ISRAEL JOURNAL OF MATHEMATICS 86 (1994), 311–329

THE PROBABILITY OF GENERATING CERTAIN PROFINITE GROUPS BY TWO ELEMENTS

BY

MEENAXI BHATTACHARJEE*

Department of Mathematics
Gauhati University, Guwahati 781014, Assam, India

ABSTRACT

In this paper we consider the question of finite generation of profinite groups. We study the class of profinite groups which are inverse limits of wreath products of alternating groups of degree ≥ 5. We prove that the probability of generating such inverse limits by two elements is strictly positive and tends to 1 as the degree of the first factor tends to infinity. Our method of analysis requires a survey of the maximal subgroups of iterated wreath products of alternating groups. Although we have been unable to classify these precisely we do obtain upper bounds for the number of conjugacy classes of maximal subgroups which we believe to be of independent interest.

1. Introduction

In this paper we shall investigate whether profinite groups which are inverse limits of wreath products of alternating groups can be generated by two elements. Here wreath products are taken with respect to the natural action of alternating groups. Let

$$W = \varprojlim(A_{m_k} \operatorname{Wr} \cdots \operatorname{Wr} A_{m_1})$$

where $m_1, m_2, \ldots, m_k, \ldots$ are integers ≥ 5 and A_m is the alternating group of degree m be such an inverse limit. We shall show that the probability $p(W)$ of generating W by two elements is strictly positive and depends primarily on the

* The author is grateful for financial support received under the FCO-award scheme.
Received August 20, 1992 and in revised form February 21, 1993

probability of generating the first factor A_{m_1} by two elements. In fact, we shall prove (in Theorem 1) that

$$p(W) \geq (1-\varepsilon)p(A_{m_1})$$

where $\varepsilon \to 0$ as $m_1 \to \infty$. This result coupled with the fact that $p(A_m) \to 1$ as $m \to \infty$ (cf. [3]) proves that $p(W) \to 1$ as $m_1 \to \infty$.

We shall first calculate the probabilities for each of the iterated wreath products

$$W_1 := A_{m_1}, \quad W_2 := A_{m_2} \operatorname{Wr} W_1, \quad \ldots, \quad W_r := A_{m_r} \operatorname{Wr} W_{r-1}, \quad \ldots$$

and then show that

$$p(W) = \lim_{r\to\infty} p(W_r).$$

The calculation of $p(W_r)$ in turn relies heavily on the determination of conjugacy classes of maximal subgroups of W_r which project onto the top group W_{r-1}. The proof of the theorem therefore produces, along the way, estimates for upper bounds for the number of conjugacy classes of such maximal subgroups — an analysis which is of considerable interest in itself.

In the following section we set up the necessary basic machinery. We prove (in Lemma 2) that if Y is the wreath product

$$Y := A_m \operatorname{Wr}_\Omega X$$

where $m \geq 5$ and X is transitive on a finite set Ω, and if all the maximal subgroups M of Y which project onto X are conjugate to $M_1, M_2, \ldots, M_k$ then

$$p(Y) \geq \Big(1 - \sum_{i=1}^{k} \frac{1}{|Y\colon M_i|}\Big)p(X).$$

An investigation of such maximal subgroups is therefore made in the third section of this paper. The results obtained are then used to prove the probability theorem in the final section.

2. Preliminaries

Let

$$G = \varprojlim G_n$$

be an inverse limit of finite groups G_n. Then G is a profinite group and hence a compact Hausdorff topological group.

For $i \geq 1$ define

$$N_i := \ker(\pi_i|_G)$$

where $\pi_i|_G: G \to G_i$ is the projection map. Define a topology $\mathcal{T}$ on G (called the **profinite topology** on G) by taking as basis of neighbourhoods of the identity the family of normal subgroups $\{N_i\}_{i\in\mathbf{N}}$ of G. A little thought shows that the profinite topology on G is the same as the topology induced on G from the product topology on $\prod_{n\in\mathbf{N}} G_n$.

A Haar measure μ that can be put on the group G can be extended in a natural way to define the product measure (also denoted by μ) on $G \times G$ (cf. [5], §58, §35).

A pair of elements $g_1, g_2 \in G$ is said to **generate G topologically** if the subgroup $\langle g_1, g_2\rangle$ of G generated by g_1 and g_2 is a dense subgroup of G. We shall denote this by

$$\overline{\langle g_1, g_2\rangle} = G.$$

Define

$$S := \{(g_1, g_2) \in G \times G \mid \overline{\langle g_1, g_2\rangle} = G\}.$$

For a finite group X let $p(X)$ be the probability of generating X by two elements. With the above definitions we can now prove the following lemma.

LEMMA 1: *The set S is measurable and*

$$\mu(S) = \lim_{r\to\infty} p(G/N_r) \cdot \mu(G).$$

Proof: Define

$$S_r := \{(g_1, g_2) \in G \times G \mid \langle g_1, g_2\rangle N_r = G\}.$$

Since S_r is a (finite) union of cosets of $N_r \times N_r$, it is open and hence measurable. A little calculation shows that for every $r \geq 1$,

$$\mu(S_r) = p(G/N_r) \cdot \mu(G).$$

It is easy to see that

$$S = \bigcap_{r\in\mathbf{N}} S_r.$$

Therefore S is measurable. Furthermore,

$$\mu(S) = \lim_{r\to\infty} p(G/N_r)\cdot\mu(G)$$

as $\mu(S_r)$ is a monotonically decreasing sequence. ∎

We next set up some notation and prove a lemma which will be crucial for the proof of our theorem. Let X be a group acting transitively on a finite set $\Omega := \{1, 2, \ldots, n\}$. Let

$$Y := A_m \operatorname{Wr}_\Omega X := K \cdot X$$

with $m \geq 5$ and $K = A_m^\Omega$, the base group in the wreath product. (For definition of wreath products see §2.3 of [2].) Elements of the wreath product Y will be denoted by fx with $f \in K$ and $x \in X$. Though an explicit description of X is not required immediately, X will, in due course, be taken to be an iterated wreath product of alternating groups

$$A_{m_k} \operatorname{Wr} A_{m_{k-1}} \operatorname{Wr} \cdots \operatorname{Wr} A_{m_1}$$

with $n = m_k m_{k-1} \cdots m_1$ and each $m_i \geq 5$. Therefore X and Y will both be groups of the same type, viz. iterated wreath products of alternating groups of degree ≥ 5.

LEMMA 2: *If the maximal subgroups M of Y such that*

$$M \cdot K = Y$$

are conjugate to $M_1, M_2, \ldots, M_k$ then

$$p(Y) \geq \Big(1 - \sum_{i=1}^{k} \frac{1}{|Y\colon M_i|}\Big) p(X).$$

Proof: If X cannot be generated by two elements then $p(X) = 0$ and the lemma is vacuously true. If $p(X) > 0$ choose elements $x_1, x_2 \in X$ such that $\langle x_1, x_2\rangle = X$. For $i = 1, 2, \ldots, k$ let

$$L_i := \{(f_1, f_2) \in K \times K \mid f_1 x_1 \text{ and } f_2 x_2 \text{ belong to a conjugate of } M_i\}.$$

Then

$$|L_i| \leq |M_i \cap K|^2 |Y\colon M_i|$$

as $|Y\colon M_i|$ is the number of conjugates of M_i in Y.

Define

$$L := \{(f_1, f_2) \mid \langle f_1 x_1, f_2 x_2\rangle \neq Y\}.$$

Then

$$|L| \leq |\bigcup_{i=1}^{k} L_i| \leq \sum_{i=1}^{k} |M_i \cap K|^2 |Y\colon M_i|$$
$$= \frac{|Y|}{|X|^2} \sum_{i=1}^{k} |M_i|$$

because $|M_i \cap K| = |M_i|/|X|$. Therefore

$$|L^c| = |\{(f_1, f_2) \mid \langle f_1 x_1, f_2 x_2\rangle = Y\}|$$
$$\geq |K|^2 - \frac{|Y|}{|X|^2} \sum_{i=1}^{k} |M_i|$$

so that

$$|\{(f_1 y_1, f_2 y_2) \mid \langle f_1 y_1, f_2 y_2\rangle = Y\}| \geq (|K|^2 - \frac{|Y|}{|X|^2} \sum_{i=1}^{k} |M_i|)|X|^2 p(X).$$

Thus, we get

$$p(Y) = \frac{1}{|Y|^2} |\{(f_1 y_1, f_2 y_2) \in Y \times Y \mid \langle f_1 y_1, f_2 y_2\rangle = Y\}|$$
$$\geq \frac{1}{|Y|^2} \Big(|Y|^2 - |Y| \sum_{i=1}^{k} |M_i|\Big) p(X)$$
$$= \Big(1 - \sum_{i=1}^{k} \frac{1}{|Y\colon M_i|}\Big) p(X)$$

which is what we wanted to show. ∎

Since $M \cdot K = Y$ we must have

$$M/M \cap K \cong X.$$

Also since X acts transitively on the set Ω, the projections of $M \cap K$ into the n factors of K must be conjugate. Let π_i be the projection of $M \cap K$ into the i-th factor of K and let

$$T_i := (M \cap K)\pi_i \leq A_m$$

for $1 \leq i \leq n$. Then

$$M \cap K \leq T_1 \times T_2 \times \cdots \times T_n.$$

Since the groups T_i for $1 \leq i \leq n$ are all conjugate subgroups of A_m we can differentiate three cases for investigation depending on whether $T_i = A_m$ or $\{1\} < T_i < A_m$ or $T_i = \{1\}$. We shall study each of these cases in turn in the next section.

3. The three cases

3.1 CASE (i). For some $i \in \Omega$, the group $T_i = A_m$. Then $T_j = A_m$ for all $j \in \Omega$, so that $M \cap K$ is a subdirect product in the base group. But $m \geq 5$, so A_m is simple and a subdirect product of a family of non-abelian simple groups can be expressed as a direct product, say

$$M \cap K = D_1 \times D_2 \times \cdots \times D_s$$

where

$$\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_s$$

is a partition of Ω and each $D_i (\cong A_m)$ is the diagonal subgroup of the direct product of the family $\{T_j \mid j \in \Omega_i\}$. (See [2], Lemma 2.3 for a proof.)

Define an X-congruence ρ on Ω as follows: two distinct elements ω_1 and ω_2 of Ω are congruent modulo ρ if and only if they belong to the same Ω_i for some i in the set $\{1, 2, \ldots, s\}$. It is obvious that, with this definition, ρ is an equivalence relation. To show that ρ is an X-congruence, it is sufficient to show that for every $x \in X$ and for every $i \in \{1, 2, \ldots, s\}$ there exists some $j \in \{1, 2, \ldots, s\}$ such that $\Omega_i x = \Omega_j$. Given $x \in X$, there exists an element fx in M for some $f \in K$ (because M projects onto X). Now $D_1, D_2, \ldots, D_s$ are the minimal normal subgroups of $M \cap K$. So conjugation by fx permutes these groups amongst themselves. If $(fx)^{-1} D_i (fx) = D_j$ for $i, j \in \{1, 2, \ldots, s\}$, a little calculation shows that $\Omega_i x = \Omega_j$. This proves that ρ is an X-congruence on Ω.

Therefore, we can write

$$M \cap K = D_1 \times D_2 \times \cdots \times D_s$$

where ρ is a non-trivial X-congruence on Ω, $\Delta := \Omega/\rho$, $|\Delta| = s$ and each D_i is the diagonal subgroup of A_m^Γ where $\Gamma := \rho(\omega)$ for some $\omega \in \Omega$.

If $n = s.l$, then each diagonal subgroup D_i is of the form

$$D_i = \{(x_i, x_i\varphi_2, \ldots, x_i\varphi_l) \mid x_i \in A_m \text{ and } \varphi_j \in \mathrm{Aut}(A_m)\}$$

where $\mathrm{Aut}(A_m)$ denotes the automorphism group of A_m. Hence elements of $M \cap K$ are of the form

$$(x_1, x_1\varphi_2, \ldots, x_1\varphi_l, x_2, x_2\varphi_{l+2}, \ldots, x_2\varphi_{2l}, \ldots, x_s, x_s\varphi_{(s-1)l+2}, \ldots, x_s\varphi_{sl})$$

where $x_i \in A_m$ and $\varphi_j \in \mathrm{Aut}(A_m)$. Since the inner automorphisms of A_m give rise to a single conjugacy class of such subgroups of K, given an X-congruence ρ as defined earlier, the number of conjugacy classes of subgroups of the form $D_1 \times D_2 \times \cdots \times D_s$ in K is at most $|\mathrm{Out}(A_m)|^{n-s}$ where $\mathrm{Out}(A_m)$ denotes the outer automorphism group of A_m. As is well known, $|\mathrm{Out}(A_m)| = 2$ if $m \neq 6$ and 4 if $m = 6$.

Furthermore, given a subgroup $D_1 \times D_2 \times \cdots \times D_s$ of K, either it corresponds to no maximal subgroup of Y or it corresponds to just one, namely, its normaliser in Y. If there exist maximal subgroups of Y of this type let us denote the maximum number of distinct conjugacy classes of such subgroups by d_0 and a lower bound to the index of such subgroups in Y by i_0. Then we have

$$d_0 \leq \begin{cases} 2^{n-s}.r & \text{if } m \neq 6 \\ 4^{n-s}.r & \text{if } m = 6 \end{cases}$$

where r is an upper bound to the number of non-trivial X-congruences ρ on Ω, and

$$i_0 = |A_m|^{n-|\Delta|} = (m!/2)^{n-s}.$$

LEMMA 3:

$$\frac{d_0}{i_0} \leq \frac{1}{m^{n/2}}, \quad \text{for all } m, n \geq 5.$$

Proof: Since ρ is non-trivial, $s \leq n/2$ and so

$$\frac{1}{m^{n-s}} \leq \frac{1}{m^{n/2}}.$$

It therefore suffices to prove that

$$d_0 \leq i_0/m^{n-s} = ((m-1)!/2)^{n-s}.$$

Substituting the expression for d_0 it follows that we only need to show that

$$r \leq \begin{cases} (\frac{4!}{2})^{n-s} \cdot \frac{1}{2^{n-s}} = 6^{n-s} & \text{if } m \neq 6 \\ (\frac{5!}{2})^{n-s} \cdot \frac{1}{4^{n-s}} = 15^{n-s} & \text{if } m = 6 \end{cases}$$

where r is an upper bound to the number of non-trivial X-congruences ρ on Ω. By transitivity of the action of X on Ω it follows that an X-congruence ρ on Ω is determined by one of its blocks, which is a subset of Ω. Thus,

$$\begin{aligned} r &\leq \text{ number of subsets of } \Omega \\ &= 2^n = 4^{n/2} \leq 6^{n/2} \leq 6^{n-s}. \end{aligned}$$ ∎

3.2 CASE (ii). For some $i \in \Omega$, the group $T_i < A_m$ and $T_i \neq \{1\}$. Then $T_j < A_m$ for all $j \in \Omega$. We will first prove a lemma.

LEMMA 4: *M normalises the group $T_1 \times T_2 \times \cdots \times T_n$.*

Proof: Let $t := (t_1, t_2, \ldots, t_n) \in T_1 \times T_2 \times \cdots \times T_n$ and $x \in M$. We want to show that

$$x^{-1}tx \in T_1 \times T_2 \times \cdots \times T_n.$$

That is, for each $i = 1, 2, \ldots, n$

$$(x^{-1}tx)\pi_i \in T_i.$$

For $j \in \Omega$ let $i := jx$. Since $t_j \in T_j$ there exists an element $k \in K \cap M$ such that $k\pi_j = t_j$. Then

$$(x^{-1}kx)\pi_i = (k)\pi_{ix^{-1}} = (k)\pi_j = t_j = (t)\pi_j = (t)\pi_{ix^{-1}} = (x^{-1}tx)\pi_i.$$

But $M \cap K \trianglelefteq M$ and so $x^{-1}kx \in M \cap K$. This proves that for every $i \in \{1, 2, \ldots, n\}$ there is an element $k_i \in K \cap M$ such that $(x^{-1}tx)\pi_i = (x^{-1}k_ix)\pi_i \in T_i$. ∎

From the last lemma we have

$$M \leq N_Y(T_1 \times T_2 \times \cdots \times T_n)$$

where $N_Y(T_1 \times T_2 \times \cdots \times T_n)$ denotes the normaliser of $(T_1 \times T_2 \times \cdots \times T_n)$ in Y. But M is maximal in Y, so we must have

$$M = N_Y(T_1 \times T_2 \times \cdots \times T_n).$$

Since all the groups $T_1, T_2, \ldots, T_n$ are conjugate, we can take them all to be equal to a subgroup, say T of A_m. Then

$$M = N_Y(T^\Omega) = (N_{A_m}(T))^\Omega.X = N_{A_m}(T) \operatorname{Wr}_\Omega X.$$

By maximality of M in Y it follows that $N_{A_m}(T) = T$ and hence

$$M = T \operatorname{Wr}_\Omega X$$

where T is a maximal proper subgroup of A_m. Furthermore,

$$|Y\colon M| = |A_m\colon T|^n \geq m^n$$

as A_m has no subgroup of index less than m.

To find an upper bound to the number of distinct conjugacy classes of maximal subgroups of this type in Y it suffices to find an upper bound to the number of distinct conjugacy classes of maximal subgroups T of A_m. As a consequence of the O'Nan–Scott theorem (cf. [8], p. 329) we know that T can be of the following six types.

1. THE INTRANSITIVE TYPE: $T = (S_l \times S_k) \cap A_m$ with $m = l + k$ and $l \neq k$.

2. THE IMPRIMITIVE TYPE: $T = (S_l \operatorname{Wr} S_k) \cap A_m$ with $m = lk$ and $l, k > 1$.

3. THE AFFINE TYPE: $T = \mathrm{AGL}(k, p) \cap A_m$ with $m = p^k$, p a prime.

4. THE DIAGONAL TYPE: $T = (H^k.(\mathrm{Out}H \times S_k)) \cap A_m$ where H is a non-abelian simple group, $k \geq 2$ and $m = |H|^{k-1}$.

5. THE PRODUCT ACTION TYPE: $T = (S_l \operatorname{Wr} S_k) \cap A_m$ with $m = l^k, k > 1$.

6. THE ALMOST SIMPLE TYPE: Here T is such that $H \lhd T \leq \mathrm{Aut}(H)$ with H non-abelian simple, $H \neq A_m$ and T acting primitively on a set of size m.

Let us denote the maximum number of distinct conjugacy classes of maximal subgroups of type r in A_m with $1 \leq r \leq 6$ by d_r and a lower bound to the index of such subgroups in W by i_r. Then, by the comments made earlier, it follows that

$$i_r \geq m^n$$

for $1 \leq r \leq 6$. Let us now try to estimate d_r for $1 \leq r \leq 6$.

The number of ways of choosing an integer l between 1 and $(m-1)/2$ is at most $(m-1)/2$, so that $d_1 \leq (m-1)/2$. The number d_2 equals the number of ways of

choosing an integer l such that $l \mid m, l \neq 1, m$, so that $d_2 = (d(m) - 2) \leq (m-2)$ where $d(m)$ is the number of positive integral divisors of m. There can be at most one way of expressing m as a power of a single prime so that we have $d_3 \leq 1$. The number d_4 is at most twice the number of non-abelian simple groups H we can find such that $m = |H|^{k-1}$ for some $k \geq 2$. By the 'Power order theorem of Cameron and Teague' ([6], Theorem 6.1), we know that there can be at most 2 such simple groups. Finally, d_5 is at most twice the number of distinct subgroups of the form $(S_l \operatorname{Wr} S_k)$ of S_m with $m = l^k$ and $k > 1$ which is certainly less than $d(m) - 2$. Therefore, $d_5 \leq 2(d(m) - 2) \leq 2(m-2)$. It follows therefore that

$$\sum_{r=1}^{5} d_r \leq 4m - 2.$$

If T is a maximal subgroup of type 6 in A_m then $T = N_{A_m}(H)$. So there can be at most as many distinct subgroups of A_m of this type as there can be simple groups contained in A_m. Since all non-abelian simple groups are two-generator groups (cf. [1], §3) there can be at most $(m!/2)^2$ of them contained in A_m. Therefore, $d_6 \leq (m!/2)^2$. It must be mentioned here that this bound is probably very far from the truth. It is however quite adequate for our purposes.

LEMMA 5:

$$\frac{d_6}{i_6} \leq \begin{cases} 1/2^{m(n-6)} & \text{if } m > 21 \\ 2/m^n & \text{otherwise} \end{cases}$$

where d_6 is as defined earlier and $i_6 = |Y\colon M|$.

Proof: Though much better estimates are now available we will use a result of Praeger and Saxl [7], which states that $|T| < 4^m$ if T is a primitive permutation group of degree m not containing A_m. Therefore,

$$|A_m\colon T| \geq \frac{m!}{2^{2m+1}}.$$

Using Stirling's approximation, we get

$$\frac{d_6}{i_6} \leq 2^{2mn}\left(\frac{e}{m}\right)^{m(n-2)}$$

If $m > 8e$ then it follows that

$$\frac{d_6}{i_6} \leq \frac{1}{2^{m(n-6)}}.$$

Since $e < 2.72$, all values of m greater than 21 satisfy the inequality $m > 8e$.

A complete list of primitive groups of degrees less than 20 is given in [9]. By going through this list for each degree m in turn and discarding those groups which are cyclic or alternating of degree m and those which contain odd permutations or a cyclic or elementary abelian minimal normal subgroup we see that there can be at most 3 conjugacy classes of primitive groups T of type 6 contained in A_m for $m \leq 20$. Considerations of maximality of such groups further reduce the number to 2. The case when $m = 21$ can be tackled separately (for example, by using [4]) to obtain the same answer. Since $i_6 \geq m^n$ for any maximal subgroup in case (ii) this completes the proof of the lemma. ∎

3.3 CASE (iii). For every i for $1 \leq i \leq n$, the group $T_i = \{1\}$. Then $M \cap K = \{1\}$ and since $M.K = Y$, it follows that M is a complement for K in Y. The base group does not always have complements which are maximal subgroups of the wreath product (for example, see [2], pp. 97–99). Rather than try to estimate numbers of conjugacy classes of maximal complements (which appears to be a very difficult problem) we shall drop the maximality condition and derive upper bounds for the number of conjugacy classes of all complements because such upper bounds ought to be of interest in their own right.

Define

$$i_7 := |Y\colon M| = |K|.$$

From now on we shall assume X to be an iterated wreath product of alternating groups

$$X = A_{m_k} \operatorname{Wr} A_{m_{k-1}} \operatorname{Wr} \cdots \operatorname{Wr} A_{m_1}$$

where $n = m_k \cdots m_1$ and each $m_i \geq 5$.

Suppose that there exist elements $g, h \in X$ that generate X, and are such that

(i) g is semi-regular on Ω (that is, it has no fixed points and all its cycles are of the same length), and

(ii) h is of order 2 in its action on Ω.

Under the above hypotheses we can prove the following lemma.

LEMMA 6: *If l is the number of transpositions of h on Ω then the number d_7 of conjugacy classes of complements of the base group K in Y is at most $|K|/|A_m|^l$.*

Proof: Let C be a complement for K in Y. Then $C \cap K = \{1\}$ and $C.K = Y$. Also there exist elements $f, f' \in K$ such that fg and $f'h$ generate C. Since C

is a complement, we must have $(fg)^r = (f'h)^2 = 1$ where r is the order of g. If $(\omega_1 \omega_2 \cdots \omega_r)$ is an r-cycle of g on Ω and $a_i := f(\omega_i)$ for $1 \leq i \leq r$ then $(fg)^r = 1$ implies $a_i a_{i+1} \cdots a_r a_1 \cdots a_{i-1} = 1$ for all possible values of i. But

$$((a_1^{-1}, (a_2 a_1)^{-1}, \ldots, (a_r a_{r-1} \cdots a_1)^{-1})1)((a_1, a_2, \ldots, a_r)(\omega_1 \omega_2 \cdots \omega_r))$$
$$((a_1, a_2 a_1, \ldots, a_r a_{r-1} \cdots a_1)1) = ((a_r a_{r-1} \cdots a_1, 1, \ldots, 1)(\omega_1 \omega_2 \cdots \omega_r))$$
$$= (1(\omega_1 \omega_2 \cdots \omega_r)).$$

(Note that terms like $(a_1, a_2, \ldots, a_r)$ are sequences in A_m while $(\omega_1 \omega_2 \cdots \omega_r)$ is an r-cycle in X.) Therefore, conjugating by a suitable element of K we may suppose that $g \in C$ so that

$$C = \langle g, f'h \rangle.$$

Now $(f'h)^2 = 1$ implies that if $(\delta_1 \delta_2)$ is a transposition of h in Ω and $b_i := f'(\delta_i)$ for $i = 1, 2$ then $b_1 b_2 = 1$. Therefore either one of b_1 and b_2 determines the second. Also, if δ is any fixed point of h in Ω then $(f'h)^2 = 1$ implies that if $b := f'(\delta)$ then $b^2 = 1$.

It follows that d_7 the number of conjugacy classes of complements of K in Y is at most the number of ways of choosing an element $f' \in K$ satisfying the requirements obtained in the last paragraph. Thus

$$d_7 \leq |A_m|^l t^{n-2l}$$

where t is the number of elements x in A_m such that $x^2 = 1$. Though t can be shown to be much smaller the worst possible bound for t will suffice for our purposes. Putting $|K| = |A_m|^n$ and $|t| \leq |A_m|$ in the expression above we obtain a proof of the lemma. ∎

We have now to show that there exist elements g and h in X satisfying the hypotheses made before the statement of the last lemma and such that l is large (equivalently, with h having relatively few fixed points). We begin by setting up some more notation. As before, set

$$W_1 := A_{m_1}$$

acting on a set Σ_1 of size $n_1 := m_1$, and define inductively for $k \geq r \geq 2$,

$$W_r := A_{m_r} \operatorname{Wr}_{\Sigma_{r-1}} W_{r-1}$$

acting on a set Σ_r of size $n_r := m_r|\Sigma_{r-1}| = m_r m_{r-1} \dots m_1$. Then $X = W_k$, $\Omega = \Sigma_k$ and $n = n_k$.

Every element $w_r \in W_r$ induces a permutation on Σ_r and hence also, by restriction, on Σ_s for $1 \leq s \leq r$. Let the permutation that an element x of $X\,(= W_k)$ induces on Σ_r be denoted by x_r for $1 \leq r \leq k$.

The sets Σ_r for $2 \leq r \leq k+1$ can be expressed as products $\Gamma_r \times \Sigma_{r-1}$ where Γ_r is a set with n_r elements. We define ρ to be the equivalence relation induced by the natural projection of $\Gamma_r \times \Sigma_{r-1}$ on Σ_{r-1}. Then two elements (γ_1, δ_1) and (γ_2, δ_2) of Σ_r are members of the same equivalence class of Σ_r under ρ if and only if $\delta_1 = \delta_2$. For $\delta \in \Sigma_{r-1}$ we denote the class

$$\{(\gamma, \delta) | \ \gamma \in \Gamma_r\}$$

of Σ_r by $\Sigma_r(\delta)$. Given an integer t, define

$$t' := \begin{cases} t & \text{if } t \text{ is odd} \\ t/2 & \text{otherwise.} \end{cases}$$

Also let

$$n'_t := m'_t m'_{t-1} \cdots m'_1 = \frac{n_t}{2^{s_t}}$$

where s_t is the number of even numbers in the sequence $m_1, m_2, \dots, m_t$. Let l_r be the number of tranpositions that h_r induces of Σ_r. Let $n' := n'_k, l := l_k$ and $s := s_k$. We can now prove the following lemma.

LEMMA 7: *There exist elements $g, h \in X$ that generate X and are such that*

(i) *g has 2^s disjoint cycles each of length n' on Ω (and is hence semi-regular on Ω) and*

(ii) *h is of order 2 and has l transpositions in its action on Ω where $l \geq (n/2) - 2^{2k-1}$.*

Proof: We shall define the elements g and h inductively, using induction on the length k of the iterated wreath product X. To simplify notation we will assume that for each r, $1 \leq r \leq k$, the set

$$\{1, 2, \dots, m_r\}$$

is an equivalence class of Σ_r under ρ. Let

$$m_r = 2l_r + \epsilon$$

where $\epsilon \in \{1,2,3,4\}$ and l_r is even. Define elements $a_r, b_r \in A_{m_r}$ as follows:

$$a_r := \begin{cases} (1,\,2,\,\ldots,\,m_r) & \text{if } m_r \text{ is odd} \\ (1,\,3,\,\ldots,\,m_r-1)(2,\,4,\,\ldots,\,m_r) & \text{otherwise} \end{cases}$$

and

$$b_r := \begin{cases} (1,\,l_r+1)(2,\,l_r+2)\ldots(l_r,\,2l_r) \\ \qquad \text{if } \epsilon \text{ is 1 or 3} \\ (1,\,2)(3,\,4)\ldots(2l_r-3,\,2l_r-2)(2l_r-1,\,2l_r+1) \\ \qquad \text{if } \epsilon \text{ is 2} \\ (1,\,2)(3,\,4)\ldots(2l_r-5,\,2l_r-4)(2l_r-3,\,2l_r+1)(2l_r-1,\,2l_r+3) \\ \qquad \text{if } \epsilon \text{ is 4.} \end{cases}$$

The commas are included for greater clarity. Since

$$a_r^{-1}b_r a_r b_r := \begin{cases} (1,\,l_r+1,\,2l_r+1) & \text{if } m_r = 2l_r+\epsilon, \epsilon = 1,3 \\ (1,\,2l_r-1,\,2l_r,\,2l_r+1,\,2) & \text{if } m_r = 2l_r+2 \\ (1,\,2l_r-3,\,2l_r-2,\,2l_r+1,\,2) & \text{if } m_r = 2l_r+4 \end{cases}$$

it is not difficult to show that the group generated by a_r and $[a_r, b_r]$ is double transitive and hence primitive. Using Theorems 13.3 and 13.9 of [10] or directly it can then be proved that the group generated by a_r and $[a_r, b_r]$ is the alternating group A_{m_r} for $m_r \geq 5$. Hence, for $m_r \geq 5$,

$$\langle a_r, b_r \rangle = A_{m_r}.$$

Define

$$g_1 := a_1 \quad \text{and} \quad h_1 := b_1.$$

Then g_1 and h_1 generate A_{m_1}. Trivially g_1 has 2^{s_1} disjoint cycles each of length n_1' on Σ_1, $h_1^2 = 1$ and h_1 has $l_1 \geq (m_1/2) - 2$ transpositions on Σ_1. This starts the induction.

Therefore, let us assume, as inductive hypothesis, that we have already defined elements g_{r-1} and h_{r-1} in $W_{r-1}, 2 \leq r \leq k$ that generate W_{r-1} and are such that

(i) g_{r-1} has $2^{s_{r-1}}$ disjoint cycles each of length n_{r-1}' on Σ_{r-1} and

(ii) h_{r-1} is of order 2 and has l_{r-1} transpositions in its action on Σ_{r-1} where $l_{r-1} \geq (n_{r-1}/2) - 2^{2(r-1)-1}$.

We want to show that we can find elements g_r and h_r in W_r that generate W_r and satisfy the requirements on their cycle structures obtained from (i) and (ii) above.

Let $J := A_{m_r}^{\Sigma_{r-1}}$ be the base group in the wreath product

$$W_r = A_{m_r} \operatorname{Wr}_{\Sigma_{r-1}} W_{r-1}.$$

Define an element $f \in J$ as follows. For every n'_{r-1}-cycle $(\omega_1 \omega_2 \dots \omega_{n'_{r-1}})$ of g_{r-1} on Σ_{r-1} let

$$f(\omega_i) := \begin{cases} a_r & \text{if } i = 1 \\ 1 & \text{otherwise.} \end{cases}$$

Then define

$$g_r := (f g_{r-1}) \in W_r.$$

It follows that every n'_{r-1}-cycle of g_{r-1} gives rise to a $m_r n'_{r-1}$-cycle of g_r if m_r is odd and to two disjoint $m_r n'_{r-1}/2$-cycles of g_r if m_r is even. It is easy to see that the element $g_r \in W_r$ so defined is semi-regular and satisfies the inductive hypothesis.

Let us now define the element h_r. Define an element $f' \in J$ as follows:

$$f'(\omega) := \begin{cases} b_r & \text{if } \omega h_{r-1} = \omega \\ 1 & \text{otherwise.} \end{cases}$$

Let

$$h_r := (f' h_{r-1}).$$

Let us first calculate the number of fixed points h_r has in Σ_r. With the above definition, if h_{r-1} fixes a point $\omega \in \Sigma_{r-1}$ then the class $\Sigma_r(\omega)$ has at most 4 fixed points while if h_{r-1} moves ω then $\Sigma_r(\omega)$ has no fixed points at all. Since by inductive hypothesis (ii) h_{r-1} fixes at most $2^{2(r-1)}$ points of Σ_{r-1} it follows that h_r has at most 2^{2r} fixed points in its action on Σ_r. So, h_r induces at least l_r transpositions on Σ_r where

$$l_r \geq (n_r/2) - 2^{2r-1}.$$

Thus the elements g_r and h_r satisfy the inductive hypotheses on their cycle structures.

It only remains to show that

$$X_r := \langle g_r, h_r \rangle = W_r \, (= J \cdot W_{r-1}).$$

Since g_{r-1} and h_{r-1} generate the whole of W_{r-1} we know that X_r projects onto the whole of W_{r-1}. So we only need to show that $J \leq X_r$. Since g_{r-1} is of order n'_{r-1}, it follows that $g_r^{n'_{r-1}}$ fixes every point of Σ_{r-1} and induces the permutation a_r on every equivalence class of Σ_r. Let us consider the element

$$x := (g_r^{n'_{r-1}})^{-1} h_r g_r^{n'_{r-1}} h_r$$

of Σ_r. It can be expressed as

$$x = (f'' h_{r-1}^2) = f''$$

where

$$f''(\omega) := \begin{cases} a_r^{-1} b_r a_r b_r & \text{if } \omega h_{r-1} = \omega \\ 1 & \text{otherwise.} \end{cases}$$

Since a_r and $[a_r, b_r]$ generate A_{m_r} it follows that the group

$$\langle g_r^{n'_{r-1}}, x \rangle$$

contained in $J \cap X_r$ projects onto one of the factors ($\cong A_{m_r}$) of J. It follows from this and the transitivity of X_{r-1} on Σ_{r-1} that $J \cap X_r$ is a subdirect product of a family of non-abelian simple groups $\{X_\sigma \mid \sigma \in \Sigma_r\}$ with each $X_\sigma \cong A_{m_r}$. As before, such a subdirect product can be expressed as a direct product, say

$$J \cap X_r = D_1 \times D_2 \times \cdots \times D_s$$

where

$$\Sigma_{r-1} = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_s$$

is a partition of Σ_{r-1} and each D_i ($\cong A_{m_r}$) is the diagonal subgroup of the direct product of the family $\{X_\sigma \mid \sigma \in \Omega_i\}$. We need to show that each Ω_i is a singleton. If not, consider the block Ω_i containing ω where ω is left fixed by h_{r-1}. Since

$$\Sigma_{r-1} = \cup_{\delta \in \Sigma_{r-2}} \Sigma_{r-1}(\delta)$$

is the minimal X_r-congruence on Σ_{r-1} the block Ω_i must contain a complete equivalence class $\Sigma_{r-1}(\delta)$ for some $\delta \in \Sigma_{r-2}$. Also, every element of $J \cap X_r$ must induce the same element (up to conjugation) on each of the classes arising from members of Ω_i. But $x \in J \cap X_r$ does not. So

$$J \leq X_r$$

and this completes the induction.

Setting $g = g_k$ and $h = h_k$ it is almost immediate that g and h satisfy all the requirements of the lemma. ∎

4. A probability theorem

After an investigation into the possible conjugacy classes of maximal subgroups M of Y which are such that $M \cdot K = Y$ in the last section we now use the information obtained there in Lemma 2 to evaluate $p(Y)$ in terms of $p(X)$.

LEMMA 8: *If*

$$X = A_{m_k} \operatorname{Wr} A_{m_{k-1}} \operatorname{Wr} \cdots \operatorname{Wr} A_{m_1},$$

acting on Ω *with* $|\Omega| = n = m_k m_{k-1} \cdots m_1$, *each* $m_i \geq 5$, $m_1 \geq 7$ *and*

$$Y := A_m \operatorname{Wr}_\Omega X$$

with $m \geq 5$ *then*

$$p(Y) \geq \Big(1 - \frac{4}{m^{n/5}}\Big) p(X).$$

Proof: From Lemma 2 we have

$$p(Y) \geq \Big(1 - \sum_{j=0}^{7} \frac{d_j}{i_j}\Big) p(X).$$

We put the values of d_r and i_r for $0 \leq r \leq 7$ obtained in the last section in the inequality above. When $m > 21$ we get

$$\sum_{j=0}^{7} \frac{d_j}{i_j} \leq \frac{1}{m^{n/2}} + \frac{4m-2}{m^n} + \frac{1}{2^{m(n-6)}} + \frac{1}{m^{n/5}}$$

where the first term comes from Lemma 3, the second is an upper bound for $\sum_{j=1}^{5} \frac{d_j}{i_j}$ obtained from the observations just before Lemma 5, the third term comes from Lemma 5 and the fourth from Lemma 6 together with the facts that $i_7 = |K|$ and $l \geq (n/2) - 2^{2k-1} \geq n/5$ if $m_1 \geq 7$. Now, each of the first, second and third terms in this case is less than the fourth, so that we have for $m > 21$

$$\sum_{j=0}^{7} \frac{d_j}{i_j} \leq \frac{4}{m^{n/5}}.$$

For $m \leq 21$ we have by a similar argument

$$\begin{aligned} \sum_{j=0}^{7} \frac{d_j}{i_j} &\leq \frac{1}{m^{n/2}} + \frac{(4m-2)+2}{m^n} + \frac{1}{m^{n/5}} \\ &\leq \frac{1}{m^{n/2}} + \frac{1}{m^{n-2}} + \frac{1}{m^{n/5}} \\ &\leq \frac{3}{m^{n/5}} \end{aligned}$$

so that in all cases we have

$$\sum_{j=0}^{7} \frac{d_j}{i_j} \leq \frac{4}{m^{n/5}}. \quad \blacksquare$$

Finally, we use all that we have obtained so far to obtain a theorem regarding the probability of generating an inverse limit of wreath products of alternating groups by two elements. Let

$$W := \varprojlim (A_{m_k} \operatorname{Wr} \cdots \operatorname{Wr} A_{m_1})$$

where $m_1, m_2, \ldots, m_k, \ldots$ are integers ≥ 5.

Being an inverse limit of finite groups W is a profinite group. Compactness of W and Lemma 1 imply that as $n \to \infty$ the probabilities $p(W_n)$ tend to $\mu(S)$, the measure of the set

$$S = \{(g_1, g_2) \in W \times W | \overline{\langle g_1, g_2 \rangle} = W\}$$

with respect to the normalised (that is, by taking $\mu(W) = 1$) Haar measure μ that can be put on W. If we define $p(W)$ to be the probability of generating W by two elements then it follows that $p(W) = \mu(S)$.

Iterating the probabilities by repeated application of Lemma 8 we have,

$$\begin{aligned} p(W_k) &\geq \prod_{i=1}^{k-1} \Big(1 - \frac{4}{m_{i+1}^{(m_1 m_2 \ldots m_i)/5}}\Big) p(W_1) \\ &\geq \prod_{i=1}^{k-1} \Big(1 - \frac{4}{5^{(m_1 m_2 \ldots m_i)/5}}\Big) p(W_1) \\ &\geq \Big(1 - 4 \sum_{i=1}^{k-1} \frac{1}{5^{(m_1 m_2 \ldots m_i)/5}}\Big) p(W_1) \\ &\geq \Big(1 - 4.\frac{2}{5^{m_1/5}}\Big) p(W_1) \end{aligned}$$

provided $m_1 \geq 7$. The cases $m_1 = 5$ and $m_1 = 6$ can be tackled directly to obtain similar bounds.

Let us denote by p_∞ the limit of the probabilities $p(W_k)$ as $k \to \infty$. Then $p_\infty = p(W)$ by the comments made earlier. The calculations above and the fact that $p(W_1) = p(A_{m_1}) > 0$ for all values of m_1 imply that $p(W) > 0$. Moreover, from ([3], Theorem 2) we know that $p(A_m) \to 1$ as $m \to \infty$. What we have just proved shows that $p(W) \to 1$ as $m_1 \to \infty$. This completes the proof of the theorem promised in the introduction.

THEOREM 1: *Let*

$$W = \lim_{\leftarrow}(A_{m_k} \operatorname{Wr} \cdots \operatorname{Wr} A_{m_1})$$

where $m_1, m_2, \ldots, m_k, \ldots$ *are integers* ≥ 5. *The probability that any two elements chosen at random from* W *generate* W *topologically is strictly positive. Furthermore,*

$$p(W) \geq (1 - \varepsilon)p(A_{m_1})$$

where $\varepsilon \to 0$ *as* $m_1 \to \infty$.

ACKNOWLEDGEMENT: This work was done at Oxford University under the supervision of Dr. Peter M. Neumann. The author wishes to thank Dr. Neumann for his help and advice both on the mathematical content of the paper as well as on its presentation.

References

[1] M. Aschbacher and R. Guralnick, *Some applications of the first cohomology group*, J. Algebra **90** (1984), 446–460.

[2] M. Bhattacharjee, *Amalgamated free products and inverse limits of wreath products of groups*, D. Phil. Thesis, Oxford, 1992.

[3] J. D. Bovey, *The probability that some power of a permutation has small degree*, Bull. London Math. Soc. **12** (1980), 47–51.

[4] J. D. Dixon and B. Mortimer, *The primitive permutation groups of degree less than 1000*, Math. Proc. Camb. Phil. Soc. **103** (1988), 213–238.

[5] P. R. Halmos, *Measure Theory*, Springer-Verlag, Berlin, 1988.

[6] Wolfgang Kimmerle, Richard Lyons, Robert Sandling and David N. Teague, *Composition factors from the group ring and Artin's theorem on orders of simple groups*, Proc. London Math. Soc. (3) **60** (1990), 89–122.

[7] C. E. Praeger and J. Saxl, *On the orders of primitive permutation groups*, Bull. London Math. Soc. **12** (1980), 303–307.

[8] L. L. Scott, *Representations in characteristic p*, in *Santa Cruz Conference on Finite Groups*, Proc. Symp. Pure Math., Vol. 37, Amer. Math. Soc., Providence, R.I., 1980, pp. 318–331.

[9] C. C. Sims, *Computational methods in the study of permutation groups*, in *Computational Problems in Abstract Algebra*, Proceedings of a conference (Oxford 1967), (J.Leech, ed.), Pergamon, Oxford, 1970, pp. 169–183.

[10] Helmut Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.