AN IMPROVED BOUND FOR BFC p-GROUPS

PETER M. NEUMANN

To my father for his 60th birthday, with love

(Received 2 May 1969)

1. Theme and first variation

The theme of this paper is a conjecture whose origins go back to work of B. H. Neumann ([5], Theorem 3.1) and his former students J. Wiegold and I. D. Macdonald ([7], [4]). B. H. Neumann proved that if there is a bound to the sizes of conjugacy classes in the group G, that is, if G is a BFC group, then the derived group G' is finite; Wiegold, and later Macdonald, produced explicit upper bounds for $|G'|$ in terms of the maximum n of the sizes of the conjugacy classes in G. The conjecture is that

$$|G'| \leqq n^{\frac{1}{2}(l(n)+1)}$$

where $l(n)$ should be the arithmetic function [1] $\lambda(n)$ for a best possible bound, or $l(n)$ may be interpreted as $\log_2 n$ for a smooth, monotonic order-of-magnitude estimate. However, the bounds produced in [7] and [4], and even the vastly better upper bounds proved by Shepperd and Wiegold [6] for soluble groups, are very much bigger than $n^{\frac{1}{2}(l(n)+1)}$, and it is my aim in this paper to take a first step towards closing the gap. This first step is a study of BFC p-groups: in a sequel I hope to show how the results proved here can be used to obtain improved bounds for arbitrary BFC groups.

The *breadth* b of a finite p-group G is defined by

$$p^b = \max\{|G : C(g)|\,|g \in G\}$$

where $C(g)$ is the centraliser of g in G. Equivalently, p^b is the maximum of the sizes of the conjugacy classes in G. For p-groups the basic conjecture takes the form

CONJECTURE A. *If G is a finite p-group of breadth b, then*

$$|G'| \leqq p^{\frac{1}{2}b(b+1)}.$$

What I shall prove is

[1] If $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ where $p_1, p_2, \ldots, p_k$ are prime, then $\lambda(n) = \alpha_1+\alpha_2\cdots+\alpha_k$.

THEOREM 1. *If G is a finite p-group of breadth b, then*

$$|G'| \leqq p^{b^2}.$$

By completely different methods I. M. Bride has shown that Conjecture A is correct for p-groups of class 2 (see [1]), but even for this special case his proof is long and difficult. It seems a good possibility that a combination of his methods and the methods to be described below will produce a proof of the conjecture, but certainly the splicing of the two lines of approach cannot be altogether straightforward.

There is [2], as is well known, a strong similarity between groups and Lie algebras (or Lie rings). It is not easy to pin down precisely what this analogy entails. At its most concrete it is embodied in the classical relation between a finite dimensional Lie group and its local Lie algebra; or it is the formal connection obtained by associating with a residually nilpotent group one of its associated graded Lie rings (cf. Lazard [2]). At its most insubstantial it is perhaps simply a similarity between the category of groups and the category of Lie algebras. However, for the quantitative problem in which we are interested the similarity can be formulated quite explicitly.

Generally the analogy seems to arise from the formal similarity between the operation of forming commutators (and multiplication) in groups and the operation of multiplication (and addition respectively) in Lie algebras. Thus the property of being abelian as a group (all commutators trivial) corresponds to the property of being abelian as a Lie algebra (all products zero); the derived group (the minimal normal subgroup with abelian factor group) should correspond to the derived algebra in a Lie algebra; the fact that the derived group G' in a group G is generated by all commutators $[x, y] = x^{-1}y^{-1}xy$, $x, y \in G$, corresponds to the fact that the derived algebra L^2 is spanned by the products xy of pairs of elements x, y in a Lie algebra L; centralisers in a group $(C_G(x) = \{y \in G | [x, y] = 1\})$ should correspond to annihilators in a Lie algebra $(\mathrm{ann}_L(x) = \{y \in L | xy = 0\})$. Clearly nilpotence and solubility will correspond as they ought (see, for example, [3] § 4 for a general setting in this case). There is less justification for making the number of prime factors in the order of a group correspond to the dimension of a Lie algebra, but at least for a soluble group G and a soluble Lie algebra L, $\lambda(|G|)$ and $\dim L$ are the lengths of composition series in G and L respectively. It is a little harder still to justify the correspondence between the number of prime factors in the index of a subgroup and the codimension of a Lie subalgebra: but at least in the nilpotent case, $\lambda(|G : H|)$ is the length of a composition series between G and its subgroup H, while

[2] In what follows groups will be assumed to be finite, and Lie algebras will be finite dimensional over some (unspecified) field. This restriction is for convenience only. It entails no real loss, for the problems we are concerned with can quite easily be reduced to the study of finite or finite dimensional cases (see, for example, [4] § 2).

codim M is the length of a composition series between the Lie algebra L and its subalgebra M.

These considerations suggested the following definition and conjecture. If L is a Lie algebra, we define the *breadth* b of L by

$$b = \max \{\text{codim ann } (x) | x \in L\}.$$

Then

CONJECTURE B. *In any Lie algebra L of breadth b,*

$$\dim L^2 \leqq \tfrac{1}{2}b(b+1).$$

In this direction the analogue of Theorem 1 is

THEOREM 2. *In any Lie algebra L of breadth b,*

$$\dim L^2 \leqq b^2.$$

The problem is now ripe for generalisation: and indeed, it is only by generalising from Lie multiplication to arbitrary bilinear maps, thereby introducing the possibility of unsymmetry into the situation, that we get a proof of Theorem 2; and it is only by generalising still further, almost to breaking point, that we finally come full circle and obtain a proof of Theorem 1.

2. Second variation: bilinear algebra

Let U, V and W be vector spaces (over some field which will remain unspecified) and let $\phi : U \times V \to W$ be a bilinear map. For $u \in U$ define

$$\text{ann}_\phi(u) = \{v \in V | (u, v)\phi = 0\} \leqq V$$

and for $v \in V$

$$\text{ann}_\phi(v) = \{u \in U | (u, v)\phi = 0\} \leqq U.$$

If $(u, V)\phi = \{(u, v)\phi | v \in V\}$ then $(u, V)\phi$ is a linear subspace of W, and of course $(u, V)\phi \cong V/\text{ann}_\phi(u)$. We put

$$b(u) = b_\phi(u) = \text{codim } (\text{ann}_\phi(u)) = \dim (u, V)\phi$$

and for $v \in V$ we define $b(v) = b_\phi(v)$ analogously. The basic result, of which Theorem 2 is clearly only a very special case, is

THEOREM 2.1. *If ϕ: $U \times V \to W$ is a bilinear map and k, l are integers such that*

(a) *for all $u \in U$, $b(u) \leqq k$;*

(b) *for all $v \in V$, $b(v) \leqq l$;*

then [3]

$$\dim \langle \text{im } \phi \rangle \leqq kl.$$

[3] Throughout, $\langle X \rangle$ denotes the subspace spanned by the set X.

https://doi.org/10.1017/S1446788700005917 Published online by Cambridge University Press

For the proof we clearly may assume that $k \leqq l$. If $k = 0$ then $(u, v)\phi = 0$ for all $u \in U$ and all $v \in V$, so that $\operatorname{im} \phi = \{0\}$, and the result is surely true in this case. This provides the start of an induction: as inductive hypothesis we assume that the statement is true for the given value of l and all smaller values of k.

If $b(u) \leqq k-1$ for all $u \in U$ then our inductive hypothesis applies and

$$\dim \langle \operatorname{im} \phi \rangle \leqq (k-1)l \leqq kl.$$

Therefore we may assume that there is an element u_1 in U for which $b(u_1) = k$ and we put

$$X = \operatorname{ann}_\phi(u_1) \leqq V$$

and

$$Y = \operatorname{ann}_\phi(X) \leqq U.$$

Let $\psi_1 : W \to W/(u_1, V)\phi = W_1$ be the canonic epimorphism, and define ϕ_1 to be the composite map $\phi_1 = \phi\psi_1 : U \times V \to W_1$. Thus ϕ_1 is bilinear and $\operatorname{ann}_{\phi_1}(u) = V$. Now we need

LEMMA 2.2. *If $u \in U$, $u \notin Y$ then $b_{\phi_1}(u) \leqq k-1$.*

PROOF. If $u \notin Y$ then there is some element x in X for which $(u, x)\phi \neq 0$. Then

$$(u, x)\phi = (u+u_1, x)\phi \neq 0. \tag{2.3}$$

Let us put $U^* = \langle u, u_1 \rangle = \langle u, u+u_1 \rangle$, and $T = \langle (U^*, V)\phi \rangle$, so that

$$\begin{aligned} T &= (u, V)\phi + (u_1, V)\phi \\ &= (u, V)\phi + (u+u_1, V)\phi. \end{aligned} \tag{2.4}$$

In the second line of (2.4) we have T expressed as the sum of two subspaces each of dimension k or less and which have (by (2.3)) non-zero intersection. Thus $\dim T \leqq 2k-1$. But $\dim (u_1, V)\phi = b_\phi(u_1) = k$. Hence

$$\begin{aligned} b_{\phi_1}(u) &= \dim\, (u, V)\phi_1 \\ &= \dim\, (u, V)\phi\psi_1 \\ &= \dim\, \{((u, V)\phi + (u_1, V)\phi)/(u_1, V)\phi\} \\ &= \dim\, \{T/(u_1, V)\phi\} \leqq k-1. \end{aligned}$$

This lemma provides the first step of an induction: the later steps are a little different. We intend to find elements $u_1, \ldots, u_r$ in U with certain special properties. To define these elements and describe their properties we will need some more notation. Suppose that $u_1, \ldots, u_i$ are defined. We will put

$$U_i = \langle u_1, \ldots, u_i \rangle \leqq U,$$

and

$$S_i = \langle (U_i, V)\phi \rangle \leqq W.$$

Since ϕ is bilinear, S_i is the sum of its subspaces $(u_1, V)\phi, \ldots, (u_i, V)\phi$ each of which has dimension k or less: hence

$$\dim S_i \leqq ik. \tag{2.5}$$

Let $\psi_i : W \to W/S_i = W_i$ be the canonic epimorphism, and put

$$\phi_i = \phi\psi_i : U \times V \to W_i.$$

Then of course ϕ_i is bilinear, and since $S_i = \ker \psi_i \leqq \langle \operatorname{im} \phi \rangle$, we have

$$\dim \langle \operatorname{im} \phi \rangle = \dim \langle \operatorname{im} \phi_i \rangle + \dim S_i \tag{2.6}$$

Notice that, if $\theta_i : W_{i-1} \to W_i$ is the canonic epimorphism with kernel S_i/S_{i-1}, then $\phi_i = \phi_{i-1}\theta_i$ and

$$\ker \theta_i = S_i/S_{i-1} = (u_i, V)\phi_{i-1}. \tag{2.7}$$

The conditions that are to be satisfied in the choice of the elements $u_1, \ldots, u_r$ are that for $1 \leqq i \leqq r$,

(a) $U_i \leqq Y$;

(b) $b_{\phi_i}(u) \leqq k-i$ for all $u \in U-Y$.

The choice of u_1 is already made: that (a) holds for $i = 1$ is in the definition of Y; and (b) is the content of Lemma 2.2. Suppose therefore that $i \geqq 1$ and that $u_1, \ldots, u_i$ are already chosen. If $i = k$ we put $r = k$ and CALL A HALT. If $i < k$ and $b_{\phi_i}(u) \leqq k-i$ for all $u \in Y$, then we put $r = i$ and CALL A HALT. Otherwise, let u_{i+1} be any element of Y such that $b_{\phi_i}(u_{i+1}) \geqq k-i+1$. Condition (a) is then automatically satisfied by U_{i+1}, and only (b) needs discussion. If $u \notin Y$ then also $u+u_{i+1} \notin Y$ and we do know that

$$\begin{aligned} \dim (u, V)\phi_i &\leqq k-i \\ \dim (u+u_{i+1}, V)\phi_i &\leqq k-i; \end{aligned} \tag{2.8}$$

while on the other hand

$$\dim (u_{i+1}, V)\phi_i \geqq k-i+1 \tag{2.9}$$

If $U^* = \langle u, u_{i+1} \rangle = \langle u, u+u_{i+1} \rangle$ then, since ϕ_i is bilinear,

$$\begin{aligned} \langle (U^*, V)\phi_i \rangle &= (u, V)\phi_i + (u_{i+1}, V)\phi_i \\ &= (u, V)\phi_i + (u+u_{i+1}, V)\phi_i \end{aligned} \tag{2.10}$$

https://doi.org/10.1017/S1446788700005917 Published online by Cambridge University Press

The second line in (2.10) coupled with (2.8) shows that $(u, V)\phi_i$ has codimension at most $k-i$ in $\langle (U^*, V)\phi_i \rangle$. Then the first line of (2.10) coupled with (2.9) shows that

$$(u, V)\phi_i \cap (u_{i+1}, V)\phi_i \neq 0.$$

Thus $(u, V)\phi_i$ has non-zero intersection with the kernel of θ_{i+1} (see (2.7)), so that

$$\dim (u, V)\phi_i\theta_{i+1} < \dim (u, V)\phi_i \leqq k-i.$$

That is $b_{\phi_{i+1}}(u) \leqq k-i-1$, and this is the required inequality.

The last stage of the proof uses the information which we have acquired with the elements $u_1, \ldots, u_r$. There are two cases to consider, corresponding to the two possible reasons for having called a halt on the preceding page.

CASE 1. If $r < k$ then we stopped simply because $b_{\phi_r}(u) \leqq k-r$ for all $u \in Y$. By (b) this inequality also holds for all $u \notin Y$: thus $b_{\phi_r}(u) \leqq k-r$ for all $u \in U$.

Now certainly $k-r < k$, and furthermore, if $v \in V$ then

$$b_{\phi_r}(v) \leqq b_{\phi}(v) \leqq l.$$

Therefore our inductive hypothesis applies,

$$\dim \langle \operatorname{im} \phi_r \rangle \leqq (k-r)l,$$

and (2.5), (2.6) give

$$\begin{aligned} \dim \langle \operatorname{im} \phi \rangle &\leqq (k-r)l+rk \\ &\leqq (k-r)l+rl = kl. \end{aligned}$$

CASE 2. If $r = k$ then for all $u \notin Y$, $(u, V)\phi_k = 0$. This means that for $u \notin Y$,

$$(u, V)\phi \leqq \langle (U_k, V)\phi \rangle \leqq \langle (Y, V)\phi \rangle,$$

and so $\langle (U, V)\phi \rangle = \langle (Y, V)\phi \rangle$. If $v_1, v_2, \ldots, v_k$ together with X span V, then

$$\begin{aligned} \langle \operatorname{im} \phi \rangle &= \langle (Y, V)\phi \rangle \\ &= (Y, v_1)\phi + (Y, v_2)\phi + \ldots + (Y, v_k)\phi + \langle (Y, X)\phi \rangle. \end{aligned}$$

Each of the first k summands has dimension at most l, and the last summand is zero by definition of Y. Thus in this case also, $\dim \langle \operatorname{im} \phi \rangle \leqq kl$, and the proof of Theorem 2.1 is complete.

A better bound than that given in Theorem 2.1 can certainly not be produced. For, if we take U to be a vector space of dimension l, V to be a space of dimension k, W the tensor product $U \otimes V$, and $\phi : U \times V \to U \otimes V$ the canonical bilinear map, then $\langle \operatorname{im} \phi \rangle = W$ and so in this case $\dim \langle \operatorname{im} \phi \rangle = kl$. Therefore further progress towards a proof of Conjecture B must necessarily use more than just the bilinear property of multiplication in a Lie algebra. It looks very likely that the following is true:

CONJECTURE B#. *If $\phi : U \times U \to W$ is an alternating*[4] *bilinear map and if $b(u) \leqq b$ for all $u \in U$, then*

$$\dim \langle \operatorname{im} \phi \rangle \leqq \tfrac{1}{2}b(b+1).$$

Probably a preliminary for an understanding of this conjecture should be a more symmetrical proof of Theorem 2.1. However, the last part of the present paper is devoted to exploiting the unsymmetry in the given proof.

3. Further variations and a proof of Theorem 1

The linear algebra described in § 2 is capable of generalisation in several ways. First, let R be a commutative ring with unit element, and replace vector spaces by R-modules and dimension[5] by composition length. The corresponding generalisation of Theorem 2.1 still holds, and the proof given in § 2 needs only trivial grammatical adjustment. Next, observe that the proof requires of V only that $k \leqq l$ and that V is spanned by elements of breadth at most l. Incorporating this fact also, and making the necessary verbal changes at the end of the proof, we get

LEMMA 3.1. *Let U, V, W be modules over the ring R, let $\phi : U \times V \to W$ be a bilinear map, and suppose that k, l are integers snch that $k \leqq l$ and*

(i) *for all $u \in U$, $b_\phi(u) \leqq k$;*

(ii) *$\{v \in V | b_\phi(v) \leqq l\}$ spans V.*

Then
$$d(\langle \operatorname{im} \phi \rangle) \leqq kl,$$
where $d(X)$ denotes the composition length of the R-module X.

We shall apply the lemma in the case where $R = \boldsymbol{Z}$, the ring of integers, and U, V, W are finite abelian p-groups. Notice that, if X is an abelian group of order p^m, then m is the composition length of X as $\boldsymbol{Z}$-module. Our variations now return to their starting point with the

PROOF OF THEOREM 1. Let G be a finite p-group of breadth b. If c is the nilpotency class of G, then the lower central series is

$$G = \gamma_1 > \gamma_2 > \ldots > \gamma_c > \gamma_{c+1} = 1,$$

[4] That is, $(u, u)\phi = 0$ for all $u \in U$. An alternating bilinear map is antisymmetric, $(u, v)\phi = -(v, u)\phi$ for all $u, v \in U$. The converse holds unless the characteristic of the underlying field is 2.

[5] Codimension of the submodule B in A becomes composition length of the factor module A/B.

https://doi.org/10.1017/S1446788700005917 Published online by Cambridge University Press

where $\gamma_{i+1} = [G, \gamma_i]$ for $i \geqq 1$. Now put

$$
\begin{aligned}
U &= G/G' \\
V_i &= \gamma_i/\gamma_{i+1} \qquad\qquad 1 \leqq i \leqq c \\
V &= V_1 \oplus V_2 \oplus \ldots \oplus V_c
\end{aligned}
$$

and

$$W = V_2 \oplus \ldots \oplus V_c.$$

Then U, V, W are finite abelian p-groups, and $|W| = |G'|$. Commutation in G can be used to define a bilinear map $\phi : U \times V \to W$ in the following way. If $g \in G$, $h \in \gamma_i$ then $[g, h] \in \gamma_{i+1}$, and we define

$$(gG', h\gamma_{i+1})\phi = [g, h]\gamma_{i+2} \in V_{i+1} \leqq W$$

It is easy to prove (and well known) that this definition is unambiguous and defines ϕ as a bilinear map, (see, for example, [2]) and we extend to a map on $U \times V$ to W by linearity. Furthermore, from the definition of γ_{i+1} we see that $V_{i+1} = \langle (U, V_i)\phi \rangle$, so that $\langle \operatorname{im} \phi \rangle = W$. Two more facts complete the picture:

(3.2) if $u \in U$ then $b_\phi(u) \leqq b$;

(3.3) if $v \in V_i$ then $b_\phi(v) \leqq b$.

To prove (3.2) let $u = gG'$, $g \in G$ and let $C = C_G(g)$. Then, by our original hypothesis, $|G : C| \leqq p^b$. Now

$$
\begin{aligned}
\operatorname{ann}_\phi(u) &\geqq \sum_{i=1}^{c} (V_i \cap \operatorname{ann}_\phi(u)) \\
&\geqq \sum_{i=1}^{c} (C \cap \gamma_i)\gamma_{i+1}/\gamma_{i+1},
\end{aligned}
$$

and so

$$
\begin{aligned}
|V : \operatorname{ann}_\phi(u)| &\leqq \prod_{i=1}^{c} |V_i : (C \cap \gamma_i)\gamma_{i+1}/\gamma_{i+1}| \\
&= \prod_{i=1}^{c} |\gamma_i : (C \cap \gamma_i)\gamma_{i+1}| \\
&= |\gamma_1 : C| \leqq p^b.
\end{aligned}
$$

That is, $b_\phi(u) \leqq b$.

The proof of (3.3) is even simpler. If $v \in V_i$, say $v = h\gamma_{i+1}$ with $h \in \gamma_i$, and if $C_G(h) = C$, then

$$|U : \operatorname{ann}_\phi(v)| \leqq |U : CG'/G'| = |G : CG'| \leqq |G : C| \leqq p^b,$$

so that $b_\phi(v) \leqq b$ as required.

Now we apply Lemma 3.1 to conclude that $|\langle \operatorname{im} \phi \rangle| \leqq p^{b^2}$, that is,

$$|G'| = |W| \leqq p^{b^2}$$

and the proof of Theorem 1 is complete.

References

[1] I. M. Bride, Ph. D. Thesis, University of Manchester Institute of Science and Technology, 1968. *See also:* 'Second nilpotent BFC groups', *J. Australian Math. Soc.* 11 (1970), 9—18.

[2] Michel Lazard, 'Sur les groupes nilpotents et les anneaux de Lie', *Ann. Sci. Ecole Norm. Sup.* (3) 71 (1954), 101—190.

[3] A. H. Livšic, M. S. Calenko, E. G. Šul'geifer, 'Varieties in categories', *Mat. Sb.* 63 (105) (1964), 554—581 = *Amer. Math. Soc. Translations* (*Series* 2) 58, 29—56.

[4] I. D. Macdonald, 'Some explicit bounds in groups with finite derived groups', *Proc. London Math. Soc.* (3) 11 (1961), 23—56.

[5] B. H. Neumann, 'Groups covered by permutable subsets', *J. London Math. Soc.* 29 (1954), 236—248.

[6] J. A. H. Shepperd and James Wiegold, 'Transitive permutation groups and groups with finite derived groups', *Math. Zeitschrift* 81 (1963), 279—285.

[7] J. Wiegold, 'Groups with boundedly finite classes of conjugate elements', *Proc. Roy. Soc.* (A) 238 (1957), 389—401.

The Queen's College
Oxford

https://doi.org/10.1017/S1446788700005917 Published online by Cambridge University Press