Proceedings of the Edinburgh Mathematical Society (1979), 22, 195–199 ©

GENERATORS FOR SUBGROUPS OF WREATH PRODUCTS

by J. A. HULSE
(Received 20th February 1978)

If G is a group, let

$$m(G)$$

be the least cardinal such that G may be generated by $m(G)$ elements, and let

$$m_s(G)$$

be the supremum of all $m(H)$ for subgroups H of G.

We are concerned with finding finite upper bounds for $m_s(G)$ for certain wreath products G and in some cases we calculate $m_s(G)$ precisely. For the definition of, and a general introduction to, wreath products see, for example, (3) p.p. 18–22.

Our first result is in answer to a question of Bowers, who uses it to prove his Tory Factor Theorem in (1), and I am grateful to him for bringing it to my attention.

Theorem A. *If p is a prime number and n is a positive integer, let*

$$W_{p,n}$$

denote the wreath product of n copies of a cyclic group of order p, taken in its right regular representation. Then

$$m_s(W_{p,n}) = p^{n-1}.$$

For convenience we define $W_{p,0}$ to be the trivial group. Since each $W_{p,n}$ is a permutation group of degree p^n, it follows that, for $n \geq 1$, the base group of $W_{p,n}$ considered as $W_{p,1}$ wr $W_{p,n-1}$, is an Abelian group of exponent p and rank p^{n-1} and so

$$m_s(W_{p,n}) \geq p^{n-1}.$$

We shall prove the reverse inequality by considering $W_{p,n}$ as $W_{p,n-1}$ wr $W_{p,1}$ and using induction on n. However, in order to make our induction agrument work we shall have to prove a little more about $W_{p,n}$ than $m_s(W_{p,n}) \leq p^{n-1}$.

If A is a group with $m_s(A) = m$ and C is a cyclic group of order p, then

$$m_s(A \text{ wr } C)$$

can be greater than pm. For example if $A = \langle a \rangle$ is cyclic of order 4 and $C = \langle c \rangle$ is cyclic of order 2 and $W = A$ wr C, then $m_s(A) = 1$ but $m_s(W) = 3$. If the base group of W is taken to be $A_1 \times A_c$, where $A_1 = \langle a_1 \rangle$ and $A_c = \langle a_c \rangle$, consider

$$H = \langle a_1^2, a_1 a_c, c \rangle = \{a_1^m a_c^n, a_1^m a_c^n c \mid m + n \equiv 0 (\text{mod } 2)\}.$$

Then the derived group, H', of H is

$$\langle a_1^2 a_c^2 \rangle$$

and H/H' has exponent 2 and order 8. Thus

$$m(H) \geqslant m(H/H') = 3$$

and so $m_s(W) \geqslant 3$. Since

$$1 \lhd A_1 \lhd A_1 \times A_c \lhd W$$

is a cyclic series for W it follows that $m_s(W) \leqslant 3$ and hence $m_s(W) = 3$.

If n and m are positive integers, let

$$\mathfrak{X}_{n,m}$$

denote the class of all groups G with $m_s(G) \leqslant m$ and such that whenever

$$H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n \leqslant G$$

then there exists $X \subseteq H_n$ with $|X| < nm$, where $|X|$ denotes the cardinal of X, and

$$\langle H_i \cap X \rangle = H_i$$

for $i = 1, 2, \ldots, n$.

We note that the second condition for $G \in \mathfrak{X}_{n,m}$ is almost implied by the first. Since if $m_s(G) \leqslant m$ and

$$H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n \leqslant G,$$

then there exist $X_i \subseteq H_i$ such that $|X_i| \leqslant m$ and $\langle X_i \rangle = H_i$ for $i = 1, 2, \ldots, n$. Thus if $X = X_1 \cup X_2 \cup \cdots \cup X_n$, then $|X| \leqslant nm$ and $\langle H_i \cap X \rangle = H_i$ for $i = 1, 2, \ldots, n$.

We see that if $m_s(G) < m$, then the above argument would show that $G \in \mathfrak{X}_{n,m}$ for any positive integer n. Also it is easy to show that $G \in \mathfrak{X}_{n,1}$ if and only if G is a finite cyclic group of composition length less than n.

Our main result is the following theorem.

Theorem B. *Let p be a prime number and m be a positive integer. If $A \in \mathfrak{X}_{p,m}$ and C is a cyclic group of order p, then*

$$A \text{ wr } C \in \mathfrak{X}_{p,pm}.$$

Since a cyclic group of order p lies in $\mathfrak{X}_{p,1}$, the following result may be deduced immediately by induction on n.

Theorem A*. *Let p be a prime number and n be a positive integer. Then*

$$W_{p,n} \in \mathfrak{X}_{p,p^{n-1}},$$

where $W_{p,n}$ is as in Theorem A.

We note that Theorem A* shows that

$$m_s(W_{p,n}) \leqslant p^{n-1}$$

and that we have already established the reverse inequality. Thus Theorem A follows from Theorem A*.

We remark here that the groups $W_{p,n}$ are of particular importance since $W_{p,n}$ is a Sylow p-subgroup of the symmetric group of degree p^n and Sylow p-subgroups of the symmetric groups of other finite degrees are formed by taking direct products of groups of the form $W_{p,n}$ (2) or (5). Also Vol'vačev (4) investigates the Sylow p-subgroups of linear groups over an arbitrary field and shows that they are direct products of groups of the form A wr $W_{p,n}$, where the group A is specified having degree 1, or, in the case $p = 2$, degree 2, over a suitable field. If $A \in \mathfrak{X}_{p,m}$, then Theorem B shows that A wr $W_{p,n} \in \mathfrak{X}_{p,p^n m}$ for all natural numbers n.

I should also remark that Dr. P. M. Neumann has independently obtained Theorem A by a different method in unpublished work.

We conclude with the proof of Theorem B and an example to show that the restriction that C have prime order is essential.

Proof of Theorem B. Let B be the base group of $W = A \text{ wr } C$ and $C = \langle c \rangle$. Then B is the direct product of p copies of A and we consider B as the group of all maps from $\{1, 2, \ldots, p\}$ to A. For $i = 0, 1, \ldots, p$, let

$$B_i = \{f \in B \mid f(j) = 1 \text{ for } j = i+1, \ldots, p\}.$$

Then $1 = B_0 \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_p = B$ and $B_i/B_{i-1} \cong A$ for $i = 1, \ldots, p$. If $i = 1, \ldots, p$, let $\pi_i : B \to A$ be given by

$$\pi_i : f \mapsto f(i)$$

for all $f \in B$; that is, let π_i be the projection of B onto its i-th coordinate.

Suppose now that $H \leqslant W$. If $H \leqslant B$, then $H \cap B_0 = 1$, $H \cap B_p = H$ and

$$(H \cap B_i)/(H \cap B_{i-1}) \cong B_{i-1}(H \cap B_i)/B_{i-1} \leqslant B_i/B_{i-1} \cong A$$

for $i = 1, \ldots, p$. Since $A \in \mathfrak{X}_{p,m}$, $m_s(A) \leqslant m$ and so

$$m[(H \cap B_i)/(H \cap B_{i-1})] \leqslant m.$$

Hence $m(H) \leqslant pm$. On the other hand if $H \not\leqslant B$, then, since W/B has prime order, it follows that $BH = W$ and so there exists $b \in B$ such that $bc \in H$. Then

$$H = \langle H \cap B, bc \rangle.$$

Now

$$(H \cap B_1)\pi_1 \trianglelefteq (H \cap B_2)\pi_1 \trianglelefteq \cdots \trianglelefteq (H \cap B_p)\pi_1 \leqslant A \in \mathfrak{X}_{p,m}$$

and so there exists $X \subseteq H \cap B_p$ such that $|X| < pm$ and

$$\langle X \cap B_i \rangle \pi_1 = (H \cap B_i)\pi_1$$

for $i = 1, \ldots, p$. We show by induction on i that

$$H \cap B_i \leqslant \langle X \cap B_i, bc \rangle$$

for $i = 0, \ldots, p$. Since $H \cap B_0 = 1$, the result is true for $i = 0$. Suppose now that $i > 0$

and

$$H \cap B_{i-1} \leq \langle X \cap B_{i-1}, bc \rangle.$$

If $h \in H \cap B_i$, then, since $(H \cap B_i)\pi_1 = \langle X \cap B_i \rangle \pi_1$,

$$(hf^{-1})\pi_1 = 1$$

for some $f \in \langle X \cap B_i \rangle$. But also $hf^{-1} \in H \cap B_i$ and so

$$hf^{-1} \in (H \cap B_{i-1})^{bc} \leq \langle X \cap B_{i-1}, bc \rangle.$$

Thus $h \in \langle X \cap B_i, bc \rangle$ and so

$$H \cap B_i \leq \langle X \cap B_i, bc \rangle$$

to complete the induction. Hence

$$H = \langle H \cap B, bc \rangle = \langle H \cap B_p, bc \rangle \leq \langle X \cap B_p, bc \rangle = \langle X, bc \rangle \leq H.$$

Since $|X| < pm$, it follows that $m(H) \leq pm$. Thus we have

$$m_s(W) \leq pm.$$

Suppose now that

$$H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_p \leq W.$$

Then for each $i = 1, \ldots, p$,

$$(H_1 \cap B_i)\pi_i \trianglelefteq (H_2 \cap B_i)\pi_i \trianglelefteq \cdots \trianglelefteq (H_p \cap B_i)\pi_i \leq A \in \mathfrak{X}_{p,m}$$

and so there exists $Y_i \subseteq H_p \cap B_i$ such that $|Y_i| < pm$ and

$$\langle H_j \cap Y_i \rangle \pi_i = (H_j \cap B_i)\pi_i$$

for $j = 1, \ldots, p$. Let $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_p$, then

$$|Y| \leq p(pm - 1) = p^2m - p$$

and $Y \subseteq H_p \cap B$. We show by induction on i that

$$\langle H_j \cap Y \cap B_i \rangle = H_j \cap B_i$$

for $i = 0, \ldots, p$ and $j = 1, \ldots, p$. If $i = 0$, the result follows since $B_0 = 1$. Suppose $i > 0$ and

$$\langle H_j \cap Y \cap B_{i-1} \rangle = H_j \cap B_{i-1}$$

for $j = 1, \ldots, p$. Let $g \in H_j \cap B_i$ for some j. Since

$$(H_j \cap B_i)\pi_i = \langle H_j \cap Y_i \rangle \pi_i,$$

there exists $f \in \langle H_j \cap Y_i \rangle$ such that

$$(gf^{-1})\pi_i = 1.$$

But also $gf^{-1} \in H_j \cap B_i$, since $Y_i \subseteq B_i$, and so

$$gf^{-1} \in H_j \cap B_{i-1} = \langle H_j \cap Y \cap B_{i-1} \rangle.$$

However, $f \in \langle H_j \cap Y_i \rangle \leqslant \langle H_j \cap Y \cap B_i \rangle$ and so

$$g \in \langle H_j \cap Y \cap B_i \rangle.$$

Thus

$$\langle H_j \cap Y \cap B_i \rangle = H_j \cap B_i$$

for $j = 1, \ldots, p$ and so the induction on i is complete. In particular, taking $i = p$ we have

$$\langle H_j \cap Y \rangle = \langle H_j \cap Y \cap B \rangle = H_j \cap B$$

for $j = 1, \ldots, p$.

If $H_p \leqslant B$, then we would have $Y \subseteq H_p$, $|Y| \leqslant p^2m - p < p.pm$ and $\langle H_j \cap Y \rangle = H_j$ for $j = 1, \ldots, p$. On the other hand, if $H_p \not\leqslant B$, then let r be the least integer r such that $H_r \not\leqslant B$. Since W/B has prime order, there exists $b \in B$ such that $bc \in H_r$. Then $H_j = H_j \cap B$ for $j < r$ and $H_j = \langle H_j \cap B, bc \rangle$ for $j \geqslant r$. If now $X = Y \cup \{bc\}$, then $X \subseteq H_p$,

$$|X| \leqslant p^2m - p + 1 < p.pm$$

and $\langle H_j \cap X \rangle = H_j$ for $j = 1, \ldots, p$. Hence it follows that $W \in \mathfrak{X}_{p,pm}$ to complete the proof of Theorem B.

Finally we note an example to show that the restriction that p be prime in Theorem B cannot be omitted. If A and $C = \langle c \rangle$ are both cyclic of order 4 and the base group of A wr C is taken to be $A_1 \times A_2 \times A_3 \times A_4$ with $A_i = \langle a_i \rangle$ for $i = 1, \ldots, 4$ and

$$H = \langle a_1^2, a_2^2, a_1a_3, a_2a_4, c^2 \rangle,$$

then $H' = \langle a_1^2a_3^2, a_2^2a_4^2 \rangle$ and H/H' has exponent 2 and rank 5 and so $m(H) = 5$. Thus A wr $C \notin \mathfrak{X}_{4,4}$, whereas $A \in \mathfrak{X}_{4,1}$.

REFERENCES

(1) J. F. Bowers, Normal series of soluble groups of finite rank (Preprint).

(2) L. A. Kaloujnine, La structure des p-groupes de Sylow des groupes symétriques finis, *Ann. Sci. École Norm. Sup.* **65** (1948), 239–276.

(3) D. J. S. Robinson, Finiteness conditions and generalized soluble groups, part 2 (Springer-Verlag, Berlin, 1972).

(4) R. T. Vol'vačev, Sylow p-subgroups of the general linear group, *Izv. Akad. Nauk SSSR Ser. Mat.* **27** (1963), 1031–1054 = *Amer. Math. Soc. Transl.* (2) **64** (1967), 216–243.

(5) A. J. Weir, The Sylow subgroups of the symmetric groups, *Proc. Amer. Math. Soc.* **6** (1955), 534–541.

Department of Mathematics,
University of Edinburgh,
James Clerk Maxwell Building,
Edinburgh, EH9 3JZ.