

GROWTH SEQUENCES OF FINITE GROUPS

In grateful memory of Hanna Neumann

JAMES WIEGOLD

(Received 27 June 1972)

Communicated by M. F. Newman

1. Introduction

During his investigation of the possible non-Hopf kernels for finitely generated groups in [1], Dey proves that the minimum number of generators $d(G^n)$ of the n -th direct power G^n of a non-trivial finite group G tends to infinity with n . This has prompted me to ask the question: what are the ways in which the sequence $\{d(G^n)\}$ can tend to infinity? Let us call this the *growth* sequence for G ; it is evidently monotone non-decreasing, and is at least logarithmic (Theorem 2.1). This paper is devoted to a proof that, broadly speaking, there are two different types of behaviour. If G has non-trivial abelian images (the imperfect case, § 3), then the growth sequence of G is eventually an arithmetic progression with common difference $d(G/G')$. In special cases (Theorem 5.2) the initial behaviour can be quite nasty. Our arguments in § 3 are totally elementary. If G has only trivial abelian images (the perfect case, § 4), then the growth sequence of G is eventually bounded above by a sequence that grows logarithmically. It is a simple consequence of this fact that there are arbitrarily long blocks of positive integers on which the growth sequence takes constant values. This is a characteristic property of perfect groups, and indeed it was this feature in the growth sequences of large alternating groups (which I found by using *ad hoc* permutational arguments) that attracted me to the problem in the first place. The discussion of the perfect case rests on the lovely paper of Hall [2], which was brought to my notice by M. D. Atkinson.

The situation for infinite groups is much less clear-cut, though some brief comments are perhaps in order. Growth sequences of finitely generated infinite soluble groups are eventually arithmetic (§ 3), while those of groups having non-trivial finite images are at least logarithmic (this is a simple consequence of Theorem 2.1). On the other hand, Mary Tyrer has constructed a remarkable infinite finitely generated group, T shall we call it, isomorphic to its own direct square. This example will be published shortly [5]. Consequently, the growth sequence

of T is constant. It will be seen that all images of T have growth sequences that are eventually constant; including, of course, the simple images, which are presumably fairly numerous. Thus, in the infinite case, there are at least three different possibilities for growth sequences: they can be eventually arithmetic and non-constant (soluble groups), eventually essentially logarithmic ($T \times G$, for any non-trivial finite perfect group G), or eventually constant. I doubt very much if that is the end of the story.

I thank the referee for some useful suggestions.

2. Preliminaries

All notation not explained here is standard. The proof of the first result is essentially that of Dey in [1].

THEOREM 2.1. *For every non-trivial finite group G and every positive integer n , $d(G^n) > \log_{|G|} n$.*

PROOF. Suppose that $d(G^n) = k$, so that G^n is an epimorphic image of the free group F of rank k of the variety generated by G . A famous result of Neumann ([3]; a convenient reference is [4, 15.4]) tells us that F is a subgroup of G^l , where $l = |G|^k$. Since $d(F/F') = k$, while $d(G^l/(G^l)') = ld(G/G')$ by the following lemma, F must be a proper subgroup of G^l . In particular, $|G|^n < |G|^l$. Now take logarithms to the base $|G|$, twice.

In fact one can derive slightly better answers than that given by Theorem 2.1, simply by investigating the kernel of the epimorphism from F to G^n , and the index of F in G^l . However, it is scarcely worth the effort, especially as the lower bound $\log_{|G|} n$ is really very near the truth for non-abelian simple groups, as we shall see later.

The theorem says that growth sequences are not too small; neither are they too large, even though the growth is monotone:

LEMMA 2.2. *Let G be a finitely generated group and m, n positive integers. Then*

- (i) $d(G^{n+1}) \geq d(G^n)$,
- (ii) $d(G^{m+n}) \leq d(G^m) + d(G^n)$,
- (iii) $d(G^n) \leq n d(G)$,
- (iv) $d(G^n) \geq n d(G/G')$,
- (v) if $d(G) = d(G/G')$, then $d(G^n) = n d(G)$.

PROOF. The first part follows since G^n is an epimorphic image of G^{n+1} ; the second since G^{m+n} is $G^m \times G^n$; and the third is an immediate consequence of the second. To prove (iv), observe that $d(A^n) = n d(A)$ for any finitely generated abelian group A . Part (v) follows from (iii) and (iv).

One consequence of the lemma is that the growth sequence of a finitely

generated nilpotent group G is arithmetic with first term and common difference $d(G)$, and therefore devoid of interest.

The paper could be construed as a tentative first step towards a solution of the following problem.

PROBLEM. *Find arithmetical conditions on a sequence of positive integers that are necessary and sufficient for it to be the growth sequence of a finite group.*

Thus the results of this section give the obvious necessary conditions; later results are somewhat less obvious ones. Apart from extreme trivialities, I know of no general sufficient conditions.

3. The imperfect case

The basic lemma here is very elementary indeed:

LEMMA 3.1. *Let G be a finite imperfect group, and set $d(G/G') = \beta$. Then there exist elements z_1, z_2, \dots, z_β in G such that $G = \langle z_1, \dots, z_\beta, G' \rangle$ and $G' = \langle [z_1, G], \dots, [z_\beta, G] \rangle$.*

PROOF. Induct on the order of G . Everything is clear for $|G| = 2$ (the smallest possibility), so suppose that $|G| > 2$ and that the lemma is true for smaller imperfect groups. Let N be a minimal normal subgroup of G contained in G' , assuming — as we may — that G is not abelian. Then the inductive assumption applies to G/N to yield the existence of elements y_1, \dots, y_β such that $G/N = \langle y_1N, \dots, y_\betaN, G'/N \rangle$ and $G'/N = \langle [y_1, G], \dots, [y_\beta, G] \rangle N/N$; that is, such that $G = \langle y_1, \dots, y_\beta, G' \rangle$ and $G' = UN$, where we have set $U = \langle [y_1, G], \dots, [y_\beta, G] \rangle$ for short. Note that U is normal in G . Two cases arise:

(i) $U \cap N \neq 1$. Then $U \geq N$ so that $G' = U$ in this case, and y_1, \dots, y_β do the work required of z_1, \dots, z_β .

(ii) $U \cap N = 1$. Then $G' = U \times N$ so that $G'' = U' \times N'$. However, $G = \langle y_1, \dots, y_\beta, G' \rangle$, and simple commutator calculus shows that $G' = UG''$, whence it follows that $G' = U \times N'$. Thus $N = N'$ and in particular N is not abelian. Take any element a of N not in the centre of N , and put $z_1 = y_1a, z_2 = y_2, \dots, z_\beta = y_\beta$. We shall show that these elements do what is required. Firstly, $G = \langle z_1, \dots, z_\beta, G' \rangle$ since $a \in N' \leq G'$. Next, $[z_1, G]$ contains $[y_1a, x]$ for all x in N ; since $[y_1, x] \in U \cap N = 1$, this gives that $[z_1, G]$ contains $[a, x]$ for every x in N . Thus $[z_1, G]$ contains non-trivial elements of N , and so contains the whole of N . Finally, $[z_1, G]$ contains $[y_1a, u]$ for every u in G , that is, it contains $[y_1, u]^a[a, u]$. But $[a, u]$ is in N , and it follows that $[z_1, G]$ contains $[y_1, G]$. This is enough to show that $G' = \langle [z_1, G], \dots, [z_\beta, G] \rangle$, and so to complete the induction and the proof of the lemma.

Note that, in general, not every minimal generating set of G modulo G' has the property described in Lemma 3.1. For instance, if G is $A \times B$, where A

is abelian and B is perfect, then a minimal set of generators of A generates G modulo G' , minimally. Furthermore, the lemma fails for infinite groups in general even when the commutator quotient group is finite. A simple example is the direct product of a finite abelian group and infinitely many non-trivial perfect groups. I do not know what happens for finitely generated infinite groups in general; however, the reader will have no difficulty in proving the following result for soluble groups:

LEMMA 3.2. *Let G be a soluble group, and X any generating set whatever of G modulo G' . Then $G' = \langle [x, G] : x \in X \rangle$.*

LEMMA 3.3. *Let G be a finite group, or a finitely generated soluble group such that $d(G/G') = \beta \geq 1$. Then for all integers $n \geq 1$, $d(G^{n+1}) \leq d(G^n) + \beta$.*

PROOF. For convenience we shall write the elements of direct powers as sequences. Suppose that G^n is generated by the r elements

$$(3.4) \quad (a_{11}, a_{12}, \dots, a_{1n}), \dots, (a_{r1}, a_{r2}, \dots, a_{rn}).$$

We shall show that G^{n+1} is generated by the $r + \beta$ elements

$$(3.5) \quad (a_{11}, \dots, a_{1n}, a_{11}), \dots, (a_{r1}, \dots, a_{rn}, a_{r1})$$

and

$$(3.6) \quad (1, \dots, 1, z_1), \dots, (1, \dots, 1, z_\beta).$$

In this, (3.5) is obtained from (3.4) by simply repeating the first component of each sequence at the end, and z_1, \dots, z_β are generators of G modulo G' with the properties described in Lemmas 3.1 and 3.2. Let K be the subgroup of G^{n+1} generated by the elements in (3.5) and (3.6). Observe that $\{a_{11}, \dots, a_{r1}\}$ must be a generating set for G , since (3.4) generates G^n ; thus, by taking a suitable word in the elements (3.5), we can generate an element of G^{n+1} whose last component is any prescribed element x of G . The commutator of such an element with the i -th element of (3.6) is $(1, \dots, 1, [z_i, x])$. Since i, x are arbitrary, K therefore contains all elements of the form $(1, \dots, 1, u)$ with u in G' ; but G is generated by G' and z_1, \dots, z_β , so that K contains the whole of the last component of G^{n+1} . Thus K contains $(a_{11}, \dots, a_{1n}, 1), \dots, (a_{r1}, \dots, a_{rn}, 1)$, and so it contains the ‘‘initial segment’’ G^n of G^{n+1} . Thus $K = G^{n+1}$, as claimed.

We can now state the main result of this section.

THEOREM 3.4. *Let G be a finite group, or a finitely generated soluble group, such that $d(G/G') = \beta \geq 1$. Put $d(G) = \alpha$. Then there exists an integer k , $0 \leq k \leq \alpha - \beta$, and a positive integer f such that $d(G^n) = \beta n + k$ for $n \geq f$*

PROOF. Lemmas 3.3 and 2.2 combine to give that

$$\beta n \leq d(G^n) \leq \beta n + (\alpha - \beta)$$

for all $n \geq 1$. Therefore there exists k , $0 \leq k \leq \alpha - \beta$, such that $d(G^n) > \beta n + k - 1$ for all n , but $d(G_f) = \beta f + k$ for some f . Since $d(G^{n+1}) \leq d(G^n) + \beta$ for all n , we must have that $d(G^n) \leq \beta n + k$ for all $n \geq f$; and the choice of k, f gives the answer.

Although this theorem says that the growth sequence of an imperfect group cannot be too wild, it is incomplete in a number of ways. Firstly, can every k between 0 and $\alpha - \beta$ actually occur? The only examples I have been able to find have $l = 0$, and this might indeed reflect a general truth.* Secondly, how long can growth sequences take before settling down linearity? Examples in §5 show that they can take quite long over this, though it seems possible that the smallest f satisfying Theorem 3.4 depends on α, β rather than on G itself (except insofar as α, β depend on G , of course).

4. The perfect case

For finite perfect groups we have no analogue of Lemma 3.1 to help us, and a completely different approach is necessary. In fact a crude application of the elegant results in [2] is the key here, and we begin with a brief description of some basic points from that article.

For any finite group G , let $\phi(m, G)$ denote the number of m -bases of G , that is, ordered m -tuplets (x_1, \dots, x_m) of elements of G that generate G ; this is to include the case $m < d(G)$, when $\phi(m, G) = 0$. Two m -bases are *equivalent* if there is an automorphism of G taking one to the other, preserving order. This defines an equivalence relation, and the number $h(m, G)$ of equivalence classes is $\frac{1}{|\text{Aut } G|} \phi(m, G)$, since $\text{Aut } G$ permutes the m -bases regularly. From the definition, $h(m, G)$ is also the number of normal subgroups D of the absolutely free group F rank m such that $F/D \cong G$. Suppose that $d(G) \leq m$, so that G is an epimorphic image of F , and let I stand for the intersection of all the normal subgroups D with the property just mentioned. Then there is a natural monomorphism

$$F/I \hookrightarrow \prod^{\times} F/D \cong G^{h(m, G)}$$

which is an epimorphism if G is non-abelian and simple. Thus in this case, $d(G^{h(m, G)}) \leq m$, whereas $d(G^{h(m, G)+1}) \geq m + 1$. In fact it is straightforward to verify the following result:

4.1. *For every finite non-abelian simple group G , and every integer $m \geq d(G)$, $h(m, G) = \max\{n : d(G^n) = m\}$.*

In other words, the eventual behaviour of the growth sequence of G is deter-

* I understand from the referee that K. W. Gruenberg has shown that k is in fact zero for a certain class of finite imperfect groups including all soluble groups.

mined by that of the sequence $\{h(m, G)\}$ in this case. (What a pity that we do not know for sure that $d(G) = 2!$) This behaviour is revealed by the following theorem.

4.2. (Hall [2]). *For every finite group G and every integer $m \geq 1$,*

$$(4.3) \quad |\text{Aut } G| h(m, G) = \sum \mu(H) |H|^m.$$

Here the sum is taken all subgroups of G , and μ is the Möbius function of G given by the rules: $\mu(G) = 1$, and $\sum_{H \leq K} \mu(K) = 0$ for every proper subgroup H of G .

This result ties the growth sequence of a non-abelian simple group firmly to its lattice of subgroups, and it enables us to say with considerable accuracy what $d(G^n)$ is in terms of n , for large enough n . One wonders, incidentally, whether equation (4.3) could be used to prove that $h(2, G) \neq 0$, and hence that $d(G) = 2$, for finite non-abelian simple G .

For the next little while, G will stand for a finite non-abelian simple group, $h(m)$ for $h(m, G)$, a for $|\text{Aut } G|$, and $\varepsilon(m)$ for $\sum_{H \neq G} \mu(H) |G:H|^{-m}$. Note that $\varepsilon(m) \rightarrow 0$ as $m \rightarrow \infty$, since it is a finite sum of parts tending to zero. Then $h(m) \leq n \leq h(m + 1)$ if and only if

$$|G|^m (1 + \varepsilon(m)) \leq an \leq |G|^{m+1} (1 + \varepsilon(m + 1)).$$

Whenever $m \geq d(G)$, so that $1 + \varepsilon(m) > 0$, these inequalities are equivalent to

$$m + \sigma(m) - \delta \leq \log_{|G|} n \leq m + 1 + \sigma(m + 1) - \delta,$$

where now $\sigma(m) = \log_{|G|} (1 + \varepsilon(m))$ and $\delta = \log_{|G|} a$. Putting all this together, and keeping notation fixed, we can state:

4.4. *For any finite non-abelian simple group G ,*

$$\log_{|G|} n - 1 - \sigma(m + 1) + \delta \leq d(G^n) \leq \log_{|G|} n + 1 - \sigma(m) + \delta,$$

provided that $m \geq d(G)$ and $h(m) \leq n \leq h(m + 1)$.

The reader is warned that $\sigma(m)$, δ and $h(m)$ depend on G . Since m, n tend to infinity together, $\sigma(m)$ and $\sigma(m + 1)$ are eventually small enough to have little influence on the size of $d(G^n)$, and 4.4 forces it to take one of two or three values near $\log_{|G|} n + \delta$. In fact δ is often very small as well, very small indeed for simple groups that I know anything about; but even if not, we have justified the claim made in § 2 that Theorem 2.1 is near the truth for simple groups.

In the next theorem I have not been at pains to derive the best possible answers. One can easily give better variants, but they are somewhat less straightforward to state and prove; and certainly the loss in accuracy is more than outweighed by the gain in simplicity. I shall make one or two comments to this after the proof.

In the theorem, $\lambda(G)$ denotes the composition length of G .

THEOREM 4.5. *Let G be a non-trivial finite perfect group. Then $d(G^n) \leq \lambda(G)\log_2 n$ for all large enough n .*

PROOF. Induct on $|G|$. For simple groups, the result follows swiftly from 4.4. Suppose that G is not simple and that the theorem is true for smaller groups than G , and let N be a minimal normal subgroup of G . We shall consider the obvious power N^n of N inside G^n . Two cases arise:

1. *N is abelian.* If N is central in G , then N^n is central in G^n , and so is in the Frattini subgroup of G^n since G^n is perfect. Thus $d(G^n) = d(G^n/N^n)$, which by induction is eventually bounded by $\lambda(G/N)\log_2 n$. Since $\lambda(G/N) < \lambda(G)$, this is more than enough to satisfy us. If N is not central, then $N = [x, G]$ for any non-trivial x in N . A simple calculation shows that N^n is the normal closure in G^n of the element y whose components are all equal to x ; thus as N^n is abelian, G^n is generated by y and any generating set of G^n modulo N^n . Thus by induction $d(G^n) \leq 1 + \lambda(G/N)\log_2 n$ for large enough n , so that $d(G^n) \leq \lambda(G)\log_2 n$ for large enough n .

2. *N is not abelian.* Then N is perfect, and we have that $d(N^n) \leq \lambda(N)\log_2 n$, as well as $d(G^n/N^n) \leq \lambda(G/N)\log_2 n$, both for large enough n . Thus, as $d(G^n) \leq d(N^n) + d(G^n/N^n)$, it follows that $d(G^n) \leq (\lambda(G/N) + \lambda(N))\log_2 n = \lambda(G)\log_2 n$ for large enough n . This completes the induction.

The reader will observe that the only properties required of the function λ are that the inequality $d(G^n) \leq \lambda(G)\log_2 n$ should be almost always true for every non-abelian simple G , and that $\lambda(K/N) + \lambda(N) \leq \lambda(K)$ whenever K, N are perfect groups, N normal in K . It is quite evident that there are smaller functions with these properties: $\frac{1}{3}\lambda$, for example. However, to get much better answers will probably require a less simpleminded approach than the one I have adopted. I would imagine that for any perfect G , $d(G^n)$ is usually much smaller than $\log_2 n$, though this does not seem easy to prove.

5. Examples

Hall's Theorem 4.2 gives full details of the behaviour of growth sequences for simple groups, once the minimum number of generators and the Möbius function are known. The growth is quite astonishingly slow: for instance, $A_5^{6,464,040}$ needs only five generators!! It is this slow growth, which is shared by all perfect groups, as we have seen, that enables us to give examples of initial bad behaviour in the imperfect case. First a simple lemma:

LEMMA 5.1. *Let A, B be finitely generated abelian and perfect groups respectively. Then $d(A \times B) = \max(d(A), d(B))$.*

PROOF. It is clear that $d(A \times B) \geq d(A), d(B)$. Set $m = \max(d(A), d(B))$. Then, supplementing a minimal generating set of one or other of these groups with dummy generators if necessary, we get generating sets $\{a_1, \dots, a_m\}$ for A and $\{b_1, \dots, b_m\}$ for B . It is easy to check that $a_1 b_1, \dots, a_m b_m$ generate $A \times B$. For, if X is the subgroup they generate, then X contains all commutators $[b_i, b_i]^b$, with b in B , since A is central. But these commutators generate $B' = B$ so that $X \geq B$. Thus $X \geq A$ as well, and so $X = A \times B$, as claimed.

Roughly speaking, we use this lemma as follows. Let K be a finite non-abelian simple group, and set $h(k, K) = h(k)$ for short; and let A be a non-trivial finite abelian group, say $d(A) = \beta$. Put $G = K^{h(k)} \times A$. Then the lemma says that $d(G^n) = \max(d(K^{h(k)n}), \beta n)$ for all n . That is, as long as k is large, the growth sequence of G is like that of $K^{h(k)}$ for a long time, with many long stretches of being constant; but eventually it becomes arithmetic with common difference β . The details, which unfortunately are a bit messy, go like this:

THEOREM 5.2. *Let β be a positive integer, k an integer not less than $\max(2, \beta)$, A a finite abelian group such that $d(A) = \beta$, and K a finite non-abelian simple group such that $k \geq d(K)$. For $i \geq 0$, set $l(i)$ for the integer part of $h(k + i)/h(k)$, where we have set $h(j, K) = h(j)$ for short. Assume that $l(i + 1) > l(i)$ for each i . Then*

(i) *for each i , $d(K^{h(k)l(i)}) = k + i$, $d(K^{h(k)(l(i)+1)}) = k + i + 1$. Further, let t be the smallest non-negative integer such that $l(t)\beta > k + t$, and s the largest non-negative integer such that $(l(t - 1) + s)\beta \leq k + t$. Then*

(ii) $s < l(t) - l(t - 1)$.

Finally, set $G = K^{h(k)} \times A$. Then

(iii) $d(G) = k$, $d(G/G') = \beta$,

(iv) $d(G^{l(t-1)+1}) = d(G^{l(i)}) = k + i$ for $1 \leq i \leq t - 1$,

(v) $d(G^n) = k + t$ for $l(t - 1) + 1 \leq n \leq l(t - 1) + s$,

(vi) $d(G^n) = \beta n$ for $n > l(t - 1) + s$.

PROOF. The first claim follow from 4.1 since $h(k)l(i) \leq h(k + i)$ and $h(k + i + 1) \geq h(k)(l(i) + 1) > h(k + i)$.

Clearly, $t \geq 1$ since $l(0) = 1$ and $\beta \leq k$. It could perhaps happen that $t = 1$, in which case (iv) is vacuous; otherwise, for $l(i - 1) + 1 \leq n \leq l(i)$, $1 \leq i \leq t - 1$, we get from Lemma 5.1 and (i) that $d(G^n) = (d(K^{h(k)n}), \beta n) = k + i$.

Statement (ii) is obvious from the definitions of s and t , while (iii) is clear. Statement (v) follows from the definitions and Lemma 5.1; note that it is vacuous if $s = 0$. Finally, it is readily checked that $n\beta \geq k + n$ whenever $n > l(t - 1) + s$, and Lemma 5.1 then gives (vi).

As far as I know all simple groups satisfy the condition that $l(i + 1) > l(i)$; it is certainly true for almost all i , since $l(i + 1)/l(i) \rightarrow |K|$ as $i \rightarrow \infty$. To prove that the inequality is true in all cases would require a more detailed examination of the

Möbius function than is worthwhile in this context. Suffice it to say that there are simple groups that satisfy it ; small alternating groups, and $PSL(2, 7)$, for instance.

By taking k large enough in comparison with β , one can make t as large as desired, so that the growth sequence begins as a “step function” with as many steps as desired. However, the examples given by the theorem are rather schizophrenic, and it may be that a group that does not split as a central product of a non-trivial perfect group and a nilpotent group must have a pleasanter growth sequence. All other examples that I have looked at are very well-behaved indeed. For example, any group G generated by f (let us say) elements of mutually coprime orders satisfies $d(G^n) = n$ for $n \geq f$, provided that it is not perfect; and this yields fairly quickly that $d(S_r^n) = n$ for $n \geq 2$, S_r being the symmetric group of degree $r \geq 2$.

NOTE ADDED IN PROOF:

“Many of the problems posed in this paper have now been solved. The constant k in Theorem 3.4 is always zero. For $\beta \geq 2$ the theorem works with $f = \frac{\alpha - 1}{\beta - 1}$, and for $\beta = 1$ with $f = 2\alpha + 1$. Examples show that these values are reasonably near the truth. The conjecture at the end of Section 3 is patently false, and is not what I intended to convey. Finally the conjecture at the end of Section 4 is substantially correct; for perfect G , $d(G^n)$ is eventually less than $\log_2 n$.”

References

- [1] I. M. S. Dey, ‘Embeddings in non-Hopf groups’, *J. London Math. Soc.* (2) 1 (1969), 745–749.
- [2] P. Hall, ‘The Eulerian functions of a group’, *Quart. J. Math. (Oxford)* 7 (1936), 134–151.
- [3] B. H. Neumann, ‘Identical relations in groups I’, *Math. Ann.* 114 (1937), 506–525.
- [4] Hanna Neumann, *Varieties of groups* (Ergebnisse der Mathematik and ihrer Grenzgebiete, 37, 1967).
- [5] J. M. Tyrer-Jones. ‘Direct products and the Hopf property’, *J. Austral. Math. Soc.* 17 (1974), 174–196.

University College
Cardiff, U. K.