ISRAEL JOURNAL OF MATHEMATICS **94** (1996), 7–19

VARIATIONS ON POLYNOMIAL SUBGROUP GROWTH

BY

DAN SEGAL

All Souls College, Oxford OX1 4AL, England
e-mail: dsegal@vax.ox.ac.uk

ABSTRACT

A group G has **weak polynomial subgroup growth (wPSG)** of degree $\leq \alpha$ if each finite quotient $\bar{G}$ of G contains at most $|\bar{G}|^\alpha$ subgroups. The main result is that wPSG of degree α implies polynomial subgroup growth (PSG) of degree at most $f(\alpha)$. It follows that wPSG is equivalent to PSG. A corollary is that if, in a profinite group G, the k-generator subgroups have positive "density" δ, then G is finitely generated (the number of generators being bounded by a function of k and δ).

1. Introduction

A group G has **polynomial subgroup growth** (PSG) of degree at most α if, for each n, the number $s_n(G)$ of subgroups of index $\leq n$ in G is bounded above by n^α. (If G is a profinite group, "subgroup" is taken to mean "closed subgroup".) Thus to say that G has PSG is to say that there are not very many subgroups whose distance from G is small, where our measure of distance is the index. In the context of profinite groups, it may be more natural to say that a subgroup H is close to G if H "appears" in a small finite quotient of G, in the sense that $H \geq N$ where N is an open normal subgroup and $|G/N|$ is small. This suggests a variant of our original definition:

Received January 16, 1995

Definition: The group G has **weak PSG** (wPSG) of degree at most α if for every finite quotient $\bar{G}$ of G, the total number of subgroups $s(\bar{G})$ of $\bar{G}$ satisfies

$$s(\bar{G}) \leq |\bar{G}|^{\alpha}.$$

It is obvious that PSG of degree α implies wPSG of degree at most α. At first sight, wPSG would seem to be a substantially weaker condition than PSG. However, on looking at the characterisation of finitely generated groups with PSG given in [LMS] (or in [DDMS], chapter 6), one sees that most of the major steps in the proof only use the weaker hypothesis; and it is not difficult to adjust the remaining steps (see the proofs of Proposition 1 and Lemma 3, below). Thus we have

THEOREM A: *The finitely generated residually finite groups with wPSG are precisely the finite extensions of finitely generated torsion-free soluble minimax groups.*

It follows that a finitely generated group has wPSG if and only if it has PSG. This conclusion depends on a substantial amount of infinite group theory; one is led to ask whether there is a more direct connection between wPSG and PSG. The answer is provided by our main result,

THEOREM B: *There is a function f such that every group (abstract or profinite) with wPSG of degree α has PSG of degree at most $f(\alpha)$.*

In recent work, Avinoam Mann has discovered a beautiful connection between the subgroup growth and the distribution of finite generating sets in profinite groups. Theorem 2 of [M1] shows that if a profinite group G has PSG of degree β, then G has a generating set of size at most $\beta + 3$. With Theorem B this gives

COROLLARY 1: *If a profinite group G has wPSG of degree α then $d(G) \leq f(\alpha) + 3$.*

(Here, $d(G)$ denotes the size of a minimal generating set for G as a profinite group.)

In [M2], Mann considers groups G in which the k-generator subgroups have **positive density**: that is, there exists $\delta > 0$ such that $s_n^{(k)}(G) \geq \delta s_n(G)$ for all n, where $s_n^{(k)}(G)$ denotes the number of k-generator subgroups of index at most n in G. In particular, Theorem 14 of [M2] states that if G is prosoluble and its k-generator subgroups have positive density, for some finite k, then G

has PSG. In the spirit of the present work, it is more natural to consider the density of **all** k-generator subgroups in finite quotients of a group G, irrespective of their index. Thus, writing $s^{(k)}(\bar{G})$ for the number of k-generator subgroups in a group $\bar{G}$, let us say that the k-generator subgroups have **positive profinite density** in a profinite group G if there exists $\delta > 0$ such that $s^{(k)}(\bar{G}) \geq \delta s(\bar{G})$ for every finite quotient $\bar{G}$ of G. The advantage of this new definition is that the connection with wPSG is immediate: since $s^{(k)}(\bar{G}) \leq |\bar{G}|^k$, we see that

$$s(\bar{G}) \leq \delta^{-1}|\bar{G}|^k \leq |\bar{G}|^\alpha,$$

where $\alpha = k + \log_2(\delta^{-1})$, provided $|\bar{G}| \geq 2$. Thus if G is profinite and, for some finite k, its k-generator subgroups have positive profinite density, then G has wPSG, and hence (by Theorem B) G has PSG. In particular, it follows that G itself is finitely generated.

In quantitative form, this argument yields a result which is significant even for finite groups:

COROLLARY 2: *There is a function d such that if G is a profinite group, k is a positive integer, and $0 < \delta \leq 1$, $0 < \lambda \leq 1$ satisfy $s^{(k)}(\bar{G}) \geq \delta s(\bar{G})^\lambda$ for every finite quotient $\bar{G}$ of G, then $d(G) \leq d(k, \delta, \lambda)$.*

In fact, the methods of [M2] show that for each $\varepsilon \in (0, 1)$, there exists a number $d_\varepsilon(k, \delta, \lambda)$ such that a random $d_\varepsilon(k, s, \lambda)$-tuple in G generates G with probability at least ε.

I shall say no more about the proof of Theorem A; in any case, it follows from [LMS] and Theorem B. It is easy to see that if Theorem B is true for finite groups, then it is true for all groups (with the same function f). For the rest of the paper, which is devoted to the proof of Theorem B, **all groups are finite.**

The theorem is deduced in Section 4 from four Propositions. Propositions 1 and 2, proved in Section 2, give detailed information about the structure of a (finite) group with wPSG of given degree (taking inverse limits, one can read off similar information about the structure of a profinite group with wPSG). In Section 3 we prove Proposition 3, which shows that the index $|G: \mathrm{core}_G(H)|$ is polynomially bounded in terms of $|G: H|$, for any group G with the specified structure and any subgroup H of G; and Proposition 4, which gives a polynomial bound for the normal subgroup growth of such a group.

NOTATION

$Z(G), G', F(G), R(G)$: the centre, derived group, Fitting subgroup and soluble radical of G.

$E(G)$: subgroup generated by the subnormal quasi-simple subgroups of G.

$\mathrm{soc}(G)$: the socle of G.

$\mathrm{Out}(G)$: the outer automorphism group of G.

$M(G)$: the Schur multiplier of G.

$\mathrm{core}_G(H)$: the biggest normal subgroup of G contained in H.

$\mu(G)$: the maximum multiplicity of any non-abelian composition factor of G.

$\sigma(G)$: the product of the orders of all non-abelian composition factors of G, counted with their multiplicities.

$d(G)$: size of a minimal generating set for G.

$\mathrm{rk}(G) = \max\{d(H) | H \leq G\}$.

$r_p(G) = \max\{d(H) | H \text{ is a } p\text{-subgroup of } G\}$.

$\log x = \log_2 x$.

The symbol $f(x, y, \ldots)$ denotes a function of the displayed arguments, not necessarily the same one each time. f_i, for $i = 1, 2, \ldots$, denote fixed functions.

2. Structural results

To state these, let us introduce some *ad hoc* notation: $\mathcal{X}(c)$ will denote the class of all simple groups of Lie type, over fields $\mathbb{F}_{p^e}$ with $e \leq c$, and of rank parameter at most c. A group G is in $\mathcal{Y}(c)$ if $G/R(G)$ is a direct product of groups in $\mathcal{X}(c)$.

The first result is a variation on Proposition 1.2 of [Sh2] (I am grateful to Aner Shalev for sending me an early draft of [Sh2]):

PROPOSITION 1: *If a group G has wPSG of degree α, then G has a normal subgroup G_0 such that*

$$|G: G_0| \leq f_1(\alpha), \quad \mu(G_0) \leq f_2(\alpha), \quad G_0 \in \mathcal{Y}(f_3(\alpha)).$$

The other main result of this section is

PROPOSITION 2: *Let $G \in \mathcal{Y}(c)$. If G has wPSG of degree β, then there exists $Y \leq Z(G)$ such that*

$$|Y| \leq |G: R(G)|^{f_4(c)}, \quad \mathrm{rk}(F(G)/Y) \leq f_5(c, \beta).$$

We shall need

LEMMA 1: *If G has wPSG of degree α and*

$$G(n) = \bigcap \{N \lhd G \mid |G: N| \,|n\},$$

then $|G: G(n)| \leq f(\alpha, n)$.

Proof: We may assume that $G(n) = 1$. Choose $K_1, ..., K_t \lhd G$ with $|G: K_i| \,|n$ for each i, so that $K_1 \cap \cdots \cap K_t = 1$ and t is minimal. Put $L_i = \bigcap_{j \neq i} K_j$. Then $1 \neq |L_i| \,|G: K_i| \,|n$. Suppose n is divisible by $\lambda = \lambda(n)$ distinct primes. Then for some prime p, we have $p \,|L_i|$ for at least $[t/\lambda]$ distinct values of i. Since the product $L_1 L_2 \cdots L_t$ is direct, it follows that G contains an elementary abelian p-subgroup of rank at least $[t/\lambda]$, hence contains at least $p^{([t/\lambda]-1)^2/4}$ distinct subgroups. Hence

$$p^{([t/\lambda]-1)^2/4} \leq s(G) \leq |G|^\alpha \leq n^{t\alpha}$$

so

$$([t/\lambda] - 1)^2 \leq 4t\alpha \log_p n \leq 4t\alpha \log n.$$

It follows that $t \leq f(\alpha, n)$ for some function f, and this gives the result since $|G| \leq n^t$.

Proof of Proposition 1: Suppose S is a non-abelian composition factor of G. Then G has a quotient $\bar{G}$ such that $\bar{G}$ has a normal subgroup $B \cong S^{(r)}$, for some r, and such that $C_{\bar{G}}(B) = 1$. By the Classification of Finite Simple Groups, S is (a) sporadic, (b) alternating of degree n, for some n, or (c) a Chevalley or twisted Chevalley group $X_n(p^e)$, for some n, e and prime p. Lemma 4.4 of [MS] shows that

$$|\bar{G}| \leq r! |S|^{2r}.$$

By Lemmas 4.3 and 4.2 of [MS], B contains an elementary abelian subgroup H of order p^d (for some prime p) where $d \geq cner$ (here c is an absolute positive constant, and we set $e = 1$, $n = 2$ in case (a), $e = 1$ in case (b)); and

$$|S|^r = |B| \leq p^{kd \log n}$$

where k is an absolute constant. Since H contains at least $p^{[d/2]^2}$ subgroups we have

$$p^{[d/2]^2} \leq s(\bar{G}) \leq |\bar{G}|^\alpha.$$

Combined with the above estimates this gives (crudely)

$$(d-1)^2 \leq 4\alpha d \log(c^{-1}d)(c^{-1}+2k).$$

It follows that d is bounded by a function of α, and hence that n, e and r are bounded above by an integer m depending only on α. In particular, in case (c) we have $S \in \mathcal{X}(m)$.

Now if $S \in \mathcal{X}(m)$ then $|\mathrm{Out}(S)| \leq 18m(m+1)$; see for example [C] Chapter 3, Table 5. Let g be the l.c.m. of the numbers

$$|\mathrm{Aut}(S)|,\ S \text{ sporadic or alternating of degree } \leq m;\ |\mathrm{Out}(S)|,\ S \in \mathcal{X}(m).$$

Then g is finite and depends only on m. Put

$$q = m!g^m,$$

and finally put

$$G_0 = G(q)$$

in the notation of Lemma 1. The lemma shows that $|G\colon G_0| \leq f_1(\alpha)$.

If B/A is a non-abelian chief factor of G, then B/A is a product of at most m simple groups like S, above, and these are permuted by G. Hence they are normalised by G_0; also if S is of type (a) or (b) then S is centralised by G_0, while if S is of type (c) then G_0 induces only inner automorphisms on S. It follows that every non-abelian chief factor of G_0 is in fact simple, of type (c), hence in $\mathcal{X}(m)$, and G_0 acts on it by inner automorphisms. Lemma 3.5 of [Sh1] now shows that $G_0/R(G_0) = S_1 \times \cdots \times S_t$, with $S_i \in \mathcal{X}(m)$ for each i. Suppose r of the factors S_i are isomorphic to S; if their product is $B/R(G_0)$ then $B \triangleleft G$ and $B/R(G_0) \cong S^{(r)}$, so the first part of the proof shows that $r \leq m$.

Thus $G_0 \in \mathcal{Y}(m)$ and $\mu(G_0) \leq m$. We take $f_2(\alpha) = f_3(\alpha) = m$ to complete the proof.

Proposition 2 depends on the next two lemmas.

LEMMA 2: *Let G be a group such that $G/R(G) = S_1 \times \cdots \times S_t$, where each S_i is a non-abelian simple group. Put $R = R(G)$ and $E = E(G)$. Then we have*

(i) *$E(G/E) = 1$ and $Z(E) = E \cap R \leq Z(G)$;*

(ii) *if $Z(G) = 1$ then $E \subseteq \mathrm{soc}(G)$;*

(iii) *if $O_{p'}(R) = 1$ then $O_{p'}(R/(E \cap R)) = 1$ and $O_{p'}(G/E) = 1$;*

(iv) *put* $E_p/O_{p'}(R) = E(G/O_{p'}(R))$, $X_p = E_p \cap R$ *and* $Y_p = O_p(X_p)$ *for each prime* p. *Then* $[X_p, G] \leq O_{p'}(R)$ *for each* p, *and the group* $Y = \langle Y_p | \text{ all } p\rangle$ *satisfies* $Y \leq Z(G)$ *and* $|Y| \mid \prod_{i=1}^{t} |M(S_i)|$.

Proof: Recall ([A], §31) that the **components** of G are its perfect subnormal subgroups X such that $X/Z(X)$ is simple; E is the subgroup they generate, and $[E, R] = 1$.

Let X be a component. Then $RX/R = S_i$ for some i, so if $C/R = \prod_{j \neq i} S_j$ then $[C, X] \leq R$. It follows that $[C, \langle X^G\rangle, \langle X^G\rangle] = 1$ and hence that $[C, X] = 1$ since X is perfect (3-subgroup lemma). Clearly $CX = G$, so $X \lhd G$. Therefore $E = X_1 \cdots X_k$ (where $X_1, ..., X_k$ are the components of G) and $G = EC_G(E)$. This implies that $Z(E) \leq Z(G)$, and it is clear that $Z(E) = E \cap R$.

Suppose Y/E is a component of G/E. Put $U = C_Y(E)$ and $V = U \cap R$. Then $V = Y \cap R$ and $Y = EU$, $Y \cap ER = EV$. I claim that U' is a component of G. To see this, note that $U/(E \cap U) \cong Y/E$ is perfect; as $E \cap U \leq Z(U)$ this implies that U' is perfect. Clearly U' is subnormal in G. Now

$$U \cap EV = (U \cap E)V = Z(E)V = V,$$

so $U/V \cong Y/EV \cong YR/ER \cong S_i$ for some i. Therefore $U = U'V$, and so $U'/(U' \cap V) \cong S_i$ is simple. Since $E \leq EV \lhd\!\!\!\neq Y$, we have $[EV, Y] \leq E$, and so $[V, U] \leq E \cap U \leq Z(U)$. Hence $U' \cap V \leq Z(U')$, and the claim follows. But then $U' \leq E$, making Y/E abelian, a contradiction. This shows that $E(G/E) = 1$, and establishes (i).

Now suppose that $Z(G) = 1$. Then $E \cap R = 1$, so if X is a component of G then $X \cap R = 1$, whence $X \cong RX/R = S_i$ for some i. Since (as we have seen) $X \lhd G$, it follows that $X \leq \text{soc}(G)$. Thus (ii) follows.

Suppose that $O_{p'}(R) = 1$. If $E \cap R \leq Q \lhd R$ and $Q/(E \cap R)$ is a q-group for some $q \in p'$, then Q is nilpotent, so the Sylow q-subgroup of Q is contained in $O_{p'}(R) = 1$, forcing $Q = E \cap R$. As R is soluble this shows that $O_{p'}(R/(E \cap R)) = 1$. Now, since $E(G/E) = 1$, the minimal normal subgroups of G/E are abelian and therefore lie inside RE/E. So if $O_{p'}(G/E) \neq 1$ there exists a normal p'-subgroup $M/E \neq 1$ in G/E with $M \leq RE$. But then $M/E \cong (M \cap R)/(E \cap R) \leq O_{p'}(R/(E \cap R)) = 1$, a contradiction. Thus $O_{p'}(G/E) = 1$, giving (iii).

Finally, we prove (iv). Writing $\bar{} : G \to G/O_{p'}(R)$, we have $\bar{X}_p = E(\bar{G}) \cap R(\bar{G})$, so $\bar{X}_p \leq Z(\bar{G})$ and $[X_p, G] \leq O_{p'}(R)$. It follows that $[Y_p, G] \leq Y_p \cap O_{p'}(R) = 1$,

so $Y_p \leq Z(G)$. Since $\bar{E}_p = E(\bar{G})$ is perfect, it also follows that $|\bar{X}_p|\,|\,|M(E_p/X_p)|$. But $Y_p \cong \bar{Y}_p \leq \bar{X}_p$ so $|Y_p|\,|\,|M(E_p/X_p)|$. Since $E_p/X_p \cong E_pR/R \lhd G/R$, we have $E_p/X_p \cong \prod_{j\in J(p)} S_j$ for some subset $J(p)$ of $\{1,...,t\}$, and so ([H] Chapter V, Satz 25.10)

$$|Y_p|\,|\,|M(\prod_{j\in J(p)} S_j)| = \prod_{j\in J(p)} |M(S_j)|\,|\,\prod_{j=1}^{t} |M(S_i)|.$$

This implies (iv) since $Y = \prod_p Y_p$ and Y_p is a p-group for each prime p.

LEMMA 3: *Let $G \in \mathcal{Y}(c)$. If $E(G) = O_{p'}(G) = 1$ and G has wPSG of degree β, then $r_p(G) \leq f(\beta, c)$.*

Proof: This is an adaptation of [M1], Theorem 1, and [MS], Theorem 3.9. Put $F = O_p(G)$. Then $F = F(G)$ and, since $E(G) = 1$, $C_G(F) \leq F$ (see [A], 31.13). Put $V = F/F'F^p$, $d = \dim_{\mathbb{F}_p}(V)$. Then V is a faithful module for G/F, by [M1], Lemma 1.5, and it follows that $|G\colon F| \leq p^{dt}$, for some t depending only on c, by [M1], Lemma 1.2 (an application of [BCP], Cor. 3.3). Since V contains at least $p^{[d/2]^2}$ subspaces, we have

$$p^{[d/2]^2} \leq s(G/F'F^p) \leq p^{d(t+1)\beta},$$

giving $d \leq 4(t+1)\beta + 2$. Hence $|G\colon F| \leq p^m$ where m depends only on β and c.

Now put $F_0 = F$ and, for $i \geq 0$, $F_{i+1} = F_i'F_i^p$. Let $s = \max_i \dim_{\mathbb{F}_p}(F_{i-1}/F_i)$, $q = 2 + [\log s]$. Then [DDMS], Chapter 2, Exercises 6 and 7 show that F_q is a powerful p-group, $|F\colon F_q| \leq p^{sq}$ and $\mathrm{rk}(F) \leq s(q+1)$. Since F_q is powerful, we have $\dim_{\mathbb{F}_p}(F_{i-1}/F_i) \leq \dim_{\mathbb{F}_p}(F_q/F_{q+1})$ for all $i > q$ (*loc. cit.*, Theorem 2.9); hence $\dim_{\mathbb{F}_p}(F_{i-1}/F_i) = s$ for some $i \leq q+1$. Then $|G\colon F_i| \leq p^{(q+1)s+m}$, and as above we infer that $[s/2]^2 \leq ((q+1)s+m)\beta$. Since $q \leq 2 + \log s$ this implies that s is bounded by some function of m and β, and hence of c and β. As

$$r_p(G) \leq r_p(G/F) + \mathrm{rk}(F) \leq m + (q+1)s,$$

the result follows.

Proof of Proposition 2: Now $G \in \mathcal{Y}(c)$. Let Y be the subgroup of $Z(G)$ defined in Lemma 2(iv). Then $|Y| \leq \prod_i^t |M(S_i)|$ where $G/R(G) = S_1 \times \cdots \times S_t$. Now $S_i \in \mathcal{X}(c)$; it follows that $|M(S_i)| \leq 16(c+1)$ (see for example [C] Chapter 3, Table 5), and hence that $|Y| \leq |G\colon R(G)|^{f_4(c)}$ where $f_4(c) = \log 16(c+1)/\log 60$.

Now let p be a prime. Applying Lemma 2(iii) in turn to $G/O_{p'}(R)$ and to G/X_p (in the notation of Lemma 2(iv)), we see that $O_{p'}(G/E_p) = 1$. Lemma 2(i) shows that $E(G/E_p) = 1$. We may therefore apply Lemma 3 to infer that $r_p(G/E_p) \leq f(\beta, c)$. If $P = O_p(R)$ then $P \cap X_p = Y_p$, so

$$P/Y_p \cong PX_p/X_p \cong PE_p/E_p \leq G/E_p.$$

Hence $\mathrm{rk}(P/Y_p) \leq f(\beta, c)$.

It follows that $\mathrm{rk}(F(G)/Y) \leq f(\beta, c)$, since $F(G)/Y \cong \prod_p O_p(R)/Y_p$.

3. Some polynomial bounds

In this section we prove

PROPOSITION 3: *Let $G \in \mathcal{Y}(c)$ and let H be a subgroup of G with $\mathrm{core}_G(H) = 1$. Then*

$$|G| \leq |G\colon H|^{f_7(c,r,\mu)}$$

where $r = \mathrm{rk}(F(G)/Z(G))$ and $\mu = \mu(G)$.

PROPOSITION 4: *Let $G \in \mathcal{Y}(c)$ and suppose that G has wPSG of degree β. Then, for each n, the number of normal subgroups of index at most n in G is at most $n^{f_8(c,\beta,\mu)}$, where $\mu = \mu(G)$.*

Two further lemmas are needed for Proposition 3.

LEMMA 4: *Let A be a soluble group, let n be the exponent of $F(A)$ and $r = \mathrm{rk}(F(A))$. Then*

$$|A| \leq n^{4r(3+\log r)}.$$

Proof: Let p be a prime and suppose that p^m exactly divides n, where $m \geq 1$. Let P be the Sylow p-subgroup of $F(A)$. Then $P^{p^m} = 1$. By [DDMS], Theorem 2.13, P has a powerful normal subgroup Q of index at most $p^{r(2+\log r)}$, and [DDMS], Cor. 2.8 shows that $|Q| \leq p^{mr}$. Thus $|P| \leq p^{mr(3+\log r)}$. It follows that $|F(A)| \leq n^{r(3+\log r)}$, and this gives the result since $|A| \leq |F(A)|^4$ (see [P], remark on page 204).

LEMMA 5: *Let G be a transitive subgroup of $\mathrm{Sym}(n)$. If every non-abelian composition factor of G is in $\mathcal{X}(c)$, then $\sigma(G) \leq n^{\mu(G)f(c)}$.*

Proof: This is by induction on n. Let $H = G_1$, so $|G\colon H| = n$ and $\mathrm{core}_G(H) = 1$. Choose $M \leq G$ so that H is a maximal subgroup of M, and put $K = \mathrm{core}_G(M)$.

Then $|M\colon H| = r > 1$ and $|G\colon M| = s$, with $rs = n$. Inductively, we may assume that $\sigma(G/K) \leq s^{\mu(G/K)f(c)}$.

Now put $H_M = \operatorname{core}_M(H)$. Then M/H_M is a primitive subgroup of $\mathrm{Sym}(r)$. Since every non-abelian composition factor of M/H_M occurs as a section of some group in $\mathcal{X}(c)$, the group M/H_M belongs to the class $\mathcal{G}(c_0)$ considered in [BCP], where c_0 depends only on c. It follows by [BCP], Theorem 1.1, that $|M/H_M| \leq r^{f(c)}$ where $f(c)$ depends only on c.

Write $K_0 = K \cap H_M$. Each composition factor of K occurs as a composition factor of K/K_0, since $K_0^g \lhd K$ for each $g \in G$ and $\bigcap_{g\in G} K_0^g \leq \operatorname{core}_G(H) = 1$. Hence

$$\sigma(K) \leq \sigma(K/K_0)^{\mu(K)} \leq |K/K_0|^{\mu(K)} \leq r^{f(c)\mu(K)}$$

since $|K/K_0| \leq |M/H_M|$. The result follows since $\sigma(G) = \sigma(G/K)\sigma(K)$, $\mu(G/K) \leq \mu(G)$, $\mu(K) \leq \mu(G)$ and $rs = n$.

Proof of Proposition 3: Now $G \in \mathcal{Y}(c)$ and $H \leq G$ satisfies $\operatorname{core}_G(H) = 1$. Put $n = |G\colon H|$ and $\mu = \mu(G)$, and let $R = R(G)$, $F = F(G)$, $Z = Z(G)$. Then

$$|G\colon R| = \sigma(G) \leq n^{\mu f(c)},$$

by Lemma 5.

Since $H^g \cap F$ is subnormal in F for each $g \in G$, we have $F^n = 1$. Put $A = R/Z$; then $F(A) = F/Z$, so Lemma 4 gives

$$|R\colon Z| = |A| \leq n^{4r(3+\log r)}$$

where $r = \mathrm{rk}(F/Z)$. Also $|Z| \leq n$ since $Z \cap H \leq \operatorname{core}_G(H) = 1$. Thus $|G| \leq n^{f(c,r,\mu)}$ where $f(c, r, \mu) = \mu f(c) + 4r(3 + \log r) + 1$.

LEMMA 6: *Let G be a direct product of non-abelian simple groups. Then, for each n, the number of normal subgroups of index at most n in G is at most $n^{2+2\mu(G)}$.*

Proof: Put $\mu = \mu(G)$. Denote by a_m the number of normal subgroups of index exactly m in G, and by b_m the number of isomorphism types of images of G of order m. If F is any such image, then $|\mathrm{Aut}(F)| \geq m$, so

$$a_m \leq m^{d(G)-1} b_m.$$

Since $d(S) = 2$ for each non-abelian simple group S, we have $d(G) \leq 2\mu$.

It remains to estimate b_m. We have $G = \prod S_i^{(f_i)}$ where $S_1, S_2, \ldots$ are pairwise non-isomorphic simple groups, $f_i \leq \mu$ for each i, and, putting $s_i = |S_i|$, we may suppose that

$$60 \leq s_1 \leq s_2 \leq \cdots.$$

Since there are at most 2 non-isomorphic simple groups of each order, no integer appears more than twice in the sequence (s_i). Now b_m is just the number $N(m)$ of sequences (e_i) such that $0 \leq e_i \leq f_i$ and $\prod s_i^{e_i} = m$. I claim that $N(m) \leq m^2$. The lemma will follow, since we then have

$$\sum_{m=1}^{n} a_m \leq \sum_{m=1}^{n} m^{2\mu-1}.m^2 \leq n^{2\mu+2}.$$

The claim is proved by induction on m. If $m < 60$ then $N(m) = 0$. Suppose that $m \geq 60$. Then

$$N(m) \leq \sum_{s_i \mid m} N(m/s_i) \leq \sum_{s_i \mid m} (m/s_i)^2 \leq 2m^2 \sum_{r \geq 60} r^{-2} < m^2.$$

Proof of Proposition 4: Now $G \in \mathcal{Y}(c)$ and G has wPSG of degree β. Put $\mu = \mu(G)$ and $R = R(G)$. Let n be a positive integer. If $N \lhd G$ and $|G\colon N| \leq n$ then $|G\colon RN| \leq n$, so there are at most $n^{2+2\mu}$ possibilities for RN, by Lemma 6. Let us fix $K \lhd G$, with $R \leq K$ and $|G\colon K| \leq n$, fix $m \leq n$, and put

$$\mathcal{N} = \{N \lhd G \mid RN = K \text{ and } |K\colon N| = m\}.$$

It will suffice to prove that $|\mathcal{N}| \leq n^{f(c,\beta)}$.

Now if $N \in \mathcal{N}$ then K/N is soluble, of derived length at most $\log m$; so putting $D = \bigcap \mathcal{N}$ we have $\bar{G} = G/D \in \mathcal{Y}(c)$ and $\bar{K} = K/D = R(\bar{G})$. Also $\bar{K}^m = 1$.

By Proposition 2, $\bar{G}$ has a central subgroup Y, with

$$|Y| \leq |\bar{G}\colon \bar{K}|^{f_4(c)} \leq n^{f_4(c)},$$

such that $\mathrm{rk}(F(\bar{G})/Y) \leq f_5(c,\beta)$. Lemma 4, applied to the group $A = \bar{K}/Y$, then shows that

$$|\bar{K}\colon Y| \leq m^{h(c,\beta)} \leq n^{h(c,\beta)},$$

where $h(c,\beta) = 4r(3 + \log r)$ with $r = f_5(c,\beta)$. It follows that $|\bar{G}| \leq n^{h(c,\beta)+f_4(c)+1}$. Hence

$$|\mathcal{N}| \leq s(\bar{G}) \leq |\bar{G}|^{\beta} \leq n^{f(c,\beta)}$$

where $f(c,\beta) = \beta(h(c,\beta) + f_4(c) + 1)$.

4. Proof of Theorem B

We need one more simple lemma:

LEMMA 7: *Let G be a group with wPSG of degree $\alpha \geq 1$, and let $G_0 \triangleleft G$ with $|G: G_0| = m > 1$.*

(i) *G_0 has wPSG of degree at most $(m + \log m)\alpha$.*

(ii) *If G_0 has PSG of degree γ, then G has PSG of degree at most $\gamma + \alpha \log m$.*

Proof: (i) Let $K \underset{\neq}{\triangleleft} G_0$ and put $K^0 = \mathrm{core}_G(K)$. Then $|G/K^0| \leq m|G_0: K|^m$, so

$$s(G_0/K) \leq s(G/K^0) \leq m^\alpha |G_0/K|^{m\alpha} \leq |G_0/K|^{(m+\log m)\alpha}$$

since $|G_0/K| \geq 2$.

(ii) [MS] Lemma 3.1 shows that G has PSG of degree at most $\gamma + \max\{\alpha^*, r\}$, where $r = \mathrm{rk}(G/G_0)$ and G/G_0 has PSG of degree α^*. It is easy to see that $\alpha^* \leq \alpha \log m$ and that $r \leq \log m$, so we have (ii).

Proof of Theorem B: Now let G be a group with wPSG of degree α. By Proposition 1, G has a normal subgroup $G_0 \in \mathcal{Y}(c)$, with $c = f_3(\alpha)$, $|G: G_0| = m \leq f_1(\alpha)$ and $\mu(G_0) = \mu \leq f_2(\alpha)$. Lemma 7 shows that G_0 has wPSG of degree at most $\beta = (m + \log m)\alpha$.

Put $q = f_7(c, f_5(c, \beta), \mu)$. If H is a subgroup of index at most n in G_0 and $H^0 = \mathrm{core}_{G^0}(H)$, then $|G_0: H^0| \leq n^{f_7(c,r,\mu)}$ by Proposition 3, where $r = \mathrm{rk}(F(G_0/H^0)/Z(G_0/H^0))$; and Proposition 2 shows that $r \leq f_5(c, \beta)$. Thus $|G_0: H^0| \leq n^q$, and so $s(G_0/H^0) \leq n^{q\beta}$.

By Proposition 4, G_0 has at most $n^{qf_8(c,\beta,\mu)}$ normal subgroups like H^0. It follows that

$$s_n(G_0) \leq n^\gamma$$

where $\gamma = q(\beta + f_8(c, \beta, \mu))$. Lemma 7(ii) now shows that G has PSG of degree at most $\gamma + \alpha \log m$. This concludes the proof.

References

[A] M. Aschbacher, *Finite Group Theory*, CUP, Cambridge, 1986.

[BCP] L. Babai, P. J. Cameron and P. Palfy, *On the orders of primitive groups with restricted nonabelian composition factors*, Journal of Algebra **79** (1982), 161–168.

[C] J. H. Conway *et al.*, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[DDMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic Pro-p Groups*, CUP, Cambridge, 1991.

[H] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin–Heidelberg–New York, 1967.

[K] L. G. Kovacs, *On finite soluble groups*, Mathematische Zeitschrift **103** (1968), 37–39.

[LM] A. Lubotzky and A. Mann, *Powerful p-groups. I. Finite groups*, Journal of Algebra **105** (1987), 484–505.

[LMS] A. Lubotzky, A. Mann and D. Segal, *Finitely generated groups of polynomial subgroup growth*, Israel Journal of Mathematics **82** (1993), 363–371.

[M1] A. Mann, *Some properties of polynomial subgroup growth groups*, Israel Journal of Mathematics **82** (1993), 373–380.

[M2] A. Mann, *Positively finitely generated groups*, Forum Mathematicum, to appear.

[MS] A. Mann and D. Segal, *Uniform finiteness conditions in residually finite groups*, Proceedings of the London Mathematical Society **61** (1990), 529–545.

[P] L. Pyber, *Asymptotic results for permutation groups*, DIMACS Series, Discrete Mathematics and Theoretical Computer Science **11** (1993), 197–219.

[Sh1] A. Shalev, *On the fixity of linear groups*, Proceedings of the London Mathematical Society **68** (1994), 265–293.

[Sh2] A. Shalev, *Subgroup growth and sieve methods*, preprint.