RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

C. DAVID

Generating numbers for wreath products

Rendiconti del Seminario Matematico della Università di Padova, tome 92 (1994), p. 71-77

<http://www.numdam.org/item?id=RSMUP_1994__92__71_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 92 (1994)

Generating Numbers for Wreath Products.

C. DAVID (*)

The aim of this paper is to prove the following theorem.

THEOREM. *For every positive integer m there exists a group A with $d(A) = m$ and a cyclic group B such that $d(A \,\mathrm{wr}\, B) = 2$.*

Here, as always, d stands for the minimum number of generators.

Our notation for calculating in wreath products is as follows. If G, H are groups, the wreath product, G wr H, is a splitting extension of the base group G^* (which is isomorphic to the restricted direct product of $|H|$ copies of G) by a group isomorphic to H, $G^* = \prod_{h \in H} G_h$ where $G_h \cong G$ and $g \to g_h$ is the isomorphism.

The action of H on G^* is the usual one:

$$\text{for } h_1, h_2 \in H, \qquad h_2^{-1} g_{h_1} h_2 = g_{h_1 h_2} .$$

For ease of notation, we denote the identity element of H by ε. We also note that for $x, y \in G$ and $m, n \in H$ with $m \neq n$ then $x_m y_n = y_n x_m$.

If $G = A$ wr B then $G/G' \cong A/A' \times B/B'$, so that examples will be easier to find when A is perfect. (In any case we will need $d(A/A') \leq \leq 2$).

The proof of the theorem is in two parts. In the first, Lemma 1, we show that if $d(A) = m$, $d(B) = 1$ and $A = < \alpha^{(1)}, \alpha^{(2)}, \dots \alpha^{(m)} \rangle$ with A perfect and the orders $o(\alpha^{(1)}), o(\alpha^{(2)}), \dots o(\alpha^{(m)})$ co-prime and $B = = \langle z \colon z^{m-1} = 1 \rangle$, then $d(A \,\mathrm{wr}\, B) = 2$. In the second part we show that such an A exists for each m, using results of P. Hall [1] on direct powers of simple groups.

LEMMA 1. *Let $A = \langle \alpha^{(1)}, \alpha^{(2)}, \dots \alpha^{(m)} \rangle$ be a perfect group, where*

(*) School of Mathematics, University of Wales, College of Cardiff, Senghennydd Road, Cardiff CF2 4AG.

$o(\alpha^{(1)})$, $o(\alpha^{(2)})$, …, $o(\alpha^{(m)})$ are co-prime, and let $B = \langle z \colon z^{m-1} = 1\rangle$ be a cyclic group of order $m - 1$. Then $d(A \operatorname{wr} B) = 2$.

Let $H = \langle x, y\rangle$, where

$$x = \alpha_{\varepsilon}^{(1)} \alpha_{z}^{(2)} \alpha_{z^2}^{(3)} \ldots \alpha_{z^{m-2}}^{(m-1)}\,, \qquad y = \alpha_{\varepsilon}^{(m)} z\,.$$

We shall prove that $A \operatorname{wr} B = H$. Firstly, as $o(\alpha^{(1)})$, $o(\alpha^{(2)})$, …, $o(\alpha^{(m-1)})$ are co-prime, $\alpha_{\varepsilon}^{(1)}$, $a_{z}^{(2)}$, $\alpha_{z^2}^{(3)}$, …, $\alpha_{z^{m-2}}^{(m-1)}$ can be expressed in terms of x. But

$$y^{-1} \alpha_{z^{m-2}}^{(m-1)} y = z^{-1} (\alpha_{\varepsilon}^{(m)})^{-1} \alpha_{z^{m-2}}^{(m-1)} (\alpha_{\varepsilon}^{(m)}) z = \alpha_{\varepsilon}^{(m-1)}\,,$$

and in the same way

$$y^{-j} \alpha_{z^{m-j-1}}^{(m-j)} y^{j} = \alpha_{\varepsilon}^{(m-j)}\,, \qquad \text{for } j = 2, \ldots (m-2)\,.$$

Thus $\alpha_{\varepsilon}^{(1)}$, $\alpha_{\varepsilon}^{(2)}$, …, $\alpha_{\varepsilon}^{(m-1)}$ belong to H, and therefore so do all commutators $[\alpha^{(i)}, \alpha^{(j)}]_{\varepsilon}$ for $i, j = 1, 2, \ldots (m-1)$.

But $y^{-(m-1)}(\alpha_{z}^{(1)})\ y^{m-1} = \alpha_{\varepsilon}^{(1)}$ and so $\alpha_{z}^{(1)} = y^{m-1} \alpha_{\varepsilon}^{(1)} y^{-(m-1)})$. Also

$$y^{-1} \alpha_{\varepsilon}^{(1)} y = z^{-1} \alpha_{\varepsilon}^{(m)-1} \alpha_{\varepsilon}^{(1)} \alpha_{\varepsilon}^{(m)} z = \alpha_{z}^{(m)-1} \alpha_{z}^{(1)} \alpha_{z}^{(m)}\,.$$

From this we see that $[\alpha_{z}^{(1)}, \alpha_{z}^{(m)}]$ lies in H. However, $y^{-(m-1)}[\alpha_{z}^{(1)}, \alpha_{z}^{(m)}] y^{m-1} = [\alpha^{(1)}, \alpha^{(m)}]_{\varepsilon}$ and so $[\alpha^{(1)}, \alpha^{(m)}]_{\varepsilon}$ lies in H. A similar argument applies to the commutators $[\alpha^{(i)}, \alpha^{(m)}]_{\varepsilon}$ for $i = 1, 2, \ldots (m-1)$.

For $i = 1, 2, \ldots (m-1)$ and $j, k = 1, 2 \ldots m$ we know that $\alpha_{\varepsilon}^{(i)} \in H$ and

$$[\alpha_{\varepsilon}^{(j)}, \alpha_{\varepsilon}^{(k)}] \in H \text{ and so } (\alpha_{\varepsilon}^{(i)})^{-1} [\alpha_{\varepsilon}^{(j)}, \alpha_{\varepsilon}^{(k)}] \alpha_{\varepsilon}^{(i)} \in H\,.$$

Next we show that $(\alpha_{\varepsilon}^{(m)})^{-1} [\alpha_{\varepsilon}^{(j)}, \alpha_{\varepsilon}^{(k)}] \alpha_{\varepsilon}^{(m)}$ is a product of commutators and elements each of which is in H.

The resulting product is

$$[\alpha_{\varepsilon}^{(m)}, \alpha_{\varepsilon}^{(j)}] (\alpha_{\varepsilon}^{(j)})^{-1} [\alpha_{\varepsilon}^{(m)}, \alpha_{\varepsilon}^{(k)}] (\alpha_{\varepsilon}^{(k)})^{-1} \cdot$$

$$\cdot [\alpha_{\varepsilon}^{(m)}, (\alpha_{\varepsilon}^{(j)})^{-1}] \alpha_{\varepsilon}^{(j)} [\alpha_{\varepsilon}^{(m)}, (\alpha_{\varepsilon}^{(k)})^{-1}] \alpha_{\varepsilon}^{(k)}\,.$$

Since $A = \langle \alpha^{(1)}, \ldots, \alpha^{(m)}\rangle$ this means that H contains A_{ε}'. But A_{ε} is perfect so that A_{ε} is contained in H. As $y = \alpha_{\varepsilon}^{(m)} z$ and $\alpha_{\varepsilon}^{(m)} \in H$ we see that z is in H. So $\langle A_{\varepsilon}, z\rangle$ is contained in H, that is $H = A \operatorname{wr} B$, so that $d(A \operatorname{wr} B) = 2$.

We now have to show that we can find an $A = \langle \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(m)} \rangle$ with A perfect, $o(\alpha^{(1)}), o(\alpha^{(2)}), \ldots, o(\alpha^{(m-1)})$ co-prime and $d(A) = m$. We look at the direct product A_p^n of n alternating groups A_p, choosing n and p so that $d(A_p^n) = m$.

To obtain the general result we have found it helpful to construct a set of co-prime numbers, as follows.

Set $a_0 = 2$, $a_1 = 3$, and for $n \geqslant 2$, $a_{n+1} = a_n(a_n - 1) + 1$.

We use the following two results about this sequence. The proof of the first of these is elementary and we omit it.

LEMMA 2.

$$2 + \frac{a_n - 1}{a_{n-1}} + \frac{a_n - 1}{a_{n-1}} + \frac{a_n - 1}{a_{n-2}} + \frac{a_n - 1}{a_{n-2}} + \ldots + \frac{a_n - 1}{a_2} + $$
$$+ \frac{a_n - 1}{a_2} + \frac{a_n - 3}{2} = \frac{5a_n - 11}{6}, \qquad \text{for } n > 2.$$

LEMMA 3. *$(1 + ka_{n-1})$ is not a proper divisor of a_n, for every n and k.*

PROOF. By definition, $a_n = a_{n-1}(a_{n-1} - 1) + 1$. If $(1 + ka_{n-1})$ is a proper divisor of a_n, then $a_n = t(1 + ka_{n-1})$ for some $t > 1$ and $k < a_{n-1} - 1$. Thus $a_{n-1}(a_{n-1} - 1) + 1 = t(1 + ka_{n-1})$ and hence $t \equiv 1 (\operatorname{mod} a_{n-1})$. We have therefore $t = ra_{n-1} + 1$ for some integer $r > 0$.

So

$$a_{n-1}(a_{n-1} - 1) + 1 = ra_{n-1} + 1 + (ra_{n-1} + 1)ka_{n-1}$$
$$\Rightarrow a_{n-1} - 1 = r + k(ra_{n-1} + 1) \Rightarrow r + (kr - 1)a_{n-1} + (k + 1) = 0.$$

But all the terms are positive so there is a contradiction, and we conclude that $1 + ka_{n-1}$ is not a proper divisor of a_n.

We now return to our construction of the direct product A_p^n of n alternating groups A_p. We set our p to be a_m, the m-th member of our sequence of co-prime numbers. Consider the following elements of A_p^n written as strings in the usual way:

$$\alpha^{(1)} = (\alpha_{11}, \alpha_{12}, \ldots \alpha_{1n}),$$
$$\alpha^{(2)} = (\alpha_{21}, \alpha_{22}, \ldots \alpha_{2n}),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\alpha^{(m)} = (\alpha_{m1}, \alpha_{m2}, \ldots \alpha_{mn}).$$

Here for $1 \leqslant k \leqslant n$, α_{1k} is an a_m-cycle,

α_{2k} is the product of $(a_m - 1)/a_{m-1}$ a_{m-1}-cycles,

α_{3k} is the product of $(a_m - 1)/a_{m-2}$ a_{m-2}-cycles,

....

$\alpha_{(m-1)k}$ is the product of $(a_m - 1)/7$ 7-cycles,

α_{mk} is the product of $(a_m - 3)/2$ 2-cycles and a single 3-cycle.

(Note that a_{mk} is constructed in a different way from the others.)

Let $\varDelta$ be the set of all columns $\begin{pmatrix}\alpha_{1k}\\ \alpha_{2k}\\ \vdots\\ \alpha_{mk}\end{pmatrix}$. There are

$$(a_m!)^m/a_m(a_{m-1})^{(a_m-1)/a_{m-1}}((a_m-1)/a_{m-1})!\ldots 2^{(a_m-3)/2}((a_m-3)/2)!\cdot 3$$

such columns. We shall show later that the elements of each column generate A_p; we assume that at this stage.

The authomorhpism group $\operatorname{Aut} A_p = S_p$ acts on $\varDelta$ by the rule

$$\begin{pmatrix}\alpha_{1k}\\ \alpha_{2k}\\ \vdots\\ \alpha_{mk}\end{pmatrix}\beta = \begin{pmatrix}\alpha_{1k}^{\beta}\\ \alpha_{2k}^{\beta}\\ \vdots\\ \alpha_{mk}^{\beta}\end{pmatrix}, \qquad \beta \in S_p .$$

The number of elements in each S_p-orbit is at most $a_m!$, so the number of orbits is at least

$$(a_m!)^m/a_m(a_{m-1})^{(a_m-1)/a_{m-1}}((a_m-1)/a_{m-1})!\ldots((a_m-3)/2)!\cdot 3\cdot a_m!.$$

So the number of S_p-inequivalent columns is at least

$$(a_m!)^{m-1}/a_m(a_{m-1})^{(a_m-1)/a_{m-1}}((a_m-1)/a_{m-1})!\ldots((a_m-3)/2)!\cdot 3.$$

We now use an application of results in a paper of P. Hall [1] which are used similarly in a paper of James Wiegold [2].

For any finite group G, let $\phi_m(G)$ denote the number of m-bases of G, that is, ordered m-tuplets $(x_1, x_2, \ldots x_m)$ of elements of G that generate G. 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 equivalent classes is $(1/|\operatorname{Aut} G|)\,\phi_m(G)$ since $\operatorname{Aut} G$ permutes the m-bases regularly.

Hall in [1] shows the following result.

For every finite group G and every integer $m \geqslant 1$

$$\phi_m(G) = \sum_{H \leqslant G} \mu(H)\,|H|^m .$$

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

So we have

$$h(m, G) = \frac{1}{|\operatorname{Aut} G|} \sum_{H \leqslant G} \mu(H)\,|H|^m .$$

For non-abelian simple G, it is shown in [1] that $h(m, G)$ is equal to $d_m(G)$ the greatest number l for which the l-th direct power of G can be generated by m elements. This means, for example, that as $d_2(A_5) = 19$ then the direct product of nineteen A_5's can be generated by two elements but not the direct product of twenty. In our case $G = A_p$, and we see that if the direct product of n groups isomorphic to A_p can be generated by $(m-1)$ elements, then the maximum value of n is $(1/|\operatorname{Aut} A_p|) \sum_{H \leqslant G} \mu(H)\,|H|^{m-1}$.

If the direct product of n groups isomorphic to A_p is to be generated by m elements, and not less than m, then n must be greater than $(1/|\operatorname{Aut} A_p|) \sum_{H \leqslant G} \mu(H)\,|H|^{m-1}$.

But $|A_p|^{m-1} \geqslant \sum_{H \leqslant G} \mu(H)\,|H|^{m-1}$, and so, showing that n is greater than $(1/|\operatorname{Aut} A_p|) \cdot |A_p|^{m-1}$ will be sufficient for our needs.

It can be shown that $n \leqslant ((a_m!)/2)^{m-1}/a_m!$ if A_p^n can be generated by $(m-1)$ elements. To show that $d(A_p^n) = m$, it is enough to show that

$$\frac{(a_m!)^{m-1}}{a_m(a_{m-1})^{(a_m-1)/a_{m-1}}((a_m-1)/a_{m-1})! \ldots ((a_m-3)/2)! \cdot 3} >$$

$$> \frac{((a_m!)/2)^{m-1}}{a_m!},$$

or equivalently

$$\frac{a_m!}{a_m \ldots 7^{(a_m-1)/7}((a_m-1)/7)!\,(a_m-3)(a_m-5)\ldots 6 \cdot 4 \cdot 2 \cdot 3} > (1/2)^{m-1}.$$

The numerator of the fraction on the left hand side has a_m factors. The denominator has

$$1 + \frac{a_m - 1}{a_{m-1}} + \frac{a_m - 1}{a_{m-1}} + \frac{a_m - 1}{a_{m-2}} + \frac{a_m - 1}{a_{m-2}} + \ldots + \frac{a_m - 3}{2} + 1 \text{ factors}.$$

Using Lemma 2 we can show that the number of factors in the denominator is less than the number of factors in the numerator.

So the factors of the denominator can be paired with a subset of the factors of the numerator so that each numerator factor is at least equal to its paired denominator factor. This shows that the left hand side is greater than 1, which is more than enough.

We now have to show that every column $\begin{pmatrix} \alpha_{1k} \\ \alpha_{2k} \\ \vdots \\ \alpha_{mk} \end{pmatrix}$ will generated A_p.

To do this we shall show that the entries generate a primitive subgroup of A_p containing a 3-cycle. Theorem 13.3 of Wielandt[3] then completes the proof.

Let x be an a_m-cycle and y be any product of $(a_m - 1)/a_{m-1}$, a_{m-1}-cycles in A_p.

Then $\langle x, y \rangle$ is certainly transitive and we shall show that it is primitive.

Let T be a block containing the point which is not moved by y, so $Ty = T$. Let r be the number of cycles in y that contain elements of T. So T contains exactly $(1 + ra_{m-1})$ elements.

So for imprimitivity we must have $(1 + ra_{m-1})$ as a proper divisor of a_m. But Lemma 3 shows that this is not so and therefore the group $\langle x, y \rangle$ is primitive.

The generating m-tuple is such that

α_{1k}	is an a_m cycle,
$\langle \alpha_{1k}, \alpha_{2k} \rangle$	is primitive, and
$(\alpha_{mk})^2$	is an three-cycle.

This shows that the m-tuple generates A_p.

So we have m elements of co-prime orders generating the genuinely m-generator group A_p^n which is perfect.

I thank Prof. J. Wiegold for suggesting the problem and for his invaluable help and encouragement.

REFERENCES

[1] P. HALL, *The Eulerian functions of a group*, Quart. J. Math. (Oxford), **7** (1936), pp. 134-151.

[2] J. WIEGOLD, *Growth sequences of finite groups*, J. Austral. Math. Soc., **17**, pp. 133-141.

[3] H. WIELANDT, *Finite Permutation Groups*, Lectures, University of Tübingen (1954/55); English trans., Academic Press, New York (1964).

Manoscritto pervenuto in redazione il 21 gennaio 1993
e, in versione definitiva, il 22 marzo 1993.