA 2.2: *Let G be a poly-Σ group. Then we have:*

(i) $\mathrm{com}(\mathrm{soc}(G)) \geq \frac{4}{5}\,\mathrm{com}(G)$;

(ii) *if G admits a faithful permutation representation of degree n, then* $n \geq 4\,\mathrm{com}(G)$.

Proof: First we consider the special case when $\mathrm{sol}(G) \leq 1$. Burnside's famous pq-Theorem implies that the order of a non-abelian finite simple group is divisible by at least one prime $p \geq 5$. Since $G = \mathrm{soc}(G)$ is the direct product of $\mathrm{com}(G)$ many non-abelian finite simple groups, it contains a subgroup A which is the direct product of $\mathrm{com}(G)$ many cyclic groups, each of prime order at least five. If G embeds into $\mathrm{Sym}(n)$, so does A, and Lemma 2.1 shows that $n \geq 5\,\mathrm{com}(G)$. Now we are ready to consider the general case.

(i) For brevity write $r := \mathrm{sol}(G)$, and for every $i \in \{1, 2, \ldots, r\}$ put $k_i := \mathrm{com}(\mathrm{soc}_i(G)/\mathrm{soc}_{i-1}(G))$. If $r = 0$, write $k_1 := 0$ nonetheless. Suppose that $1 \leq i \leq r-1$. Then, by the remarks just before Lemma 2.1, the group $G/\mathrm{soc}_i(G)$ and thus $\mathrm{soc}_{i+1}(G)/\mathrm{soc}_i(G)$ embeds into $\mathrm{Sym}(k_i)$. The "special case" now yields $k_i \geq 5k_{i+1}$.

This implies

$$\mathrm{com}(\mathrm{soc}(G)) = k_1 \geq \frac{4}{5}\sum_{i=0}^{r-1} 5^{-i}k_1 \geq \frac{4}{5}\sum_{i=1}^{r} k_i = \frac{4}{5}\,\mathrm{com}(G).$$

(ii) Suppose that G and thus $\mathrm{soc}(G)$ admits a faithful permutation representation of degree n. By the "special case" and (i) we get

$$n \geq 5\,\mathrm{com}(\mathrm{soc}(G)) \geq 4\,\mathrm{com}(G). \qquad \blacksquare$$

As an immediate consequence of Lemma 2.2(i) we record

COROLLARY 2.3: *The socle length of a poly-Σ group G is at most* $1+\log_5 \mathrm{com}(G)$.

3. Generating poly-Σ groups

In this section we prove

PROPOSITION 3.1: *Let $C := 2/\log(\frac{5}{3})$. Then every non-trivial poly-Σ group G satisfies*

$$d(G) \leq C \log \mathrm{com}(G) + 2.$$

Note that $C = 2/\log(\frac{5}{3}) < 3$, so Proposition 1.1 follows. Apart from improvements upon the constant C one cannot hope to do much better. This is illustrated by

Example 3.2: Let $G = S \times \cdots \times S$ be a direct power of some non-abelian finite simple group S. Then we have

$$d(G) \geq \log_{|S|} \operatorname{com}(G) = (\log |S|)^{-1} \log \operatorname{com}(G).$$

Indeed, put $d := d(G)$ and $k := \operatorname{com}(G)$. Choose a minimal generating set $\{g_i |\ 1 \leq i \leq d\}$ for G, and for every $j \in \{1, 2, \ldots, k\}$ let $\pi_j \colon G \to S$ denote the projection onto the j-th factor of G. Then the tuples $(g_1\pi_j, g_2\pi_j, \ldots, g_d\pi_j)$, $1 \leq j \leq k$, are pairwise distinct. So we obtain the inequality $|S|^d \geq k$.

The sequence $d(G^k)$, $k \in \mathbb{N}$ — for any given (finite) group G — has been studied extensively by Wiegold and others. For instance, in [10] it is shown that for every $S \in \Sigma$ and $k \in \mathbb{N}$ one has $d(S^k) > \log_{|S|} k + \log_{|S|} |\operatorname{Aut}(S)|$.

Proof of Proposition 3.1: Let G be a non-trivial poly-Σ group. Note that $M := \operatorname{soc}(G) = N_1 \times \cdots \times N_r$, where N_i, $1 \leq i \leq r$, are the minimal normal subgroups of G. Choose $s \in \{1, 2, \ldots, r\}$ such that the normal subgroups

$$H_1 := N_1 \times \cdots \times N_{s-1}, \quad H_2 := N_s, \quad H_3 := N_{s+1} \times \cdots \times N_r \trianglelefteq G$$

satisfy

$$\operatorname{com}(H_1) \leq \operatorname{com}(M)/2 \quad \text{and} \quad \operatorname{com}(H_3) \leq \operatorname{com}(M)/2. \tag{3.1}$$

We distinguish two cases.

CASE 1: $\operatorname{com}(H_2) \leq \operatorname{com}(M)/2$. If $H_1H_2 = G$, then clearly we have $d(G/H_1H_2) \leq C \log \operatorname{com}(G)$. Otherwise induction on $\operatorname{com}(G)$ shows that

$$\begin{aligned} d(G/H_1H_2) &\leq C \log \operatorname{com}(G/H_1H_2) + 2 \\ &\leq C \log(\operatorname{com}(G) - \operatorname{com}(M)/2) + 2 \\ &\leq C \log(3 \operatorname{com}(G)/5) + 2 && \text{by Lemma 2.2(i)} \\ &= C \log \operatorname{com}(G) + C \log(3/5) + 2 \\ &= C \log \operatorname{com}(G) && \text{by definition of } C. \end{aligned}$$

Similarly, we obtain

$$d(G/H_2H_3) \leq C \log \operatorname{com}(G) \quad \text{and} \quad d(G/H_1H_3) \leq C \log \operatorname{com}(G).$$

Put $d := \lfloor C \log \operatorname{com}(G) \rfloor$. Then we find $g_1, \ldots, g_d \in G$ such that $G/M = \langle g_1M, \ldots, g_dM \rangle$. By [5, Satz 1], we find $h_{i1}, \ldots, h_{id} \in H_i$ for $i \in \{1, 2, 3\}$ such that

$$\begin{aligned} G/H_1H_2 &= \langle \overline{g_1h_{31}}, \ldots, \overline{g_dh_{3d}} \rangle, \\ G/H_2H_3 &= \langle \overline{g_1h_{11}}, \ldots, \overline{g_dh_{1d}} \rangle, \\ G/H_1H_3 &= \langle \overline{g_1h_{21}}, \ldots, \overline{g_dh_{2d}} \rangle. \end{aligned}$$

For every $i \in \{1, 2, \ldots, s\}$ choose $n_i \in N_i \setminus \{1\}$, and put

$$h_1^* := n_1 \cdots n_{s-1} \in H_1, \quad h_2^* := n_s \in H_2.$$

Now it suffices to show that the subgroup

$$U := \langle g_1 h_{11} h_{21} h_{31}, \ldots, g_d h_{1d} h_{2d} h_{3d}, h_1^*, h_2^* \rangle \leq G$$

is in fact equal to G. By construction, we certainly have $UH_1H_2 = UH_2H_3 = UH_1H_3 = G$. So it is enough to show that $H_1H_2 \subseteq U$, equivalently that $N_i \subseteq U$ for all $i \in \{1, 2, \ldots, s\}$.

Suppose that $i \in \{1, 2, \ldots, s-1\}$, and choose $m_i \in N_i$ such that $[n_i, m_i] \neq 1$. Since $UH_2H_3 = G$, we find $h \in H_2H_3 = C_M(H_1)$ such that $m_i h \in U$. Then we have $[n_i, m_i] = [h_1^*, m_i h] \in U$, hence

$$N_i = \langle [n_i, m_i] \rangle^G = \langle [n_i, m_i] \rangle^{UH_2H_3} = \langle [n_i, m_i] \rangle^U \subseteq U.$$

Similarly, one shows that $N_s \subseteq U$. This finishes the proof in Case 1.

CASE 2: $\mathrm{com}(H_2) > \mathrm{com}(M)/2$. Write $N := H_2$. If $N = G$, then obviously we have $d(G/N) \leq C \log \mathrm{com}(G)$. Otherwise induction on $\mathrm{com}(G)$ shows that

$$\begin{aligned} d(G/N) &\leq C \log \mathrm{com}(G/N) + 2 \\ &\leq C \log(\mathrm{com}(G) - \mathrm{com}(M)/2) + 2 \\ &\leq C \log(3\,\mathrm{com}(G)/5) + 2 && \text{by Lemma 2.2(i)} \\ &= C \log \mathrm{com}(G) + C \log(3/5) + 2 \\ &= C \log \mathrm{com}(G) && \text{by definition of } C. \end{aligned}$$

Put $d := \lfloor C \log \mathrm{com}(G) \rfloor$. Then we find $g_1, \ldots, g_d \in G$ such that $G/N = \langle g_1 N, \ldots, g_d N \rangle$. Writing $k := \mathrm{com}(N)$, we have $N = S_1 \times \cdots \times S_k$, a direct product of non-abelian simple groups. Moreover, conjugation induces a transitive action of G/N on $\{S_1, \ldots, S_k\}$. According to CFSG, every finite simple group is two-generated. Choose generators h_1, h_2 for S_1. Then $G = \langle g_1, \ldots, g_d, h_1, h_2 \rangle$, and $d(G) \leq C \log \mathrm{com}(G) + 2$ as claimed. ∎

4. Normal subgroups of poly-Σ groups

The number of normal subgroups of a poly-Σ group is very restricted.

LEMMA 4.1: *Let G be a poly-Σ group, and put $k := \mathrm{com}(G)$. Let $n \in \{0, 1, \ldots, k\}$. Then the number of normal subgroups $N \trianglelefteq G$ with $\mathrm{com}(N) = n$ is at most $\binom{k}{n}$.*

This bound is sharp. Indeed, we have

Example 4.2: If $G = S^k$ is the direct k-th power of a non-abelian finite simple group S, then the number of normal subgroups $N \trianglelefteq G$ with $\mathrm{com}(N) = n$ is precisely $\binom{k}{n}$.

Proof of Lemma 4.1: If G is trivial, there is nothing to prove. So suppose that $G \neq 1$. Let $M \trianglelefteq_{\mathrm{min}} G$ be a minimal normal subgroup, and write $m := \mathrm{com}(M)$. If $N \trianglelefteq G$, then either (i) $N \supseteq M$ or (ii) $[N, M] = 1$, i.e., $N \subseteq C_G(M) \trianglelefteq G$. Note that both G/M and $C_G(M)$ are poly-Σ groups. Moreover, we have $\mathrm{com}(G/M) = k - m$ and $\mathrm{com}(C_G(M)) \leq k - m$; the latter inequality follows from $C_G(M) \cap M = Z(M) = 1$.

By induction, we know that there are at most $\binom{k-m}{n-m}$ subgroups N with $M \leq N \trianglelefteq G$ and $\mathrm{com}(N) = n$. Similarly, there are at most $\binom{k-m}{n}$ subgroups N with $N \trianglelefteq G$, $N \leq C_G(M)$ and $\mathrm{com}(N) = n$.

So altogether there are at most

$$\binom{k-m}{n-m} + \binom{k-m}{n} \leq \binom{k-1}{n-1} + \binom{k-1}{n} = \binom{k}{n}$$

normal subgroups $N \trianglelefteq G$ with $\mathrm{com}(N) = n$. ∎

For completeness we also state

PROPOSITION 4.3: *Let G be a poly-Σ group. Then there exists $g \in G$ such that $G = \langle g \rangle^G$.*

Proof: For $G = 1$ the claim is trivial; so assume that $G \neq 1$. Let $M \trianglelefteq_{\mathrm{min}} G$ be a minimal normal subgroup. Then M is the direct power of a non-abelian simple group, in particular $Z(M) = 1$.

By induction we find $g_1 \in G$ such that $G = \langle g_1 \rangle^G M$. If $[M, g_1] \neq 1$, then $M \subseteq \langle g_1 \rangle^G$; we are done. So suppose that $[M, g_1] = 1$. Choose any $g \in M \setminus \{1\}$ and put $g_2 := g_1 g$. Then $G = \langle g_2 \rangle^G M$ and $[M, g_2] \neq 1$, so as before $M \subseteq \langle g_2 \rangle^G$, and $\langle g_2 \rangle^G = G$. ∎

5. Permutation representations of poly-Σ groups

In this section we bound the number of permutation representations of a poly-Σ group. To render the text more readable we sometimes omit terms like "up to isomorphism" or "up to equivalence". Our first observation is that Proposition 1.2 readily follows from

PROPOSITION 5.1: *There exists $C \in \mathbb{R}_{>1}$ such that for all $n \in \mathbb{N}$ every non-trivial poly-Σ group G admits (up to equivalence) at most $C^{n(\log \mathrm{com}(G)+\log n)}$ transitive permutation representations of degree n. In fact, one may take $C = 2^{23}$.*

Proposition 5.1 implies Proposition 1.2: Choose $C_{\mathrm{tr}} \in \mathbb{R}_{>1}$ such that for all $n \in \mathbb{N}$ every non-trivial poly-Σ group G admits at most $C_{\mathrm{tr}}^{n(\log \mathrm{com}(G)+\log n)}$ transitive permutation representations of degree n, and put $C := 2C_{\mathrm{tr}}$.

Let G be a non-trivial poly-Σ group and $n \in \mathbb{N}$. Up to rearrangement of letters, a choice of orbits for a representation $G \to \mathrm{Sym}(n)$ corresponds to an additive partition of n. Clearly, n has less than 2^{n-1} such partitions, and if $n = n_1 + \cdots + n_r$ then $\sum_{i=1}^{r} n_i \log n_i \leq n \log n$. This shows that G has at most

$$\sum_{\substack{\text{all partitions} \\ n_1+\cdots+n_r=n}} \prod_{i=1}^{r} C_{\mathrm{tr}}^{n_i(\log \mathrm{com}(G)+\log n_i)} \leq C^{n(\log \mathrm{com}(G)+\log n)}$$

permutation representations of degree n. ∎

Next we state a technical lemma whose verification is a matter of routine and hence omitted.

LEMMA 5.2: *Let $n \in \mathbb{N}_{\geq 5}$, and $C \in \mathbb{R}_{\geq 4}$. Put $\lambda := \log_C(2)$. Then the functions $f_1, f_2 \colon [2, n/2] \to \mathbb{R}$ defined by*

$$f_1(x) := \frac{n}{x} + x + \lambda x + 3\lambda x \log \frac{n}{x} \quad \text{and} \quad f_2(x) := \frac{n}{x} + x + 2\lambda x + \lambda$$

satisfy the following properties.

(1) *Both f_1 and f_2 take their global maximum at $x_{\max} := n/2$.*
(2) *If $C \geq 2^{20}$ then $f_1(x_{\max}) \leq n$ and $f_2(x_{\max}) \leq n - \lambda$.*

With this we are ready to embark upon the

Proof of Proposition 5.1: We show that $C := 2^{23}$ is large enough. The proof is divided into three steps, the last being the most complicated.

STEP 1: *Reduction to faithful representations.* Let G be a non-trivial poly-Σ group and $n \in \mathbb{N}$. If $\mathrm{com}(G) = 1$, then G is simple and has precisely two

normal subgroups. Now suppose that $\mathrm{com}(G) \geq 2$. We claim that G has at most $2^{n \log \mathrm{com}(G)}$ normal subgroups $N \trianglelefteq G$ such that $G/N \hookrightarrow \mathrm{Sym}(n)$. If $\varphi\colon G \to \mathrm{Sym}(n)$ is a permutation representation with kernel $N := \ker(\varphi)$, then Lemma 2.2(ii) shows that $n \geq 4\,\mathrm{com}(G/N)$. By Lemma 4.1 the group G has no more than

$$\sum_{j=0}^{\lfloor n/4 \rfloor} \binom{\mathrm{com}(G)}{j} \leq \sum_{j=0}^{\lfloor n/4 \rfloor} \mathrm{com}(G)^j \leq \mathrm{com}(G)^n = 2^{n \log \mathrm{com}(G)}$$

normal subgroups $N \trianglelefteq G$ such that $\mathrm{com}(G/N) \leq n/4$. This yields the desired bound and shows that, writing $C_{\mathrm{fa}} := C/2 = 2^{22}$, it suffices to justify the following

CLAIM: *For all $n \in \mathbb{N}$ every non-trivial poly-Σ group G admits (up to equivalence) at most $C_{\mathrm{fa}}^{n(\log \mathrm{com}(G) + \log n)}$ faithful transitive permutation representations of degree n.*

Put $C_{\mathrm{ch}} := C/8 = 2^{20}$; the meaning of the subscript-notation will become clear later. For more flexibility it is convenient to continue the argument with reference to $C_0 \in \{C_{\mathrm{ch}}, C_{\mathrm{fa}}\}$.

STEP 2: *The case when G is simple.* Let $G \in \Sigma$ and $n \in \mathbb{N}$. Then G is two-generated by CFSG, and clearly $|\mathrm{Sym}(n)| \leq n^n$. So there are at most $4^{n \log n}$ homomorphisms from G to $\mathrm{Sym}(n)$. As $C_0 \geq 4$, we are okay.

STEP 3: *The case when G is not simple.* Let G be a poly-Σ group with $\mathrm{com}(G) \geq 2$, and let $n \in \mathbb{N}$. Choose a minimal normal subgroup $N \trianglelefteq_{\min} G$, and put $H := G/N$. Put $d := d(H)$, and choose $h_1, \ldots, h_d \in G$ such that $G = \langle h_1, \ldots, h_d \rangle N$. By Proposition 1.1 we have $d \leq 3 \log \mathrm{com}(H) + 2$.

Suppose that $\varphi\colon G \to \mathrm{Sym}(n)$ is a faithful transitive permutation representation; in particular, this presumes that $n \geq 5$. Then the G-space $\Omega := \{1, 2, \ldots, n\}$ falls into r separate N-orbits $\Omega_1, \ldots, \Omega_r$, say. They form a system of blocks for φ: the N-spaces $\Omega_1, \ldots, \Omega_r$ are pairwise isomorphic, and they are permuted transitively by the induced H-action. In particular, r divides n, and since N is non-trivial and acts faithfully on Ω, we have $1 \leq r \leq n/2$.

To recognise the action φ of G on Ω **up to equivalence**, it is enough to know

- the number r of N-orbits on Ω — there are no more than n possibilities;
  - *at this point we may assume without extra-cost that we also know the partition of Ω into N-orbits $\Omega_1, \ldots, \Omega_r$, and for each $i \in \{1, 2, \ldots, r\}$ we may choose a reference point $\alpha_i \in \Omega_i$;*

- the action of N on one (and hence, after rearrangement, on all) of its orbits — by induction (on the composition length) there are no more than $C_0^{(n/r)(\log \mathrm{com}(N)+\log(n/r))}$ possibilities;

- the induced action φ_H of H on $\{\Omega_1, \ldots, \Omega_r\}$ — this need not be faithful, but based upon our considerations in Steps 1 and 2 induction (on the composition length) shows that there are at most $2^{r \log \mathrm{com}(H)} C_0^{r(\log \mathrm{com}(H)+\log r)}$ possibilities;

- finally, for all $i \in \{1, 2, \ldots, r\}$ and $j \in \{1, 2, \ldots, d\}$ the images $\alpha_i h_j \in \Omega_i \overline{h}_j$ of our reference points under the chosen generators for G modulo N — there are no more than $(n/r)^{rd}$ possibilities.

Indeed, suppose that we know all the data listed above. Then first of all, we know the induced action φ_N of N on Ω. Since $G = \langle h_1, \ldots, h_d \rangle N$, in order to recognise φ it is enough to know how $h_1, \ldots, h_d$ act on Ω. So let $j \in \{1, 2, \ldots, d\}$ and $\omega \in \Omega$. Then $\omega \in \Omega_i$ for some $i \in \{1, 2, \ldots, r\}$. Because we know φ_N, we find $g \in N$ such that $\alpha_i g = \omega$, and we also know the action of $h_j^{-1} g h_j \in N$ on Ω. Since $\alpha_i h_j$ is given, we can successfully compute $\omega h_j = \alpha_i h_j (h_j^{-1} g h_j)$.

Unfortunately, the estimates given above are not quite sufficient to deal with the situation $r = 1$, i.e., when N acts transitively. To resolve this problem, we first condsider faithful transitive representations $G \to \mathrm{Sym}(n)$ with N acting intransitively, then with N acting transitively. In each case the number of representations is bounded by $\frac{1}{2} C_{\mathrm{fa}}^{n(\log \mathrm{com}(G)+\log n)}$; this will finish the overall proof.

CASE 1: *N acts intransitively.* Then the range of r is restricted by $2 \leq r \leq n/2$. Put $\lambda := \log_{C_0}(2)$. Then multiplying all the estimates given above, we find that the number of faithful transitive representations $G \to \mathrm{Sym}(n)$ with N acting intransitively is bounded above by $C_0^{f(n)}$, where

$$f(n) := \max_{2 \leq r \leq n/2} \; [\lambda \log n] + \left[\frac{n}{r}\left(\log \mathrm{com}(N) + \log \frac{n}{r}\right)\right] + [\lambda r \log \mathrm{com}(H) + r(\log \mathrm{com}(H) + \log r)] + \left[\lambda r d \log \frac{n}{r}\right].$$

Recall that $d \leq 3\log \mathrm{com}(H) + 2$. With Lemma 5.2 we obtain

$$\begin{aligned} f(n) &\leq \max_{2\leq r\leq n/2} \left\lfloor \frac{n}{r}\log \mathrm{com}(N) + \left(1+\lambda+3\lambda\log\frac{n}{r}\right) r\log \mathrm{com}(H)\right\rfloor \\ &\quad + \left\lfloor \lambda\log n + \frac{n}{r}\log\frac{n}{r} + r\log r + 2\lambda r\log\frac{n}{r}\right\rfloor \\ &\leq \max_{2\leq r\leq n/2} \left\lfloor \frac{n}{r} + r + \lambda r + 3\lambda r\log\frac{n}{r}\right\rfloor \log \mathrm{com}(G) \\ &\quad + \left\lfloor \frac{n}{r} + r + 2\lambda r + \lambda\right\rfloor \log n \\ &\leq n\log \mathrm{com}(G) + (n-\lambda)\log n \\ &\leq -\lambda + n(\log \mathrm{com}(G) + \log n), \end{aligned}$$

as wanted.

CASE 2: *N acts transitively.* First we finish the overall proof in the special case where G is characteristically simple, that is when $G \cong S^k$ for suitable $S \in \Sigma$ and $k \in \mathbb{N}$. This is quite easy. Read all previous occurrences of C_0 as C_{ch}, and suppose that $G \cong S^k$ with $S \in \Sigma$ and $k \in \mathbb{N}$. Since N is a minimal normal subgroup, we have $N \cong S$, $C_G(N) \cong S^{k-1}$, and $G = N \times C_G(N)$. Since N acts transitively, its centraliser $C_G(N)$ acts semi-regularly. This implies $|C_G(N)| \leq n \leq |N|$, and since $N \neq G$, we must have $C_G(N) \cong N$. Thus $\mathrm{com}(G) = 2$. By CFSG the group G is four-generated, and there are at most $16^{n\log n}$ homomorphisms from G to $\mathrm{Sym}(n)$; cf. Step 2. Since $16^{n\log n} \leq \frac{1}{2}C_{\mathrm{ch}}^{n(\log \mathrm{com}(G)+\log n)}$, we are okay.

We have shown: *for all $n \in \mathbb{N}$ every non-trivial characteristically simple poly-Σ group G admits at most $C_{\mathrm{ch}}^{n(\log \mathrm{com}(G)+\log n)}$ faithful transitive permutation representations of degree n, up to equivalence.*

Finally, we return to the general case. Read all occurrences of C_0 prior to the beginning of Case 2 as C_{fa}, and recall the general set-up introduced before the argument divided into cases. Since N is a minimal normal subgroup of G, it is characteristically simple. Since N acts transitively on Ω, we have $r = 1$ and the action of H on $\{\Omega_1\}$ is necessarily trivial. To recognise the action of G on Ω *up to equivalence*, it is therefore enough to know

- the action of N on Ω — we just proved that there are no more than $C_{\mathrm{ch}}^{n(\log \mathrm{com}(N)+\log n)}$ possibilities;
- for each $j \in \{1, 2, \ldots, d\}$ the image $\alpha_1 h_j$ of the single reference point α_1 under h_j — there are at most n^d possibilities.

Write $\lambda := \log_{C_{\mathrm{fa}}}(2) = 1/22$ and $\mu := \log_{C_{\mathrm{fa}}}(C_{\mathrm{ch}}) = 20/22$. As $n \geq 5$, we have $\log n \leq n/2$ and thus

$$\mu n + 3\lambda\log n \leq 20\lambda n + \frac{3}{2}\lambda n \leq n. \tag{5.1}$$

Multiplying the estimates given above, we find that the number of faithful transitive representations $G \to \mathrm{Sym}(n)$ with N acting transitively is bounded above by $C_{\mathrm{fa}}^{f(n)}$, where

$$f(n) := [\mu n(\log \mathrm{com}(N) + \log n)] + [\lambda d \log n].$$

Recall that $d \leq 3 \log \mathrm{com}(H) + 2$. With the inequality (5.1) we obtain

$$\begin{aligned} f(n) &\leq [\mu n \log \mathrm{com}(N) + 3\lambda \log n \log \mathrm{com}(H)] + [(\mu n + 2\lambda) \log n] \\ &\leq (\mu n + 3\lambda \log n) \log \mathrm{com}(G) + (\mu n + 2\lambda) \log n \\ &\leq n \log \mathrm{com}(G) + (n - \lambda) \log n \\ &\leq -\lambda + n(\log \mathrm{com}(G) + \log n). \end{aligned}$$

As indicated just before Case 1, this finishes the overall proof. ∎

We note that Corollary 1.3 follows immediately from Proposition 1.2 and Lemma 2.2(ii).

6. Enumerating poly-Σ groups: an upper bound

This section is entirely devoted to the proof of the upper bound in Theorem A: we claim that

$$\mathbf{g}_\Sigma(n) \leq n^{53 \log \log n} \quad \text{for all } n \in \mathbb{N}.^*$$

As in the previous section we freely omit the expressions "up to isomorphism" or "up to equivalence" where adequate.

Let $n \in \mathbb{N}$. If $n < 60$, then $\mathbf{g}_\Sigma(n) = 1$. Hence let us assume that $n \geq 60$. Although we make no attempt to optimise the constants in our bounds, we are going to compute everything quite explicitly; for this purpose we record the following basic estimates. For every poly-Σ group G with $|G| \leq n$ we have

$$\begin{aligned} &\mathrm{com}(G) \leq \log_{60} n \leq \frac{1}{5} \log n, \\ &\mathrm{sol}(G) \leq 1 + \log_5 \mathrm{com}(G) \leq \frac{1}{2} \log \log n \quad \text{(by Corollary 2.3)}, \\ &d(G) \leq 3 \log \mathrm{com}(G) + 2 \leq 3 \log \log n \quad \text{(by Proposition 1.1)}. \end{aligned} \tag{6.1}$$

Next we introduce the notion of "socle type", in addition to the basic definitions given already in Section 2. A finite **socle type** is just a tuple of finite groups each of which has socle length one. Note that a finite group has socle length one

* For $n = 1$ the reader should interpret $n^{53 \log \log n}$ as $\lim_{x \to 1^+} x^{53 \log \log x} = 1$.

if and only if it is a non-trivial direct product of finite simple groups. Let G be a finite group and $\mathbf{M} = (M_1, \ldots, M_r)$ a finite socle type. The group G **realizes** $\mathbf{M}$, if $\mathrm{sol}(G) = r$ and for all $i \in \{1, 2, \ldots, r\}$ we have $\mathrm{soc}_i(G)/\mathrm{soc}_{i-1}(G) \cong M_i$. If each component of $\mathbf{M}$ is poly-Σ, we say that $\mathbf{M}$ is poly-Σ. So, if G realizes $\mathbf{M}$, either both are poly-Σ or none of them. The **total order** of $\mathbf{M}$ is the product $\prod_{i=1}^{r} |M_i|$ of the orders of its components. Thus, if G realizes $\mathbf{M}$, the order of G equals the total order of $\mathbf{M}$.

Now, returning to the proof of our claim, we divide the argument into

STEP 1: the number of poly-Σ socle types of total order at most n which can be realized by suitable poly-Σ groups is no more than $n^{(3/2)\log\log n}$;

STEP 2: any particular poly-Σ socle type of total order at most n is realized by no more than $n^{51\log\log n}$ poly-Σ groups.

This will certainly imply $\mathbf{g}_\Sigma(n) \leq n^{53\log\log n}$, as wanted.

STEP 1: The socle length of a poly-Σ group of order at most n is bounded by $\frac{1}{2}\log\log n$; see (6.1). So we only have to consider socle types up to that length. According to [12, Lemma 2.3], the number of poly-Σ groups of socle length one and order at most n is less than or equal to n^3. Thus no more than $n^{(3/2)\log\log n}$ poly-Σ socle types of total order at most n are actually realized.

STEP 2: Fix a poly-Σ socle type $\mathbf{M} = (M_1, \ldots, M_r)$ of total order $\tilde{n} \leq n$. If $\tilde{n} = 1$, only the trivial group realizes $\mathbf{M}$. So let us assume that $\tilde{n} > 1$, and write $M := M_1$. Note that $m := |M| \neq 1$ divides $\tilde{n}$.

Suppose that G is a poly-Σ group realizing $\mathbf{M}$. Then $M \cong \mathrm{soc}(G)$ is the direct product of non-abelian simple groups, say

$$M \cong S_1^{k_1} \times \cdots \times S_s^{k_s}, \quad S_i \in \Sigma \text{ for } i \in \{1, 2, \ldots, s\},$$

where $S_i \cong S_j$ if and only if $i = j$. The factor group $H := G/M$ is again poly-Σ and realizes the socle type $(M_2, \ldots, M_r)$ of total order $|H| = \tilde{n}/m < \tilde{n}$. We can view G as an extension of M by H, and conjugation in G induces a coupling homomorphism $\chi\colon H \to \mathrm{Out}(M)$. Clearly, M has trivial centre, and so by [14, §11.4.21] the extension $1 \to M \to G \to H \to 1$ is determined up to equivalence by

(1) the isomorphism class of $M \cong M_1$,

(2) the isomorphism class of H,

(3) the coupling homomorphism $\chi\colon H \to \mathrm{Out}(M)$.

Of course, the same data then determine the group G up to isomorphism.

So we can bound the number of poly-Σ groups realizing $\mathbf{M}$ by estimating the number of possible choices in (2) and (3). By induction the number of poly-Σ groups H realizing the socle type $(M_2, \ldots, M_r)$ is at most $(n/m)^{51 \log\log(n/m)}$.

Now suppose that such a group H is fixed; it remains to estimate the number of possible homomorphisms $\chi\colon H \to \mathrm{Out}(M)$ as in (3). In Section 2 we saw that $\mathrm{Out}(M) = T \ltimes B$, where $T \cong \prod_{i=1}^{s} \mathrm{Sym}(k_i)$ and $B \cong \prod_{i=1}^{s} \mathrm{Out}(S_i)^{k_i}$. So every homomorphism $\chi\colon H \to \mathrm{Out}(M)$ induces a permutation representation $\overline{\chi}\colon H \to T \cong \prod_{i=1}^{s} \mathrm{Sym}(k_i)$. Clearly, it suffices to bound

(3a) the number of actions $\overline{\chi}\colon H \to \prod_{i=1}^{s} \mathrm{Sym}(k_i)$, up to equivalence in each factor,

(3b) for every permutation representation $\overline{\chi}$ as in (3a), the number of liftings $\chi\colon H \to \mathrm{Out}(M)$.

If $m = \tilde{n}$ and consequently $H = 1$, all estimates become trivial. So assume that $m < \tilde{n}$. Since $\sum_{i=1}^{s} k_i \leq \log m$, Proposition 1.2 together with (6.1) shows that the number of representations as in (3a) is bounded above by

$$2^{24(\log m)(\log\log(\tilde{n}/m)+\log\log m)} \leq m^{24(\log\log(n/m)+\log\log m)}.$$

The number of liftings as in (3b) is at most $|B|^{d(H)}$. By CFSG every finite simple group S is two-generated, so $|\mathrm{Aut}(S)| \leq |S|^2$ and $|\mathrm{Out}(S)| \leq |S|$. Thus $|B| \leq |M| = m$, and (6.1) shows that $d(H) \leq 3 \log\log(\tilde{n}/m)$. So the number of liftings as in (3b) is at most $m^{3 \log\log(n/m)}$.

Combining our estimates, we find that the number of poly-Σ groups realizing $\mathbf{M}$ is at most

$$(n/m)^{51 \log\log(n/m)} \cdot m^{24(\log\log(n/m)+\log\log m)} \cdot m^{3 \log\log(n/m)} \leq n^{51 \log\log n}.$$

This finishes Step 2 and the overall proof.

7. Enumerating poly-S groups: a lower bound

Throughout this section let $S \in \Sigma$. In the following context, it is convenient to regard an **action** of a group G on some set Ω as a map $\Phi\colon \Omega \times G \to \Omega$ corresponding to a homomorphism $\varphi\colon G \to \mathrm{Sym}(\Omega)$. Two actions $\Phi_1\colon \Omega_1 \times G_1 \to \Omega_1$ and $\Phi_2\colon \Omega_2 \times G_2 \to \Omega_2$ are said to be **isomorphic** if there exist a bijection $\sigma\colon \Omega_1 \to \Omega_2$ and a group isomorphism $\iota\colon G_1 \to G_2$ such that the diagram

$$\begin{array}{ccc} \Omega_1 \times G_1 & \xrightarrow{\Phi_1} & \Omega_1 \\ \downarrow{\scriptstyle (\sigma,\iota)} & & \downarrow{\scriptstyle \sigma} \\ \Omega_2 \times G_2 & \xrightarrow[\Phi_2]{} & \Omega_2 \end{array}$$

commutes.

For any permutation action $\Phi\colon \Omega \times H \to \Omega$ of a poly-S group H on some finite set Ω we define the permutational wreath product

$$G_\Phi := S \wr_\Phi H = H \ltimes \prod_{\omega \in \Omega} S_\omega,$$

where $S_\omega \cong S$ for all $\omega \in \Omega$ and H permutes the various factors according to Φ. The next lemma is easily checked.

LEMMA 7.1: (1) *If $\Phi\colon \Omega \times H \to \Omega$ describes a faithful permutation action of a poly-S group H on some set Ω, then G_Φ is a poly-S group of composition length* $\mathrm{com}(G_\Phi) = \mathrm{com}(H) + |\Omega|$ *and* $\mathrm{soc}(G_\Phi) = \prod_{\omega \in \Omega} S_\omega$.

(2) *If $\Phi_1\colon \Omega_1 \times H_1 \to \Omega_1$ and $\Phi_2\colon \Omega_2 \times H_2 \to \Omega_2$ are faithful permutation actions of poly-S groups H_1 and H_2, then G_{Φ_1} is isomorphic to G_{Φ_2} if and only if Φ_1 is isomorphic to Φ_2.*

The problem of constructing a sufficient number of poly-S groups with prescribed composition length thus reduces to the problem of constructing faithful permutation actions. We show

LEMMA 7.2: *There exists $d \in \mathbb{N}$ (depending on S) such that for every $k \in \mathbb{N}$ the group $H = S^{k+1}$ has at least k^k pairwise non-isomorphic faithful permutation actions on dk points.*

Proof: Since $S \in \Sigma$, we can fix faithful transitive permutation actions of S on Ω_1, Ω_2 and Ω_3, say, such that $|\Omega_1| < |\Omega_2| < |\Omega_3|$. We put $d_i := |\Omega_i|$ for $i \in \{1, 2, 3\}$, and $d := (d_1 + d_2)d_3$.

Write $H = H_0 \times \cdots \times H_k$ as a product of its minimal normal subgroups $H_n \cong S$, $0 \leq n \leq k$. For every $n \in \{0, 1, \ldots, k\}$ fix transitive permutation actions of H_n on Ω_1, Ω_2 and Ω_3 respectively.

For every $j \in \{1, 2, \ldots, k\}$ define

$$\Gamma_j^{(1)} := \{(1, j, \omega_1, \omega_3) |\ \omega_1 \in \Omega_1, \omega_3 \in \Omega_3\},$$
$$\Gamma_j^{(2)} := \{(2, j, \omega_2, \omega_3) |\ \omega_2 \in \Omega_2, \omega_3 \in \Omega_3\},$$

and put $\Gamma := \bigcup \{\Gamma_j^{(1)} \cup \Gamma_j^{(2)} |\ 1 \leq j \leq k\}$. Note that Γ has cardinality dk.

For every k-tuple $\pi \in \{1, 2, \ldots, k\}^k$ we are going to define a faithful permutation action Φ_π of H on Γ; then we will show that these permutation actions are pairwise non-isomorphic.

Let $\pi \in \{1,2,\ldots,k\}^k$, and define $\bar{\pi} \in \{0,1,\ldots,k\}^k$ as follows:

$$\bar{\pi}(j) := \begin{cases} \pi(j) & \text{if } \pi(j) \neq j, \\ 0 & \text{if } \pi(j) = j. \end{cases}$$

Clearly, if $\rho \in \{1,2,\ldots,k\}^k$ with $\bar{\rho} = \bar{\pi}$, then $\rho = \pi$.

For every $n \in \{0,1,\ldots,k\}$ we now define a non-trivial action of H_n on Γ; it is easily checked that these actions mutually commute and thus induce a faithful action $\Phi_\pi \colon \Gamma \times H \to \Gamma$.

Let $n \in \{0,1,\ldots,k\}$, and let $h \in H_n$. For every $j \in \{1,2,\ldots,k\}$ and all $\omega_i \in \Omega_i$, $i \in \{1,2,3\}$, define

$$(1,j,\omega_1,\omega_3)^h := \begin{cases} (1,j,\omega_1,\omega_3) & \text{if } j \neq n \text{ and } \bar{\pi}(j) \neq n, \\ (1,j,\omega_1^h,\omega_3) & \text{if } \bar{\pi}(j) = n, \\ (1,j,\omega_1,\omega_3^h) & \text{if } j = n, \end{cases}$$

$$(2,j,\omega_2,\omega_3)^h := \begin{cases} (2,j,\omega_2,\omega_3) & \text{if } j \neq n \text{ and } j \neq n+1, \\ (2,j,\omega_2^h,\omega_3) & \text{if } j = n+1, \\ (2,j,\omega_2,\omega_3^h) & \text{if } j = n. \end{cases}$$

For later use we remark that Φ_π has $2k$ orbits on Γ: there are k orbits of size $d_1 d_3$, namely $\Gamma_j^{(1)}$, $1 \leq j \leq k$, and k orbits of size $d_2 d_3$, namely $\Gamma_j^{(2)}$, $1 \leq j \leq k$. Moreover, we make the following

OBSERVATION: *For all $n \in \{0,1,\ldots,k\}$ and $j \in \{1,2,\ldots,k\}$ we have*

$$\bar{\pi}(j) = n \quad \leftrightarrow \quad j \neq n \text{ and } H_n \text{ acts non-tivially on } \Gamma_j^{(1)} \text{ under } \Phi_\pi.$$

It remains to show that the actions defined are pairwise non-isomorphic. So let $\pi, \rho \in \{1,2,\ldots,k\}^k$, and suppose that $(\sigma,\iota) \in \mathrm{Sym}(\Gamma) \times \mathrm{Aut}(H)$ is an isomorphism from Φ_π to Φ_ρ.

Then ι induces a permutation ι^* of $\{H_0, H_1, \ldots, H_k\}$, and σ induces permutations σ_1^* of $\{\Gamma_j^{(1)} \mid 1 \leq j \leq k\}$ and σ_2^* of $\{\Gamma_j^{(2)} \mid 1 \leq j \leq k\}$.

CLAIM: *All three permutations ι^*, σ_1^*, σ_2^* are in fact trivial.*

Subproof: In both actions, Φ_π and Φ_ρ, the only minimal normal subgroup of H which has no orbits of length d_3 is H_0; hence $H_0\iota^* = H_0$.

Now suppose that $j \in \{1,2,\ldots,k\}$ with $H_{j-1}\iota^* = H_{j-1}$. In both actions H_{j-1} has orbits of length d_2, and their union is $\Gamma_j^{(2)}$; thus $\Gamma_j^{(2)}\sigma_2^* = \Gamma_j^{(2)}$. In both actions, the only minimal normal subgroup of H which acts on $\Gamma_j^{(2)}$ with orbits of length d_3 is H_j; so $H_j\iota^* = H_j$. Finally, in both actions H_j has orbits of length d_3 outside $\Gamma_j^{(2)}$, and their union is $\Gamma_j^{(1)}$; thus $\Gamma_j^{(1)}\sigma_1^* = \Gamma_j^{(1)}$. The claim now follows by induction.

The Claim and the Observation show that $\bar{\pi} = \bar{\rho}$, and hence $\pi = \rho$, as required. ∎

Proof of the lower bound in Theorem B: We want to find $B \in \mathbb{R}_{>0}$ such that for all $k \in \mathbb{N}$,

$$\widehat{\mathbf{g}}_S(k) \geq k^{Bk}.$$

Lemmata 7.1 and 7.2 yield $d \in \mathbb{N}$ such that for every $k \in \mathbb{N}$ we have $\widehat{\mathbf{g}}_S(dk + k + 1) \geq k^k$. This and the fact that $\widehat{\mathbf{g}}_S$ is a non-decreasing function are enough to verify our claim.

Indeed, choose $B_1 \in \mathbb{R}_{>0}$ such that for all $k \in \{1, 2, \ldots, 2(d+1)\}$ we have $\widehat{\mathbf{g}}_S(k) \geq k^{B_1 k}$. Next put $B_2 := \log(d+1)/2(\log(2(d+1))$. Then for every $k \in \mathbb{N}$ with $k > 2(d+1)$ we get

$$\frac{k-d-1}{k} \cdot \frac{\log(k-d-1)}{\log k} > B_2,$$

and so

$$\widehat{\mathbf{g}}_S(k) \geq (k-d-1)^{k-d-1} = 2^{(k-d-1)\log(k-d-1)} \geq 2^{B_2 k \log k} = k^{B_2 k}.$$

Thus $B := \min\{B_1, B_2\}$ does the trick. ∎

ACKNOWLEDGEMENT: My thanks go to Alex Lubotzky, who conjectured freely about the number of poly-S groups in one of his lectures, and Yair Glasner, who happily discussed the problem with me afterwards on several occasions. I am also grateful to Avinoam Mann and Dan Segal for helpful comments on an earlier version of this paper.

References

[1] R. Bercov, *On groups without abelian composition factors*, Journal of Algebra **5** (1967), 106–109.

[2] H. U. Besche, B. Eick and E. A. O'Brien, *A millennium project: constructing small groups*, International Journal of Algebra and Computation **12** (2000), 623–644.

[3] A. V. Borovik, L. Pyber and A. Shalev, *Maximal subgroups in finite and profinite groups*, Transactions of the American Mathematical Society **348** (1996), 3745–3761.

[4] A. R. Camina, G. R. Everest and T. M. Gagen, *Enumerating non-soluble groups — a conjecture of John G. Thompson*, The Bulletin of the London Mathematical Society **18** (1986), 265–268.

[5] W. Gaschütz, *Zu einem von B. H. und H. Neumann gestellten Problem*, Mathematische Nachrichten **14** (1956), 249–252.

[6] G. Higman, *Enumerating p-groups. I: Inequalities*, Proceedings of the London Mathematical Society **10** (1960), 24–30.

[7] D. F. Holt, *Enumerating perfect groups*, Journal of the London Mathematical Society **39** (1989), 67–78.

[8] O. Hölder, *Die Gruppen mit quadratfreier Ordungszahl*, Nachrichten von der Königlichen Gesellschaft der Wissenschaften in Göttingen. Mathematisch-Physikalische Klasse aus dem Jahre 1895, 211–229.

[9] A. McIver and P. M. Neumann, *Enumerating finite groups*, The Quarterly Journal of Mathematics. Oxford **38** (1987), 473–488.

[10] D. Meier and J. Wiegold, *Growth sequences of finite groups V*, Journal of the Australian Mathematical Society **31** (1981), 374–375.

[11] P. M. Neumann, *Enumeration theorem for finite groups*, The Quarterly Journal of Mathematics. Oxford **20** (1969), 395–401.

[12] L. Pyber, *Enumerating finite groups of given order*, Annals of Mathematics **137** (1993), 203–220.

[13] L. Pyber, *Group enumeration and where it leads us*, in *European Congress of Mathematics, Budapest, Hungary, July 22–26, 1996. Volume II* (A. Balog et al., eds.), Progress in Mathematics 169, Birkhäuser, Basel, 1998, pp. 187–199.

[14] D. J. S. Robinson, *A Course in the Theory of Groups*, Graduate Texts in Mathematics 80, Springer-Verlag, New York–Heidelberg–Berlin, 1982.

[15] C. C. Sims, *Enumerating p-groups*, Proceedings of the London Mathematical Society **15** (1965), 151–166.