Contemporary Mathematics
Volume 93 (1989)

The Minimal Number of Generators of Wreath Products of Nilpotent Groups

K. BUZÁSI AND L. G. KOVÁCS

In memory of Samuil Davidovič Berman

1. For a group G, let $d(G)$ denote the minimum of the cardinalities of the generating sets of G.

THEOREM. *Let A and B be nontrivial finitely generated nilpotent groups. Write $A \operatorname{wr} B$ for their restricted standard wreath product, and $A \times B$ for their direct product. If the commutator subgroup B' of B is finite, then $d(A \operatorname{wr} B) = \max\{1 + d(A), d(A \times B)\}$.*

Under the stronger assumption that B is either finite or abelian, this was proved by Yeo Kok Chye [7]. In the simplest case not covered by his work, B has a cyclic subgroup of finite index, and the problem can be translated to one concerning representations of such B over finite prime fields. During the last years of his life, S. D. Berman made substantial contributions to the representation theory of (not necessarily nilpotent) groups which have cyclic subgroups of finite index. He and the first author of this paper repeatedly discussed the possibility that their results could be applied in the context of wreath products. Indeed, the results which are used in the proof below and which are more recent than Yeo Kok Chye [7] come from Berman and Buzási [2].

We do not know whether the theorem remains valid if one omits the condition that B' be finite. For example, let p and q be distinct primes, A a group of order p, and B the group defined by the presentation

$$\langle x, y, z \mid [x, z] = [y, z] = [x, y]z^q = 1 \rangle :$$

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20E22, 20C07.
The second author gratefully acknowledges the hospitality of the University of Essen and the support of the Deutsche Forschungsgemeinschaft, which he enjoyed during the preparation of this paper.

at the time of writing we have not been able to decide whether A wr B can be generated by 3 elements. (As usual, $[x,y]$ denotes the commutator $x^{-1}y^{-1}xy$.)

The proof of the theorem will occupy the rest of the paper.

2. Yeo Kok Chye [7] started by proving, in the last paragraph of his §1, that if A is a finitely generated nilpotent group and if B has a nontrivial finite quotient then

$$d(A \text{ wr } B) \geq 1 + d(A).$$

In the first paragraph of the proof of his (5), he showed that when discussing minimal generating sets of A wr B and $A \times B$ with nilpotent A, one may replace A by A/A'. He then noted that $d(A \text{ wr } B) \geq d(A \times B)$ whenever A is abelian. Thus *for proving a theorem like ours it suffices to show that* A wr B *can be generated by* $\max\{1+d(A), d(A\times B)\}$ *elements whenever* A *is abelian.*

A finitely generated abelian A is the direct product of a free abelian A_0 and a finite abelian A_1, with $d(A) = d(A_0) + d(A_1)$. For finitely generated nilpotent B one has then

$$d(A \times B) = d(A \times (B/B')) = d(A_0) + d(A_1 \times (B/B')) = d(A_0) + d(A_1 \times B).$$

Consider A and B embedded in A wr B as usual (that is, as "first coordinate subgroup" and "top group"): then A_0, A_1, B generate A wr B, while the subgroup generated by A_1 and B is isomorphic to A_1 wr B. It follows that if A_1 wr B can be generated by $\max\{1+d(A_1), d(A_1\times B)\}$ elements, then A wr B can be generated by

$$d(A_0) + \max\{1 + d(A_1), d(A_1 \times B)\},$$

that is, by $\max\{1 + d(A), d(A \times B)\}$ elements. Thus for proving a theorem like ours it suffices to show that A wr B can be generated by the right number of elements *whenever* A *is abelian and finite.*

Strictly speaking, our theorem for finite B was proved in [7], as item (4), only when A is also finite: the argument above shows that no such assumption on A was needed there. For abelian B, our theorem was item (5) in [7]. Its proof involved constructing an explicit generating set of the right size for A wr B. Beyond the initial reduction quoted above, we shall not use (5) of [7] here. Our arguments will be non-constructive in the sense that they give little help towards finding actual generating sets of minimal size in A wr B. Even for finite A and B, we know of no constructions beyond the rather special ones given in the unpublished parts of the thesis [6] of Yeo Kok Chye.

3. The central step in the proof of our theorem is the following. Let F be a free group of finite rank and F/R a nilpotent quotient of F containing a finite normal subgroup Q/R such that F/Q is infinite cyclic. Choose a prime p not dividing $|Q/R|$, denote by $R/R'R^p$ the largest elementary abelian p-quotient of R, and regard $R/R'R^p$ as an $\mathbf{F}_p(F/R)$-module with $\mathbf{F}_p$ the field of p elements and the action of F/R on $R/R'R^p$ coming from conjugation

in F. Since every finitely generated nilpotent group is finitely presented, R is the normal closure of finitely many elements in F, and therefore $R/R'R^p$ is a finitely generated $\mathbf{F}_p(F/R)$-module.

LEMMA. *The free $\mathbf{F}_p(F/R)$-module of rank $d(F)-1$ is a homomorphic image of $R/R'R^p$.*

COROLLARY. *If A is a finite abelian p-group with $d(A) < d(F)$ and α is the natural homomorphism of A wr (F/R) onto F/R, then F has a homomorphism τ onto A wr (F/R) such that the composite $\tau\alpha$ is the natural homomorphism of F onto F/R.*

Deferring the proof of the lemma until later, we show here how the corollary follows from the lemma, and in the next section we derive the theorem from this corollary.

By the lemma, $R/R'R^p$ has a submodule $S/R'R^p$ such that R/S is a free $\mathbf{F}_p(F/R)$-module of rank $d(A)$. Let f be an element of F such that $F/Q = \langle fQ\rangle$: then the index $|Q/R|$ of $\langle fS\rangle(R/S)$ in F/S is prime to p, so by a theorem of Gaschütz (I.17.4a in Huppert [5]) R/S is a semidirect factor in F/S. It follows that F/S is isomorphic to (A/A^p) wr (F/R) with R/S matching the base group. The composite of a corresponding homomorphism σ of F onto (A/A^p) wr (F/R) with the natural projection of this wreath product onto F/R then has kernel R: so it differs from the natural projection $F \to F/R$ only by some automorphism of F/R. As in any wreath product, each automorphism of F/R lifts to an automorphism of (A/A^p) wr (F/R): hence σ can be corrected if necessary to ensure that the composite mentioned is precisely the natural map $F \to F/R$. Because F is free, the σ so chosen may be written as the composite of a $\tau\colon F \to A\,\mathrm{wr}\,(F/R)$ with the homomorphism $\pi\colon A$ wr $(F/R) \to (A/A^p)$ wr (F/R) obtained from the natural projection $A \to A/A^p$. Of course then $\tau\alpha$ is the natural map $F \to F/R$.

It remains to prove that τ is surjective. Since $\tau\alpha$ is surjective, $F\tau$ supplements the kernel A^B of α. If $F\tau$ is a proper subgroup, it is contained in some maximal subgroup H of our finitely generated wreath product, and then $A^B \cap H$ is a maximal $\mathbb{Z}(F/R)$-submodule of A^B. The quotient $A^B/(A^B \cap H)$ is a simple module and so must have prime exponent: thus $A^B \cap H$ contains the kernel $(A^p)^B$ of π. It follows that $H\pi$ is still a proper subgroup, contrary to the surjectivity of σ $(= \tau\pi)$. Thus $F\tau$ cannot be proper, and the deduction of the corollary is complete.

4. We have already seen that the theorem holds when B is finite, so in the sequel B will always be assumed infinite. Then $1 + d(A) \leq d(A \times B)$, so what we have to prove is that A wr B can be generated by $d(A \times B)$ elements.

For an element g of a group G, let $\pi(g)$ denote the set of prime divisors of the order $|g|$ of g. When the subgroup generated by g is infinite, we say that $|g| = 0$ and $\pi(g)$ is the set of all primes. Each finitely generated abelian G has generating sets $\{g_1, \ldots, g_{d(G)}\}$ such that each term of the sequence

$|g_1|, \ldots, |g_{d(G)}|$ divides the next, so

$$\pi(g_1) \subseteq \cdots \subseteq \pi(g_{d(G)}).$$

Set $G = B/B'$ and choose such a generating set. Since B is nilpotent and B' is finite, in each coset g_i one can choose an element b_i such that $\pi(b_i) = \pi(g_i)$. [This is the only point where the finiteness of B' is used.] The subgroup of B generated by $b_1, \ldots, b_{d(G)}$ supplements B' and so equals B: thus $d(B) = d(G)$ and $B = \langle b_1, \ldots, b_{d(B)} \rangle$. The effect of the assumption that B be infinite is that $|b_{d(B)}| = 0$.

For each prime p, set

$$k(p) = \begin{cases} 0 & \text{when } p \in \pi(b_1), \\ \max\{\, i \mid p \notin \pi(b_i) \,\} & \text{when } p \notin \pi(b_1): \end{cases}$$

note that

$$k(p) < d(B) \text{ for all } p.$$

Let A be a finite abelian group and A_p the largest p-quotient of A. It is easy to see that

$$d(A_p \times B) = d(A_p \times G) = \max\{d(B), d(A_p) + d(B) - k(p)\}:$$

what we shall use is that consequently

$$d(A \times B) \geq d(A_p \times B) \geq d(A_p) + d(B) - k(p).$$

For each p, let B_p denote the subgroup generated in B by $\{\, b_i \mid 1 \leq i \leq k(p) \,\}$ and $b_{d(B)}$. Since the last set consists of elements of finite order prime to p, its normal closure in B_p is finite of order prime to p, and of course the quotient of B_p modulo this normal subgroup is infinite cyclic.

Let F be a free group of rank $d(A \times B)$, freely generated by a set $\mathbf{f} = \{f_1, \ldots, f_{d(A\times B)}\}$. Consider the homomorphism ρ of F onto B defined by

$$f_i\rho = \begin{cases} b_i & \text{when } i \leq d(B), \\ 1 & \text{when } i > d(B), \end{cases}$$

and denote its kernel by R. For each p, write $\mathbf{f}$ as the disjoint union $\mathbf{f} = \mathbf{f}_p \cup \mathbf{f}_{p'}$ where

$$\mathbf{f}_p = \{\, f_i \mid 1 \leq i \leq k(p) \text{ or } d(B) \leq i \leq d(A \times B) \,\},$$
$$\mathbf{f}_{p'} = \{\, f_i \mid k(p) < i < d(B) \,\},$$

and let F_p denote the subgroup of F generated by $\mathbf{f}_p$. Note that

$$d(F_p) = k(p) + d(A \times B) - d(B) + 1,$$

so by the last line of the second last paragraph $d(F_p) - 1 \geq d(A_p)$. Write R_p for the kernel $F_p \cap R$ of the restriction $\rho \downarrow F_p$. Since ρ maps F_p onto B_p, we have $F_p/R_p \cong B_p$.

We are now ready to apply the corollary of the lemma, with F_p, R_p, A_p in place of F, R, A. The conclusion may be put as follows. Let α_p be the natural homomorphism of A_p wr B onto B. Consider A_p and B embedded in

A_p wr B. The subgroup $\langle A_p, B_p\rangle$ generated by A_p and B_p is then isomorphic to A_p wr B_p. By that corollary there is a homomorphism $\tau_p\colon F_p \to A_p$ wr B such that

$$F_p\tau_p = \langle A_p, B_p\rangle \text{ and } \tau_p\alpha_p = \rho \downarrow F_p.$$

Define a homomorphism $\rho_p\colon F \to A_p$ wr B by

$$f_i\rho_p = \begin{cases} f_i\tau_p & \text{when } f_i \in \mathbf{f}_p, \\ f_i\rho & \text{when } f_i \in \mathbf{f}_{p'}. \end{cases}$$

Then $F\rho_p \geq F_p\rho_p = F_p\tau_p = \langle A_p, B_p\rangle \geq B_p$ and $\langle B_p, \mathbf{f}_{p'}\rho_p\rangle = B$ together imply that ρ_p is surjective, while of course $\rho_p\alpha_p = \rho$.

For each p, let π_p be the homomorphism of A wr B onto A_p wr B corresponding to the natural homomorphism of A onto A_p, and α the natural homomorphism of A wr B onto B: then $\pi_p\alpha_p = \alpha$ for all p. It is easy to see that the π_p and the α_p, with p ranging through the finite set of the prime divisors of $|A|$, form a pullback. This implies that there is a homomorphism $\varphi\colon F \to A$ wr B such that $\varphi\pi_p = \rho_p$ for all relevant p. We claim that this φ must be surjective. Since $\varphi\alpha$ is surjective, it suffices to show that $F\varphi$ contains the kernel of α. That kernel is the base group of A wr B, and it is an abelian torsion group: so all we need to show is that $F\varphi$ contains each prime-power order element x of that base group. If p is the prime divisor of the order of x, use that $\varphi\pi_p = \rho_p$ and ρ_p is surjective: so there is an $f\varphi$ congruent to x modulo the kernel of π_p. Choose a multiple m of the exponent of that kernel such that $m \equiv 1 \pmod{|x|}$: then $f^m\varphi = x^m = x$. This proves that φ is surjective, so A wr B can be generated by $d(A \times B)$ elements, and the deduction of the theorem from the corollary of the lemma is complete.

5. It remains to prove the lemma. The notation used in the last section has served its purpose: we now return to the notation of §3. Thus F/R is a nilpotent group with a finite normal subgroup Q/R such that F/Q is infinite cyclic: $F/Q = \langle fQ\rangle$. Since Q/R is finite, so is the index of its centralizer in F/R. Since p does not divide $|Q/R|$ and F/R is nilpotent, p cannot divide that index either. Let k be the least positive integer such that f^k centralizes Q/R: by the foregoing, p does not divide k. Now $\langle f^kR\rangle$ commutes with fR and with Q/R, so it is an infinite cyclic subgroup in the centre of F/R. Choose a prime q other than p; for each nonnegative integer m, let $R_m = \langle f^{kq^m}, R\rangle$: then each R_m is a normal subgroup in F, of index $kq^m|Q/R|$, and $\bigcap_m R_m = R$.

Let $R_m/R'_mR^p_m$ denote the largest elementary abelian p-quotient of R_m, viewed as an $\mathbf{F}_p(F/R_m)$-module. This module is completely reducible by Maschke's Theorem; in fact, by a result of Gaschütz [**4**], it is a direct sum of a 1-dimensional trivial module and a free $\mathbf{F}_p(F/R_m)$-module of rank $d(F) - 1$. Since R_m/R is cyclic and central in F/R, its largest elementary abelian p-quotient is a 1-dimensional trivial $\mathbf{F}_p(F/R_m)$-module. Obviously, that quotient is $R_m/R(R'_mR^p_m)$. It follows that $R(R'_mR^p_m)/(R'_mR^p_m)$ is a free

$\mathbf{F}_p(F/R_m)$-module of rank $d(F) - 1$, and hence so is $R/(R \cap (R'_m R^p_m))$. Of course $R'_m R^p_m \geq R'R^p$, and thus our conclusion may be put as follows. For each m, the $\mathbf{F}_p(F/R)$-module $R/R'R^p$ has a quotient on which R_m/R acts trivially and which is free of rank $d(F) - 1$ as $\mathbf{F}_p(F/R_m)$-module.

The group-theoretic preparations for the proof of the lemma are now complete. In what follows, the role of the R_m will be taken on by the kernels of the natural homomorphisms of $\mathbf{F}_p(F/R)$ onto the $\mathbf{F}_p(F/R_m)$.

6. The rest of the argument no longer involves groups, only rings and modules. Accordingly we abandon all previous notation and start afresh, except that we keep $\mathbf{F}_p$ as the name of the field of p elements.

Let R denote the group algebra over $\mathbf{F}_p$ of a group which has a finite normal subgroup of order prime to p such that the corresponding factor group is infinite cyclic. (We have no further use for the assumption that the group be nilpotent.) Let $I_0 \geq \cdots \geq I_m \geq \ldots$ be a descending chain of ideals in R such that each quotient R/I_m is finite yet $\bigcap_m I_m = 0$. Let d be a positive integer, and U a finitely generated right R-module with submodules U_m such that, for each m, U/U_m is annihilated by I_m and is free of rank d as (R/I_m)-module. *Then the free R-module of rank d is a homomorphic image of U.* The conclusions of the previous section show that if we can prove this claim, the lemma will follow.

The proof of Theorem 1 in Berman and Buzási [2] (for some suppressed detail, see also the analogous proof of Theorem 1 in Berman and Buzási [3]) readily specializes to yield that our R is a direct sum of full matrix algebras over crossed group algebras of the infinite cyclic group over finite fields. Let $R = \bigoplus R_i$ be any (two-sided) direct decomposition of R. Then $I_0R_i \geq \cdots \geq I_mR_i \geq \ldots$ is a descending chain of ideals such that each R_i/I_mR_i is finite and $\bigcap_m I_mR_i = 0$. Further, UR_i is a finitely generated R_i-module such that UR_i/U_mR_i is annihilated by I_mR_i and is free of rank d as (R_i/I_mR_i)-module. Conversely, if for each i the free R_i-module of rank d is a homomorphic image of UR_i, then the free R-module of rank d is a homomorphic image of U. This sketch shows that it suffices to prove the italicized claim above for full matrix algebras R over crossed group algebras of the kind mentioned.

Suppose then that R is the full matrix algebra of degree n over some ring S, and let e be one of the diagonal matrix units in R (that is, a matrix with one diagonal entry 1 and all the other entries 0). Then $ReR = R$, and eRe may be naturally identified with S. The functors $- \otimes_R Re$ and $- \otimes_S eR$ provide an equivalence between the categories of (right) R-modules and S-modules (see Exercise 21.6 in Anderson and Fuller [1]). Since R as right R-module is the direct sum of n copies of eR, an R-module V is free of rank d if and only if $V \otimes_R Re$ is a free S-module of rank nd. Further, $eI_0e \geq \cdots \geq eI_me \geq \ldots$ is a descending chain of ideals in S with each S/eI_me finite and $\bigcap_m eI_me = 0$; also, $U \otimes_R Re$ is a finitely generated S-module, while $(U \otimes_R Re)/(U_m \otimes_R Re)$ is

annihilated by eI_me and is free of rank nd as (S/eI_me)-module. Conversely, if the free S-module of rank nd is a homomorphic image of $U \otimes_R Re$, then the free R-module of rank d is a homomorphic image of U. This sketch shows that it suffices to prove the claim with S and nd in place of R and d.

Shifting notation, we assume instead that R itself is a crossed group algebra of an infinite cyclic group over a finite field. As was noted in the discussion preceding Lemma 2 in Berman and Buzási [2], now R is a (not necessarily commutative) principal ideal domain and so each finitely generated R-module U is a direct sum of cyclic modules. Moreover, all proper homomorphic images of R are now finite, so each such U is the direct sum of a free module V and a finite module W. Let c denote the rank of V. Since I_m annihilates U/U_m, we have $VI_m \leq U_m$ and so

$$|U/U_m| \leq |U/VI_m| = |V/VI_m||W| = |R/I_m|^c|W|.$$

Since U/U_m is (R/I_m)-free of rank d,

$$|U/U_m| = |R/I_m|^d.$$

Thus $|R/I_m|^{d-c} \leq |W|$. As R is infinite while each R/I_m is finite but $\bigcap_m I_m = 0$, $|R/I_m|$ tends to infinity with m. It follows that $d - c \leq 0$, and the proof is complete.

ADDED IN PROOF (9 March 1989).

(1) The death of the first author, Professor Károly Buzási, on 7 August 1988, is recorded here with deep regret.

(2) P. A. Linnell has proved that the wreath product named in the second last paragraph of §1 can be generated by 3 elements.

REFERENCES

1. Frank W. Anderson and Kent R. Fuller, *Rings and categories of modules*, Graduate Texts in Mathematics 13, Springer-Verlag, New York-Heidelberg-Berlin, 1974.

2. S. D. Berman and K. Buzási, *On modules over group algebras of groups containing an infinite cyclic subgroup of finite index*, Studia Math. Sci. Hungar. **16** (1981), 455–470. (Russian)

3. ——, *On representations of groups containing an infinite cyclic group of finite index*, Publ. Math. Debrecen **29** (1982), 163–170. (Russian)

4. Wolfgang Gaschütz, *Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden*, Math. Z. **60** (1954), 274–286.

5. B. Huppert, *Endliche Gruppen* I, Springer-Verlag, Berlin-Heidelberg-New York, 1967.

6. Yeo Kok Chye, *Minimal number of generators of some classes of groups*, Ph.D. Thesis, Australian National University, 1972 [Abstract: Bull. Austral. Math. Soc. **9** (1973), 301–302].

7. ——, *Minimal generating sets for some wreath products of groups*, Bull. Austral. Math. Soc. **9** (1973), 127–136.

KOSSUTH LAJOS TUDOMÁNYEGYETEM
MATEMATIKAI INTÉZETE,
POSTAFIÓK 12,
4010 DEBRECEN,
HUNGARY

AND

MATHEMATICS, IAS,
AUSTRALIAN NATIONAL UNIVERSITY,
GPO BOX 4,
CANBERRA, ACT 2601,
AUSTRALIA