BULL. AUSTRAL. MATH. SOC. 20F25
VOL. 9 (1973), 127-136.

Minimal generating sets for some wreath products of groups

Yeo Kok Chye

Let $d(G)$ denote the minimum of the cardinalities of the generating sets of the group G. Call a generating set of cardinality $d(G)$ a minimal generating set for G. If A is a finitely generated nilpotent group, B a non-trivial finitely generated abelian group and $A \text{ wr } B$ is their (restricted, standard) wreath product, then it is proved (by explicitly constructing a minimal generating set for $A \text{ wr } B$) that $d(A\text{wr}B) = \max\{1+d(A), d(A\times B)\}$ where $A \times B$ is their direct product.

1. Introduction

The rank $d(G)$ of a group G is defined as the minimum of the cardinalities of the generating sets of G, and a generating set of cardinality $d(G)$ is called a minimal generating set for G. The main result of the paper states that if A is a finitely generated nilpotent group, B is a non-trivial finitely generated abelian group, and $A \text{ wr } B$ is their (restricted, standard) wreath product then

$$d(A\text{wr}B) = \max\{1+d(A), d(A\times B)\}$$

(where $A \times B$ is their direct product)*.* The proof includes an explicit construction of a minimal generating set for $A \text{ wr } B$. For comparison, we also describe applications of results of Gaschütz to the determination of

Received 20 March 1973. The contents of this paper formed part of the author's PhD thesis written at the Australian National University under the supervision of Dr S.A. Meskin and Professor B.H. Neumann. The author is grateful to them, and also to Dr L.G. Kovács for his help in the preparation of this paper.

https://doi.org/10.1017/S0004972700042969 Published online by Cambridge University Press

the ranks of some finite wreath products. In particular, we show that the above formula for $d(A\mathrm{wr}B)$ remains valid whenever A is a finite nilpotent group and B a non-trivial finite group which is either nilpotent or has order co-prime to that of A. However, this approach does not appear to help find minimal generating sets for these wreath products.

The following notation will be used. If G is a group, denote by $|G|$ the order of G and by $\Phi(G)$ the Frattini subgroup of G. If $g, h, \ldots, k$ are elements of G, let $|g|$ be the order of the element g and let $g^h = h^{-1}gh$, $g^{1+h+\ldots+k} = g^1g^h \ldots g^k$, $[g, h] = g^{-1}h^{-1}gh = g^{-1+h}$. Also let C_p be the cyclic group of order p and A^B the base group of the restricted wreath product $A \mathrm{~wr~} B$. If G is a group and n a positive integer, G^n denotes either the direct product of n copies of G, or the subgroup generated by the nth powers of the elements of G; the context will make clear which meaning is intended.

It will be convenient to deal with a simple preliminary observation here. Namely, if A is a finitely generated nilpotent group and B is a group with a non-trivial finite homomorphic image (say C), then $d(A\mathrm{wr}B) \geq 1 + d(A)$. Indeed, in this case there is a prime p such that $C_p^{d(A)}$ is a homomorphic image of A so (by 22.11 and 26.21 in Hanna Neumann's book [7]) $C_p^{d(A)} \mathrm{~wr~} C$ is a homomorphic image of $A \mathrm{~wr~} B$. Thus $d(A\mathrm{wr}B) \geq d\left(C_p^{d(A)}\mathrm{wr}C\right)$ while of course $d\left(\left(C_p^{d(A)}\right)^C\right) = |C|d(A)$ and by the Schreier Formula (Theorem 2.10 in Magnus, Karrass and Solitar [5]) we have $|C|\left(d\left(C_p^{d(A)}\mathrm{wr}C\right)-1\right) + 1 \geq d\left(\left(C_p^{d(A)}\right)^C\right)$. The desired inequality is now an immediate consequence.

2. The ranks of some finite wreath products

We shall be concerned with $d(A\mathrm{wr}B)$ where A and B are finite and $B \neq 1$. The first thing to note is that $A\mathrm{wr}B/\Phi(A)^B \cong A/\Phi(A)\mathrm{wr}B$ and

$\Phi(A)^B = \Phi\left(A^B\right) \leq \Phi(A\text{wr}B)$ so $d(A\text{wr}B) = d\left(A/\Phi(A)\text{wr}B\right)$: thus no generality is lost if $\Phi(A) = 1$ is assumed.

Let G be any non-trivial finite group, p a prime, e an integer, $e > 1$, and F_e a free group of rank e . If R is a normal subgroup of F_e such that $F_e/R \cong G$ (and one such isomorphism is specified), then $R/R'R^p$ may be considered a G-module in a natural way. The modules which arise in this manner, and some applications to the ranks of certain groups, form the subject of paper [2] of Gaschütz. In Satz 4 of [2], he shows that if $p\nmid|G|$, then $R/R'R^p$ is the direct product of a C_p on which G acts trivially and of the base group of C_p^{e-1} wr G . As $p\nmid|G|$, it follows that $F_e/R'R^p$ splits over $R/R'R^p$ and hence that

$$F_e/R'R^p \cong C_p \times \left(C_p^{e-1}\text{wr}G\right) .$$

In fact, in this result p may be replaced by any integer t co-prime to $|G|$. This is immediate when t is square-free; for then $R/R'R^t$ is the direct product of the $R/R'R^p$ with p ranging through the prime divisors of t .

Suppose now that A is a finite nilpotent group and B a finite group with g.c.d.$(|A|, |B|) = 1$. As we noted in the opening remark of this section, we may assume that $\Phi(A) = 1$; now this means that A is abelian of square-free exponent, t say, so it is a homomorphic image of $C_t^{d(A)}$. Thus A wr B is a homomorphic image of $C_t^{d(A)}$ wr B . But from Gaschütz's result given above, $C_t^{d(A)}$ wr B can be generated by $\max\{1+d(A), d(B)\}$ elements. On the other hand, A wr B cannot be generated by fewer than $\max\{1+d(A), d(B)\}$ elements. Thus Gaschütz's result yields that

(1) *if* A *is a finite nilpotent group, if* B *is a finite non-trivial group and if* g.c.d.$(|A|, |B|) = 1$, *then* $d(A\text{wr}B) = \max\{1+d(A), d(B)\}$.

https://doi.org/10.1017/S0004972700042969 Published online by Cambridge University Press

(Note here that $\max\{1+d(A), d(B)\} = \max\{1+d(A), d(A\times B)\}$, since g.c.d.$(|A|, |B|) = 1$ implies that $d(A\times B) = \max\{d(A), d(B)\}$.)

He describes $R/R'R^p$ also in case $p \,\big|\, |G|$, but that description involves parameters which can only be calculated if the submodule structure of the regular representation of G over $\mathrm{GF}(p)$ is sufficiently well-known: we know of no effective way of determining them in general. The special cases of interest to us in which this approach could be used are more easily accessible from another result of Gaschütz [3], which we now proceed to discuss.

In Satz 4 of another paper [3], Gaschütz gives a formula for the eulerian function of an arbitrary finite soluble group G. This formula may be used to calculate $d(G)$ in the following manner. If M is an irreducible G-module, its ring of G-endomorphisms, $\mathrm{end}_G M$ is a finite field. Let $\dim M$ denote the dimension of M as a vector space over $\mathrm{end}_G M$. If M is a non-trivial irreducible G-module, take an arbitrary chief series of G, count the number of complemented factors of this chief series that are isomorphic to M (as G-modules), divide this number by $\dim M$ and denote the result by $\mu(M)$. (It is implicit in [3] and explicit in Satz 4.1 of [4], that $\mu(M)$ is independent of the particular chief series chosen.) The result of Gaschütz then yields that

(2) *if* G *is any finite soluble group, then* $d(G)$ *is the least positive integer such that* $d(G) \geq d(G/G')$ *and* $d(G) \geq 1 + \mu(M)$ *for every non-trivial irreducible* G*-module* M.

We shall now describe how (2) may be used to calculate $d(A\mathrm{wr}B)$ when A is a finite nilpotent group and B is a non-trivial finite soluble group. For $G = A \mathrm{~wr~} B$, G/G' is just the direct product $A/A' \times B/B'$. Let $d_p(G)$ denote the rank of the largest elementary abelian p-factor-group of G, so that $d(G/G') = \max_p d_p(G)$. Then one has $d_p(G) = d_p(A) + d_p(B)$, so $d(G/G') = \max_p \{d_p(A)+d_p(B)\}$. Thus the first inequality of (2) yields that $d(A\mathrm{wr}B) \geq \max_p \{d_p(A)+d_p(B)\}$.

https://doi.org/10.1017/S0004972700042969 Published online by Cambridge University Press

By the opening remark and since $d_p(A) = d_p(A/\Phi(A))$ for all p, we may again assume that A is abelian of square-free exponent. As the base group A^B of $A \operatorname{wr} B$ acts trivially on all chief factors of $A \operatorname{wr} B$, we may view M as a B-module M_B without any essential loss; in particular $\operatorname{end}_B M_B = \operatorname{end}_G M$ and $\dim M_B = \dim M$.

Let M be any non-trivial G-module, p the unique prime divisor of the order of M, and $A_{p'}$ the Sylow p-complement of A so that $A/A_{p'} \cong C_p^{d_p(A)}$ and $A_{p'}^B$ is the Sylow p-complement of A^B. Take a chief series of G through $A_{p'}^B$ and A^B. The part of this from A^B to G corresponds to a chief series of B. The contribution to $\mu(M)$ from this part is $\mu(M_B)$ where $\mu(M_B)$ is defined with reference to a chief series of B instead of G. Observe that M cannot occur below $A_{p'}^B$. Consider the complemented chief factors between $A_{p'}^B$ and A^B isomorphic to M. Let there be t such factors, choose for each a complement and let K denote the intersection of A^B and all these complements. Then K is normal in G and $K \geq A_{p'}^B$. Observe also that A^B/K is a direct sum of t isomorphic copies of M_B and $A^B/A_{p'}^B$ is the direct sum of $d_p(A)$ copies of the regular $\mathrm{GF}(p)B$-module. Now Theorem 61.16 in Curtis and Reiner [7] tells us that $t \leq d_p(A)\dim M_B$. It also tells us that there is a submodule S in A^B, with $S \geq A_{p'}^B$, such that A^B/S is the direct sum of $d_p(A)\dim M_B$ copies of M_B; a chief series of G through S and A^B then has $d_p(A)\dim M_B$ chief factors between S and A^B, all isomorphic to M_B and all complemented. Such a choice of the chief series would result in $t \geq d_p(A)\dim M_B$. Thus $t = d_p(A)\dim M_B$ and so

(3) *if A is a finite nilpotent group and B a non-trivial finite soluble group, then $d(A\mathrm{wr}B)$ is the least positive integer d such that $d \geq \max\{d_p(A)+d_p(B)\}$ and*

$d \geq 1 + d_p(A) + \mu(M_B)$ for each prime p and each non-trivial irreducible B-module M_B of characteristic p .

A special case of (3) will be of particular interest: namely, that of a nilpotent B . In this case $\mu(M_B) = 0$ for all M_B and $\max_p \{1+d_p(A)\} = 1 + d(A)$, so we have

(4) *if A and B are finite nilpotent groups with $B \neq 1$, then $d(A\mathrm{wr}B) = \max\{1+d(A), d(A\times B)\}$.*

3. Minimal generating sets for some wreath products

The purpose of this section is to establish (independently) a partial generalization of (4):

(5) *if A is a finitely generated nilpotent group and B is a finitely generated non-trivial abelian group, then $d(A\mathrm{wr}B) = \max\{1+d(A), d(A\times B)\}$.*

In fact, we can give explicit minimal generating sets for such wreath products. However, to simplify expression we first perform a reduction. A result of McLain (Lemma 2, [6]) says that if N is a nilpotent normal subgroup of a group G , and if H is a subgroup of G such that $HN' = G$, then $H = G$. It follows that if A is a nilpotent group and B an arbitrary group, the generating sets of $A \times B$ correspond naturally to those of $A/A' \times B$. Under the same assumptions, the generating sets of A wr B correspond naturally to those of A/A' wr B (the latter wreath product being isomorphic to the factor group of the first over the derived group of its base group). Thus for the purpose of discussing generating sets of $A \times B$ and A wr B with nilpotent A , one may replace A by A/A' .

Once A is abelian, $A \times B$ is a homomorphic image of A wr B , so $d(A\mathrm{wr}B) \geq d(A\times B)$. On the other hand, we have already seen that $d(A\mathrm{wr}B) \geq 1 + d(A)$ whenever $B \neq 1$. Thus for the proof of (5) it remains to construct generating sets of the appropriate size for wreath products of finitely generated abelian groups, which we now proceed to do.

Let A and B be non-trivial finitely generated abelian groups; put

$d(A) = m$ and $d(B) = n$. It is well-known (see for instance Theorem 3.6 in [5]) that A has a generating set $\{a_1, \ldots, a_m\}$ such that $|a_i| \,\big|\, |a_{i+1}|$ whenever $1 \le i < m$ (where one writes 0 for the order of an element generating an infinite cycle), and B has a generating set $\{b_1, \ldots, b_n\}$ subject to similar conditions. Put $d = \max\{1+d(A), d(A\times B)\}$ and $k = m + n - d$; note $k \le m$ and $k < n$. If $1 \le i \le k$ and g.c.d.$\big(|b_i|, |a_{k-i+1}|\big) = t$ then t divides each of $|b_i|, |b_{i+1}|, \ldots, |b_n|$, $|a_{k-i+1}|, |a_{k-i+2}|, \ldots, |a_m|$ and so C_t^{d+1} is a homomorphic image of $A \times B$: hence $t = 1$. It follows that each congruence

$$|b_i|x_i \equiv 1 \bmod |a_{k-i+1}| , \quad 1 \le i \le k ,$$

has a solution, say t_i. Observe that also

$$|b_i|t_i \equiv 1 \bmod |a_{k-j+1}| \quad \text{whenever} \quad 1 \le i \le j \le k .$$

(In particular, none of $|b_1|, \ldots, |b_k|$ can be 0.)

For $i = 1, \ldots, m$, let f_i denote that function in the base group A^B of $A \text{ wr } B$ for which $f_i(1) = a_i$ and $f_i(y) = 1$ whenever $1 \ne y \in B$; also, for $i = 1, \ldots, k$, put $h_i = f_{k-i+1}$. The integral group ring ZB acts on A^B in a natural way, and provides a convenient notation for what follows. We shall use some of its elements:

$$\beta_i = t_i\left(1 + b_i + b_i^2 + \ldots + b_i^{|b_i|-1}\right) ,$$

$$\gamma_i = 1 - b_i - \beta_i ,$$

$$\delta_i = -t_i\left(b_i + 2b_i^2 + \ldots + \left(|b_i|-1\right)b_i^{|b_i|-1}\right) ,$$

where i ranges from 1 to k. We shall make use of the following congruences, which are easily verifiable by direct calculation:

(6) $$(1-b_i)\beta_i = 0 \ ,$$

(7) $$-\gamma_i\beta_i \equiv \beta_i \bmod |h_j| \ ,$$

(8) $$(1-b_i)\delta_i \equiv 1 - \beta_i \bmod |h_j| \ ,$$

(9) $$\beta_i(1+\delta_i) + \gamma_i\delta_i \equiv 1 \bmod |h_j| \ ,$$

whenever $1 \le i \le j \le k$.

We claim that

(10) *the d-element set*

$$\left\{b_1h_1^{\gamma_1}, \ \ldots, \ b_kh_k^{\gamma_k}, \ b_{k+1}h_1h_2^{\beta_1}h_3^{\beta_1\beta_2} \ \ldots \ h_k^{\beta_1\ldots\beta_{k-1}}, \right.$$
$$\left. f_{k+1}, \ \ldots, \ f_m, \ b_{k+2}, \ \ldots, \ b_n\right\}$$

generates A wr B .

Let K be the subgroup generated by this set. Clearly $KA^B = A$ wr B , so $K \cap A^B$ is a normal subgroup of A wr B and so a $\mathbb{Z}B$-submodule of A^B . Using (7) one obtains that

$$h_i^{\beta_i} = \left(b_ih_i^{\gamma_i}\right)^{-|b_i|t_i} \in K \cap A^B \text{ whenever } 1 \le i \le k \ .$$

Next, calculate a useful form for another element of $K \cap A^B$:

$$\begin{aligned}\left[b_1h_1^{\gamma_1}, \ b_{k+1}h_1h_2^{\beta_1} \ \ldots \ h_k^{\beta_1\ldots\beta_{k-1}}\right] &= \left[b_1h_1^{\gamma_1}, \ b_{k+1}h_1\right] \text{ by (6)} \\ &= h_1^{\gamma_1(b_{k+1}-1)+(1-b_1)} \\ &= h_1^{\gamma_1b_{k+1}+\beta_1} \ .\end{aligned}$$

As we already know that $h_1^{\beta_1} \in K \cap A^B$, it follows that $h_1^{\gamma_1} \in K \cap A^B$ whence by (9) one has $h_1 \in K \cap A^B$. Consequently also $b_1 \in K$. Now look at $h_j^{(1-b_1)\gamma_j} = \left[b_1, \ b_jh_j^{\gamma_j}\right] \in K \cap A^B$ for $2 \le j \le k$: as we already have

$h_j^{\beta_j} \in K \cap A^B$, (9) tells us that $h_j^{1-b_1} \in K \cap A^B$ so that $h_j^{1-\beta_1} \in K \cap A^B$ by (8). It follows that the set

$$\left\{b_2h_2^{\gamma_2}, \ldots, b_kh_k^{\gamma_k}, b_{k+1}h_2h_3^{\beta_2} \ldots h_k^{\beta_2 \ldots \beta_{k-1}}, f_{k+1}, \ldots, f_m, b_{k+2}, \ldots, b_n\right\}$$

lies in K . By repeated application of the steps above, we may then show that $h_2, b_2, \ldots, h_k, b_k$, and finally b_{k+1} , are all in K . As $h_1, \ldots, h_k, f_{k+1}, \ldots, f_m, b_1, \ldots, b_n$ generate A wr B , this completes the proof.

It would be interesting to know whether (5) remains valid if B is assumed to be only nilpotent instead of abelian. The fact that this is true in all finite cases (4) suggests a positive answer.

References

[1] Charles W. Curtis, Irving Reiner, *Representation theory of finite groups and associative algebras* (Pure and Applied Mathematics, XI. Interscience [John Wiley & Sons], New York, London, 1962; reprinted 1966).

[2] Wolfgang Gaschütz, "Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden", *Math. Z.* **60** (1954), 274-286.

[3] Wolfgang Gaschütz, "Die Eulersche Funktion endlicher auflösbarer Gruppen", *Illinois J. Math.* 3 (1959), 469-476.

[4] Wolfgang Gaschütz, "Praefrattinigruppen", *Arch. Math.* 13 (1962), 418-426.

[5] Wilhelm Magnus, Abraham Karrass, Donald Solitar, *Combinatorial group theory* (Interscience [John Wiley & Sons], New York, London, Sydney, 1966).

[6] D.H. McLain, "Finiteness conditions in locally soluble groups", *J. London Math. Soc.* **34** (1959), 101-107.

[7] Hanna Neumann, *Varieties of groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 37. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT.

https://doi.org/10.1017/S0004972700042969 Published online by Cambridge University Press