GROWTH SEQUENCES OF FINITELY GENERATED GROUPS II

A.G.R. Stewart and James Wiegold

For Bernhard Neumann with respect and affection

A study is made of the minimum number of generators of the n-th direct power of certain finitely generated groups.

1. Introduction

For a finitely generated group G, the growth sequence of G is the sequence $\{d(G^n)\}$, where $d(G^n)$ denotes the minimum number of generators of the n-th direct power G^n of G. A very tight description was given in [3–7] for the growth sequence of a finite group G; the main gross feature is that the sequence increases roughly logarithmically in n if G is perfect, while $d(G^n) = nd(G/G')$ for large enough n if G is not perfect. For infinite groups, the picture is less clear. It is again the case (see [8]) that $d(G^n) = nd(G/G')$ eventually if G is not perfect, and that $\{d(G^n)\}$ is bounded above by a logarithmic function of n if G is perfect. The most important and apparently quite unattackable problem left is this: if G has no finite images other that the identity, prove that $d(G^n) = d(G^{n+1})$ for all large enough n.

The present article arose out of an unsuccessful attempt to answer a related problem.

Problem 1. Let G be a finitely generated group having a non-trivial finite image. Is the growth sequence of G eventually the same as that of a finite image of G?

By the above remarks, this is true if G is not perfect. The perfect case seems very hard, and we are far from a solution. Note that the positive solution to Problem 1 would entail the existence of a finite image whose growth sequence is eventually as fast as that of every finite image of G. This is true, at least in the case where G has a unique non-trivial image of smallest order (which must, of course, be simple) - see Theorem A. Whether it is true in general involves the following sort of situation. Let S and T be 2-generator non-abelian finite simple groups of the same order s. The theorem in [6] shows that $d\left(S^{s^n}\right) = d\left(T^{s^n}\right) = n + 2$ for all $n \geq 0$, so that the growth sequences are

the same infinitely often. However, it could be that $d(S^m) > d(T^m)$ and $d(T^n) > d(S^n)$ for infinitely many values of m and n; short of taking two different simple groups of the same order and examining Möbius functions (see[2]) of their subgroup lattices (a tall order!) we see no way of resolving this problem. Theorem A could be reformulated to take into account these possibilities, but we see no benefit in doing this.

A type of group where the finite image with fastest growth sequence is easily identified is the free square $G = B \star B$ of a non-abelian finite simple group B. It turns out to be B^{2+a}, where $a = |\operatorname{Aut} B|$ (Corollary to Theorem B). We believe the growth sequence of G is eventually that of B^{2+a}. In any case, by [7],

$$d(G^n) \geqq d\left(B^{(2+a)n}\right) > \log_s n + \log_s (2 + a) + \log_s a,$$

where $s = |B|$. If it is true that $d(G^n) = d\left(B^{(2+a)n}\right)$ from some point on, then by [3, 4.4],

$$d(G^n) \leqq \log_s n + \log_s a + \log_s (2 + a) + 1 + \psi(n),$$

where $\psi(n) \to 0$ as $n \to \infty$. In utmost generality, all that we can say is

$$(1.1) \qquad\qquad d(G^n) \leqq 2d(B^n) \leqq 2(\log_s n + \log_s a + \psi(n)).$$

Upper bounds for growth sequences can be attacked using a concept incorporated in the proof of Theorem 4.2 of [8], and discovered independently by David Meier (unpublished). In recognition of Dr. Meier's contribution we make the following definitions:

DEFINITION 1: A subset M of a group G is said to be a *Meier set* for G if

    (i)   for each non-trivial x in M, $\langle x \rangle^G = G$,

    (ii) for every pair of distinct elements x, y of M, $\langle xy^{-1} \rangle^G = G$.

DEFINITION 2: The *Meier number* $\mu(G)$ is the largest cardinal of a Meier set of G.

Clearly, G has Meier number 1 if and only if it is not the normal closure of a single element. Equally clearly, $\mu(B) = |B|$ for a simple group B.

The main general results using this concept are as follows.

THEOREM C. *If G is a finitely generated perfect group with $m = \mu(G)$ finite, then $d(G^{mn}) \leqq d(G^n) + 1$ for all n. Thus $d(G^n) < d(G) + \log_m n + 1$ for all n.*

THEOREM D. *If G is a finite perfect group and s the smallest order of a non-trivial image of G, then $\mu(G) = s$.*

These two theorems combine to give elementary proofs of results in [5].

To improve on (1.1), it would suffice to prove that $B \star B$ has a Meier set with more than $\sqrt{|B|}$ elements. We believe this to be true, but even the verification for A_5 took a computer! Using a computer program devised by Dr. C.H. Houghton of University College Cardiff and implemented on the University of Zimbabwe computer with the help of Dr. P.J. Fish, Dr. J.A. Howarth and Mr. P.J. McBurney, a Meier set of 15 elements of length 2 has been found in $A_5 \star A_5$. We thank all the four people mentioned for their invaluable assistance. For $G = A_5 \star A_5$, we deduce from Theorem C that

$$d(G^n) < 5 + \log_{15} n = 5 + \log_{15} 60 \log_{60} n$$

for all n. This is better than (1.1); the dominant coefficient 2 has been reduced to $\log_{15} 60 = 1.5119\ldots$, about half way to the 1 we would like it to be. The computer has also been used to check that $A_5 \star A_5$ has no Meier set of order 60 consisting of elements of length 2. Meier sets with elements of higher lengths have not yielded to attack. In this context we ask:

Problem 2. For a finite non-abelian simple group B, is $\mu(B \star B) < |B|$? Note that every finite image of $B \star B$ has Meier number $|B|$, by Theorem D.

It is clear that $\mu(B \star B)$ is at least as great as the cardinal of the smallest non-trivial Sylow subgroup of B, and thus certainly (to put it at its very crudest) at least 3. We thank the referee for pointing out that $\mu(B \star B)$ is at least the cardinal of a second largest Sylow subgroup of B, and thus certainly (to put it at its very crudest), at least 4. We repeat our belief that the answer to our final problem is yes:

Problem 3. For every finite non-abelian simple group B, is there a Meier set of $B \star B$ consisting of elements of length 2 and of cardinal more than $\sqrt{|B|}$?

In a subsequent article, we hope to turn to the study of the growth sequence of a free product $G = A \star B$, where A and B are finite simple groups with $|A| < |B|$. The growth sequence of G should eventually be the same as that of A, and the following is evidence, albeit thin, in favour of this. If $|B|$ has a prime divisor larger than $|A|$, it is evident that G has a Meier set of cardinal $|A|$, so that $d(G^n) < d(G) + \log_{|A|} n + 1$ for all n, by Theorem C. This means that $\{d(G^n)\}$ and $\{d(A^n)\}$ differ by at most a bounded quantity.

2. PROOFS

THEOREM A. *Let G be a finitely generated perfect group having non-trivial finite images, suppose that G has a unique non-trivial image S of smallest order, and let S^λ be the highest power of S that is an image of G. Then the growth sequence of S^λ is eventually as large as that of every finite image of G; that is to say, there is a constant*

K depending only on G such that $d(B^n) \leqq d(S^{\lambda n})$ for every finite image B of G and every $n \geqq K$.

PROOF: Let B be a non-trivial finite image of G, let S_1, $S_2, \ldots, S_r$ be the simple images of B, and $S_1^{\lambda_1}$, $S_2^{\lambda_2}, \ldots, S_r^{\lambda_r}$ the highest powers of S_1, $S_2, \ldots, S_r$ that are images of B. (The existence of λ, $\lambda_1, \ldots, \lambda_r$ follows since the growth sequence of every non-trivial finite group is unbounded [3].) We deal first with the case where S is not one of S_1, $S_2, \ldots, S_r$. Since $d(B) \leqq d(G)$, we get from [5] and [3] that

$$d(B^n) < d(B) + 1 + \log_t n \leqq d(G) + 1 + \log_t n,$$
$$d(S^{\lambda n}) > \log_s (\lambda n),$$

where $t = \min(|S_1|, |S_2|, \ldots, |S_r|)$ and $s = |S|$. Thus $d(S^{\lambda n}) \geqq d(B^n)$ as soon as $\log_s (\lambda n) \geqq \log_t n + d(G) + 1$; since $s < t$, this certainly holds if $\log_s (\lambda n) \geqq \log_{s+1} n + d(G) + 1$. Note that λ, s, $d(G)$ depend only on G and not on B.

Now suppose that S is one of S_1, $S_2, \ldots, S_r$, say $S = S_1$. By result of Gaschütz [1] (see [4, 6]),

$$d(B^n) = \max\left(d(B), d\left(S_1^{\lambda_1 n}\right), \ldots, d\left(S_r^{\lambda_r n}\right)\right)$$

for all n. Reasoning as in the first part of the proof, we conclude that there is a number L depending only on G such that

$$d(B^n) = \max\left(d(B), d(S^{\lambda_1 n})\right)$$

for all $n \geq L$. Thus $d(B^n) = d(S^{\lambda_1 n})$ provided $n \geqq L$ and $d(S^{\lambda_1 n}) \geqq d(G)$. Since this latter holds whenever $\log_s (\lambda_1 n) \geqq d(G)$, and $\lambda_1 \leqq \lambda$, the proof of Theorem A is complete.   □

THEOREM B. *Let B be a finite non-abelian simple group, t an integer at least 1, let B_1, $B_2, \ldots, B_t$ be groups isomorphic to B, and G be their free product $B_1 \star B_2 \star \ldots \star B_t$. If $a = |\mathrm{Aut}\,B|$, there are precisely $\sum_{r=1}^{t} \binom{t}{r} a^{r-1}$ different normal subgroups N of G such that $G/N \cong B$.*

COROLLARY. *The highest power of B that is homomorphic image of G is B^λ, where $\lambda = \sum_{r=1}^{t} \binom{t}{r} a^{r-1}$.*

PROOF OF THEOREM B: Since each B_i is simple, $N \cap B_i = 1$ or $N \supseteq B_i$ for every normal subgroup N of G. The proof proceeds by showing that for every r-element subset $K = \{i_1, i_2, \ldots, i_r\}$ of the set $I = \{1, 2, \ldots, t\}$, there are precisely a^{r-1} elements in the set

$$U(K) = \{N \mid N \trianglelefteq G \,\&\, G/N \cong B \,\&\, (k \in K \rightarrow N \cap B_k = 1) \,\&\, (j \in I \backslash K \rightarrow N \supseteq B_j)\}.$$

Since there are $\binom{t}{r}$ r-element subsets K of I, summation over r and K will give the required result.

Two cases arise.

Case 1. $r = 1$. A routine calculation shows that a non-trivial normal subgroup N of G is in $U(\{k\})$, for $k \in I$, if and only if it is the normal closure of $\bigcup_{j \neq k} B_j$. Thus $U(\{k\})$ has a single member, as required.

Case 2. Suppose that $2 \leq r \leq t$ and that $K = \{k_1, k_2, \ldots, k_r\}$ is an r-element subset of I. Case 2 will follow when we establish a bijection between $U(K)$ and the set

$$V = \{(\alpha_2, \ldots, \alpha_r) \mid \alpha_i \in \operatorname{Aut} B\}.$$

For each N in $U(K)$ and each i in K, the fact that $N \cap B_i$ is trivial implies that NB_i/N is isomorphic to B_i and thus to G/N. Thus, since G/N is finite, $NB_i = G = NB_j$ for all i, j in K. So, for each $b \in B$ and each j such that $2 \leq j \leq r$, there is a unique $b\alpha_j$ in B for which

$$N(b\psi_i) = N((b\alpha_j)\psi_j)$$

where ψ_i is the isomorphism from B to B_{k_i}. Because $N \cap B_i$ is trivial for each i in K, it follows that the maps $\alpha_j \colon B \to B$ so defined are automorphisms of B; and θ defined by $N\theta = (\alpha_2, \ldots, \alpha_r)$ is a mapping from $U(K)$ to V.

Conversely, given $(\beta_2, \ldots, \beta_r) \in V$, let T be the normal closure in G of the set $\{(b\psi_i)^{-1}(b\beta_j\psi_j) \mid b \in B, \ 2 \leq j \leq r\}$, where the ψ_i are as above. Let F be the normal closure in G of $\bigcup_{j \notin K} B_j$, and $M(\beta_2, \ldots, \beta_r)$ the product TF. Then $M(\beta_2, \ldots, \beta_r)$ is an element in $U(K)$ whose image under θ is $(\beta_2, \ldots, \beta_r)$. Moreover if N is in $U(K)$ and $N\theta = (\alpha_2, \ldots, \alpha_r)$, then $M(\alpha_2, \ldots, \alpha_r) = N$, so that θ is bijective. ☐

The Corollary follows since all the factor-groups G/N are simple. ☐

PROOF OF THEOREM C: Let G be a finitely generated perfect group with $m = \mu(G) < \infty$, let $\{1, x_2, \ldots, x_m\}$ be a Meier set for G, and let $W = \{(g_{i1}, g_{i2}, \ldots, g_{in}) \mid 1 \leq i \leq d(G^n) = d\}$ be a minimal generating set for G^n. The proof is very similar to that of Theorem 4.2 in [8].

We prove by induction on r that the subgroup H of G^{nr} generated by the following elements is G^{nr}:

$$a_i = (g_{i1}, g_{i2}, \ldots, g_{in}, g_{i1}, \ldots, g_{in}, \ldots, g_{i1}, \ldots, g_{in}), \qquad 1 \leq i \leq d,$$
$$a_{d+1} = (1, 1, \ldots, 1, x_2, \ldots, x_2, \ldots, x_r, \ldots, x_r),$$

each with r blocks of n components.

The result if trivial for $r = 1$. Suppose that $r > 1$ and that the result is established for smaller Meier sets. For arbitrary $g_1, g_2, \ldots, g_n$ in G, H contains

$$(g_1, g_2, \ldots, g_n, g_1, \ldots, g_n, \ldots, g_1, \ldots, g_n),$$

since W generates G^n. In particular, H contains

$$h = (x_2, x_2, \ldots, x_2, x_2, \ldots, x_2, x_2, \ldots, x_2)$$

and

$$ha_{d+1}^{-1} = \left(x_2, x_2, \ldots, x_2, 1, \ldots, 1, x_2 x_3^{-1}, \ldots, x_2 x_3^{-1}, \ldots, x_2 x_r^{-1}, \ldots, x_2 x_r^{-1}\right).$$

But $\{1, x_2 x_3^{-1}, \ldots, x_2 x_r^{-1}\}$ is a Meier set for G consisting of $r - 1$ elements, and thus $\{a_1, a_2, \ldots, a_d, ha_{d+1}^{-1}\}$ generates $G^{n(r-1)}$ in the last $n(r-1)$ components. Thus for arbitary g in G, and any i such that $n + 1 \leqq i \leqq nr$, H contains an element of the form

$$m_i = (\star, \star, \ldots, \star, 1, \ldots, 1, g, 1, \ldots, 1)$$

where g is in the i-th position and the stars are unknown. But

$$[a_{d+1}, m_i] = \left(1, \ldots, 1, [x_{j_i}, g] 1, \ldots, 1\right)$$

and $[x_{j_i}, G] = G$, so that H contains $(1, \ldots, 1, g, 1, \ldots, 1)$, and so H contains the whole of the i-th component. A glance at the form of W shows that $H = G^{nr}$, and the theorem follows.   ⬜

PROOF OF THEOREM D: Here G is a finite perfect group and s is the smallest order of a simple image of G, and we wish to show that $\mu(G) = s$. Firstly, it is routine to show that epimorphisms carry Meier sets injectively into Meier sets, so certainly $\mu(G) \leqq s$; and we have to establish the existence of a Meier set of cardinal s.

This we do by induction on $|G|$. The result is clear for simple groups, so let G be a non-simple group, M a normal subgroup of G so that G/M is simple of order s, and suppose the result holds for groups of smaller order than G. Let N be a normal subgroup of G that is minimal among the non-trivial normal subgroups contained in M. Then G/N is smaller than G and s is the smallest order of a simple image of G/N, so that by induction there is a Meier set $\{N, Nx_2, \ldots, Nx_s\}$ of G/N. Thus $G = N\langle x_i \rangle^G = N\langle x_i x_j^{-1} \rangle^G$ for different i and j between 1 and s. Two cases arise.

Case 1. If the $N \cap \langle x_i \rangle^G$ and the $N \cap \langle x_i x_j^{-1} \rangle^G$ are all non-trivial, then by the minimality of N, $\langle x_i \rangle^G \geqq N$ and $\langle x_i x_j^{-1} \rangle^G \geqq N$ for all i and j so that $G = \langle x_i \rangle^G = \langle x_i x_j^{-1} \rangle^G$ and $\{1, x_2, \ldots, x_s\}$ is a Meier set for G.

Case 2. One of the above intersections is trivial, so that we can write $G = N \times T$. Both N and T are perfect, all their simple images are of order at most s, and T has a simple image of order s, since $G/M = TM/M \cong T/T \cap M$. Thus by the inductive hypothesis $\mu(N) \geqq s$ and $\mu(T) = s$. If $\{1, h_2, \ldots, h_s, \ldots\}$ is a Meier set for N and $\{1, g_2, \ldots, g_s\}$ is a Meier set for T, a very simple argument shows that $\{(1,1), (g_2, h_2), \ldots, (g_s, h_s)\}$ is a Meier set for $N \times T = G$. This completes Case 2 and the proof of the theorem. $\square$

Combining Theorems C and D, we get that $d(G^n) < d(G) + \log_s n + 1$ for a finite perfect group G with s the smallest order of a simple image of G. This is Lemma 2 of [5]; the proof given here is more elementary.

REFERENCES

[1] W. Gaschütz, 'Zu einem von B.H. und H. Neumann gestellten Problem', *Math. Nachr.* **14** (1955), 249–252.

[2] P. Hall, 'The Eulerian functions of a group', *Quart. J. Math. (Oxford)* **7** (1936), 134–151.

[3] J. Wiegold, 'Growth sequences of finite groups', *J. Austral. Math. Soc.* **17** (1974), 133–141.

[4] J. Wiegold, 'Growth sequences of finite groups II', *J. Austral. Math. Soc.* **20** (1975), 225–229.

[5] J. Wiegold, 'Growth sequences of finite groups III', *J. Austral. Math. Soc.* **25** (1978), 142–144.

[6] J. Wiegold, 'Growth sequences of finite groups IV', *J. Austral. Math. Soc.* **29** (1980), 14–16.

[7] D. Meier and James Wiegold, 'Growth sequences of finite groups V', *J. Austral. Math. Soc. Ser. A.* **31** (1981), 374–375.

[8] James Wiegold and J.S. Wilson, 'Growth sequences of finitely generated groups', *Arch. Math.* **30** (1978), 337–343.

Department of Mathematics
University of Zimbabwe
Harare
Zimbabwe

School of Mathematics
University of Wales
College of Cardiff
Senghenydd Road
Cardiff, CF2 4AG
United Kingdom