Forum Math. **25** (2013), 867–886
DOI 10.1515/FORM.2011.144
Forum Mathematicum

Characterization of finitely generated infinitely iterated wreath products

Eloisa Detomi and Andrea Lucchini

Communicated by Dan Segal

Abstract. Given a sequence of $(G_i)_{i\in\mathbb{N}}$ of finite transitive groups of degree n_i, let W_∞ be the inverse limit of the iterated permutational wreath products $G_m \wr \cdots \wr G_2 \wr G_1$. We prove that W_∞ is (topologically) finitely generated if and only if $\prod_{i=1}^{\infty}(G_i/G_i')$ is finitely generated and the growth of the minimal number of generators of G_i is bounded by $d \cdot n_1 \cdots n_{i-1}$ for a constant d. Moreover we give a criterion to decide whether W_∞ is positively finitely generated.

Keywords. Generation, wreath product, probability.

2010 Mathematics Subject Classification. Primary 20F05; secondary 20E18, 20E22.

1 Introduction

Let $(G_i)_{i\in\mathbb{N}}$ be a sequence of finite transitive permutation groups of degree n_i and let $W_m = G_m \wr \cdots \wr G_2 \wr G_1$ be the iterated (permutational) wreath product of the first m groups. The infinitely iterated wreath product is the inverse limit

$$W_\infty = \varprojlim_m W_m = \varprojlim_m (G_m \wr \cdots \wr G_2 \wr G_1).$$

In a recent paper Bondarenko [2] studies some sufficient conditions on the sequence $(G_i)_{i\in\mathbb{N}}$ to get that the profinite group W_∞ is (topologically) finitely generated: under the conditions that the minimal number of generators $d(G_i)$ of G_i is bounded by a constant d and $\prod_{i=1}^{\infty}(G_i/G_i')$ is finitely generated, using techniques from branch groups, he produces a finitely generated dense subgroup of W_∞.

Since $\prod_{i=1}^{\infty}(G_i/G_i')$ is a homomorphic image of W_∞, the second condition is clearly also a necessary condition: if W_∞ is generated as a profinite group by d elements, then $d(\prod_{i=1}^{\infty}(G_i/G_i')) \le d$.

Another necessary condition comes from the observation that if K is a finite permutation group of degree n and H is finite, then $d(H) \le n \cdot d(H \wr K)$ (see the remark at the beginning of Section 5). Since $W_i = G_i \wr W_{i-1}$ where W_{i-1} is a permutation group of degree $n_1 n_2 \cdots n_{i-1}$, it follows that if W_∞ is finitely generated by d elements, then $d(G_i) \leq d \cdot n_1 n_2 \cdots n_{i-1}$ for every $i > 1$.

The main result of this paper is that these two necessary conditions are also sufficient.

Theorem 1.1. *Let $(G_i)_{i \in \mathbb{N}}$ be a sequence of transitive permutation groups of degree n_i. The inverse limit W_∞ of the iterated wreath products $G_m \wr \cdots \wr G_2 \wr G_1$ is finitely generated if and only if*

(1) $\prod_{i=1}^{\infty}(G_i/G_i')$ *is finitely generated,*

(2) *there exists an integer d such that $d(G_i) \leq d \cdot n_1 \cdots n_{i-1}$ for every $i > 1$.*

Actually, we prove that there exists an absolute constant k_0 such that

$$d(W_\infty) \leq \max(d+2, d(W_{i_0})) + d\left(\prod_{i=1}^{\infty}(G_i/G_i')\right),$$

where i_0 denotes the first index such that $n_1 \cdots n_{i_0-1} \geq \log_{60} k_0$. Indeed, k_0 is the smallest positive integer with the property: if a finite group L has a unique minimal normal subgroup N and $|N| \geq k_0$, then $P_L(d) \geq \frac{1}{2} P_{L/N}(d)$ for each $d \geq 2$, where $P_L(d)$ (resp. $P_{L/N}(d)$) denotes the probability of generating L (resp. L/N) with d elements. The existence of such a constant is ensured by the main theorem in [19]. On the other hand, we conjecture that for every $d \geq 2$ and every monolithic group L with socle N

$$P_L(d) \geq \frac{53}{90} P_{L/N}(d) \tag{1.1}$$

(equality holds if $L = \mathrm{Alt}(6)$ and $d = 2$). If this were true, our result would become

$$d(W_\infty) \leq \max(d+2, d(G_1)) + d\left(\prod_{i=1}^{\infty}(G_i/G_i')\right).$$

For example, the inequality (1.1) is satisfied if the socle of N is a direct power of alternating or sporadic simple groups [25]: this implies that if every non-abelian composition factor in the transitive permutation groups G_i is alternating or sporadic, then $d(W_\infty) \leq \max(d+2, d(W_1)) + d(\prod_{i=1}^{\infty}(G_i/G_i'))$.

The proof of Theorem 1.1 relies on a generalization to the "non-soluble" case of some results in [15] and [16]. In that papers the author considered the generation of the wreath product $W = H \wr K$ of two finite permutation groups H and K and a formula was found for $d(W)$ in the case where H is soluble. Later, in [4], the minimal number of generators of a group G was connected to some special homomorphic images of G whose behavior can be studied with the help of an equivalence relation among the chief factors of G (see Section 2 for more details). Using these new techniques, we are able to control the "non-abelian" part of the problem and to produce a formula for $d(W)$ whenever the degree of K is large enough.

Infinitely iterated wreath products appear in literature with several motivations. For example they can be viewed as automorphism groups of suitably constructed rooted trees and play a relevant role in the study of self-similar groups (see e.g. [9] and [10]). Moreover, they provide a useful tool to construct examples and counterexamples in the context of profinite groups (see e.g. [20], [24], and [17]). Bhattacharjee [1] and Quick [21,22] considered wreath products of non-abelian simple groups with transitive action and proved that their inverse limit is generated by two elements even with positive probability. Recall that a profinite group G may be viewed as a probability space with respect to the normalized Haar measure and that G is called positively finitely generated (PFG) if for some k a random k-tuple generates G with positive probability. From the papers of Bhattacharjee and Quick, it follows that an infinitely iterated wreath product of transitive groups G_i is PFG when every G_i is a nonabelian simple group. However, in [17] an example is given of an infinitely iterated wreath product of transitive groups that is 2-generated but non-PFG.

In Proposition 6.2, with the help of a result by Jaikin-Zapirain and Pyber [11], we will obtain a criterion that makes it possible to decide whether W_∞ is PFG from information on the structure of the transitive groups G_i and their degree n_i.

2 Generating crown-based powers

Let L be a monolithic primitive group and let A be its unique minimal normal subgroup. For each positive integer k, let L^k be the k-fold direct product of L. The *crown-based power* of L of size k is the subgroup L_k of L^k defined by

$$L_k = \{(l_1, \dots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \bmod A\}.$$

Equivalently, $L_k = A^k \operatorname{Diag} L^k$.

Let, as usual, $d(G)$ denote the minimal number of generators of a finite group G. In [4] it is proved that for every finite group G there exists a monolithic group L and a homomorphic image L_k of G such that

(1) $d(L/\operatorname{soc} L) < d(G)$,

(2) $d(L_k) = d(G)$.

An L_k with this property will be called a *generating crown-based power* for G. In [4] it is explained how $d(L_k)$ can be computed in terms of k and the structure of L. A key ingredient when one wants to determine $d(G)$ from the behavior of the crown-based power homomorphic images of G is to evaluate for each monolithic group L the maximal k such that L_k is a homomorphic image. This integer k comes from an equivalence relation among the chief factors of G. More generally, following [12], we say that two irreducible G-groups A and B are *G-equivalent* and we put $A \sim_G B$ if there is an isomorphism $\Phi : A \rtimes G \to B \rtimes G$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & A \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\ & & \big\downarrow \phi & & \big\downarrow \Phi & & \big\| & & \\ 1 & \longrightarrow & B & \longrightarrow & B \rtimes G & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

Note that two G-isomorphic G-groups are G-equivalent. In the particular case where A and B are abelian the converse is true: if the groups A and B are abelian and G-equivalent, then A and B are also G-isomorphic. It is proved that two chief factors A and B of G are G-equivalent if and only if either they are G-isomorphic between them or there exists a maximal subgroup M of G such that $G/\operatorname{Core}_G(M)$ has two minimal normal subgroups N_1 and N_2 G-isomorphic to A and B respectively. For example, the minimal normal subgroups of L_k are all L_k-equivalent.

Let $A = X/Y$ be a chief factor of G. A complement U to A in G is a subgroup U of G such that $UX = G$ and $U \cap X = Y$. We say that $A = X/Y$ is *Frattini* if X/Y is contained in the Frattini subgroup of G/Y; this is equivalent to saying that A is abelian and there is no complement to A in G. The number $\delta_G(A)$ of non-Frattini chief factors G-equivalent to A in any chief series of G does not depend on the series. Now, we denote by L_A the *monolithic primitive group associated to* A, that is

$$L_A = \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

If A is a non-Frattini chief factor of the group G, then L_A is a homomorphic image of G. More precisely, there exists a normal subgroup N such that $G/N \cong L_A$ and $\operatorname{soc}(G/N) \sim_G A$ (in the following we will sometimes identify $\operatorname{soc} L_A$ with A as G-groups). Consider now all the normal subgroups N with the property that $G/N \cong L_A$ and $\operatorname{soc}(G/N) \sim_G A$: the intersection $R_G(A)$ of all these subgroups has the property that $G/R_G(A)$ is isomorphic to the crown-based power $(L_A)_{\delta_G(A)}$ ($L_{A,\delta_G(A)}$ for short). The socle $I_G(A)/R_G(A)$ of $G/R_G(A)$ is called the *A-crown of G* and it is a direct product of $\delta_G(A)$ minimal normal subgroups G-equivalent to A. Later we will use the facts that

$$I_G(A) = \{g \in G \mid g \text{ induces an inner automorphism on } A\}$$

and $A \sim_G B$ implies $I_G(A) = I_G(B)$. In particular, if A and B are chief factors of G and $A \sim_G B$, then $R_G(A) = R_G(B)$ and $L_A \cong L_B$.

Note that if L_k is a homomorphic image of G for some $k \geq 1$, then L is associated to a non-Frattini chief factor A of G ($L \cong L_A$) and $k \leq \delta_G(A)$. If $L_{A,k}$ is a generating crown-based power, then $L_{A,\delta_G(A)}$ has the same property: in this case, by abuse of notation, we will say that A is a *generating chief factor* for G.

The minimal number of generators of a generating crown-based power can be computed when A is abelian with the help of the following formula: for an irreducible G-module M, set

$$r_G(M) = \dim_{\mathrm{End}_G(M)} M, \quad s_G(M) = \dim_{\mathrm{End}_G(M)} H^1(G, M)$$

and define

$$h_G(M) = \begin{cases} \delta_G(M) & \text{if } M \text{ is a trivial } G\text{-module,} \\ \left\lceil \frac{s_G(M)-1}{r_G(M)} \right\rceil + 2 & \text{otherwise.} \end{cases}$$

Note that, as $G/R \cong L_{M,k}$ where $R = R_G(M)$ and $k = \delta_G(M)$, we obtain $\delta_G(M) = \delta_{G/R}(M) = \delta_{L_{M,k}}(M)$. Moreover, if $\delta_G(M) > 0$, then $R \leq C_G(M)$ and $\dim_{\mathrm{End}_G(M)} H^1(G, M) = \delta_G(M) + \dim_{\mathrm{End}_G(M)} H^1(G/C_G(M), M)$ (see e.g. [1.2] in [16]) and therefore $r_G(M) = r_{G/R}(M)$ and $s_G(M) = s_{G/R}(M)$. We conclude that if $\delta_G(M) > 0$, then

$$h_G(M) = h_{L_{M,\delta_G(M)}}(M). \tag{2.1}$$

From a result by Gaschütz [8, Satz 2], we have either $h_G(M) = d(L_{M,\delta_G(M)})$ or $h_G(M) < d(L_M/M)$. Therefore we have the following:

Proposition 2.1. *If there exists an abelian generating chief factor A for G, then*

$$d(G) = h_G(A).$$

In our discussion we will employ different arguments according to the existence or not of an abelian generating chief factor. In the first case it is useful to notice that

Proposition 2.2. *Let $d(I_G)$ be the minimal number of generators of the augmentation ideal of $\mathbb{Z}G$ as a G-module. If G has an abelian generating chief factor A, then*

$$d(G) = d(I_G) = h_G(A).$$

Proof. By a result of Cossey, Gruenberg and Kovács [3, Theorem 3]

$$d(I_G) = \max\{h_G(M) \mid M \text{ irreducible } G\text{-module}\},$$

thus $d(I_G) \geq h_G(A) = d(G)$. Since $d(I_G) \leq d(G)$, we have an equality. □

Theorem 1.1 will be derived by an extension to the non-abelian crowns of the following:

Proposition 2.3 ([16, Proposition 1]). *If H is a finite group and G is a transitive permutation group of degree n, then*

$$d(I_{H \wr G}) = \max\left\{ d(I_{H/H' \wr G}), \left\lceil \frac{d(I_H) - 2}{n} \right\rceil + 2 \right\}.$$

3 Crowns in wreath products

Let H be a finite group and K be a transitive group of degree n and denote by

$$W = H \wr K = H^n \rtimes K$$

the (permutational) wreath product of H and K, where K permutes the components of the base subgroup $H^n = H_1 \times \cdots \times H_n$.

In this section we want to study the relation between the chief factors of H and the chief factors of W. First note that if A is an H-group, then A^n can be seen as a W-group where H^n acts componentwise and K permutes the components of the elements. When dealing with A^n as a W-group, we will usually refer to this action. We say that an H-group A is *irreducible* if the only H-groups contained in A are A and $\{1\}$; we say that an H-group is *trivial* if the action of H on A is the trivial one, that is, $H = C_H(A)$.

Proposition 3.1. *Let A and B be irreducible H-groups.*

(1) *If A is a non-trivial H-group, then A^n is an irreducible non-trivial W-group.*

(2) *If $A \sim_H B$, then $A^n \sim_W B^n$.*

(3) *If A and B are non-trivial H groups and $A \nsim_H B$, then $A^n \nsim_W B^n$.*

(4) *If A is a non-central chief factor of H and L is the associated monolithic group, then A^n is a chief factor of W and the monolithic primitive group associated to A^n is isomorphic to $L \wr K$.*

Proof. (1) Let $N \neq 1$ be a W-group contained in $A^n = A_1 \times \cdots \times A_n$ and suppose $1 \neq (x_1, \dots, x_n) \in N$ is a non-trivial element. As K is transitive on the components, we can assume $x_1 \neq 1$. Note that $C_A(H)$ is a proper H-subgroup of A, hence $C_A(H) = 1$ by irreducibility of A. Thus we obtain $[x_1, H] \neq 1$ and in particular $[x_1, H]$ is a non-trivial H-subgroup of A, hence $[x_1, H] = A$. Therefore $[(x_1, \dots, x_n), H_1] = [x_1, H] \times \{1\} \times \cdots \times \{1\} = A_1$ is contained in N and, by the transitivity of the action of K, we conclude that $A^n \leq N$.

(2) Let $A \sim_H B$: there exists an isomorphism $\Phi : A \rtimes H \to B \rtimes H$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & A \rtimes H & \longrightarrow & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \Phi} & & \| & & \\ 1 & \longrightarrow & B & \longrightarrow & B \rtimes H & \longrightarrow & H & \longrightarrow & 1. \end{array} \tag{3.1}$$

Now define $\Psi : A^n \rtimes W \to B^n \rtimes W$ by the position

$$((a_1, \dots, a_n)(h_1, \dots, h_n)k)^\Psi = (a_1^\phi, \dots, a_n^\phi)(h_1^\Phi, \dots, h_n^\Phi)k.$$

Thus Ψ is a well-defined isomorphism for which the following diagram is commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A^n & \longrightarrow & A^n \rtimes W & \longrightarrow & W & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \Psi} & & \| & & \\ 1 & \longrightarrow & B^n & \longrightarrow & B^n \rtimes W & \longrightarrow & W & \longrightarrow & 1 \end{array} \tag{3.2}$$

where ψ is the restriction to A^n of Ψ, and therefore $A^n \sim_W B^n$.

(3) Assume, by contradiction, that $A^n \sim_W B^n$. We shall first consider the case where the groups A and B are abelian. Then the W-equivalence relation is simply the W-isomorphism relation and $A^n \sim_W B^n$ implies that there exists a W-isomorphism $\psi : A^n \to B^n$. Note that we have $C_{A^n}(K) = \mathrm{Diag}(A^n) \cong A$ and similarly $C_{B^n}(K) = \mathrm{Diag}(B^n) \cong B$. Since ψ is a W-isomorphism, it follows that the restriction of ψ to $C_{A^n}(K)$ is a W-isomorphism between $C_{A^n}(K) = \mathrm{Diag}(A^n)$ and $C_{B^n}(K) = \mathrm{Diag}(B^n)$. This implies that there is an H-isomorphism between A and B, and we conclude that $A \sim_H B$.

We now consider the case where A and B are non-abelian. Assume that the diagram (3.2) is commutative. First of all we note that the minimal normal subgroups of $A^n \rtimes H^n$ contained in A^n are the subgroups A_i. Moreover the A_i^ψ are minimal normal subgroups of $(A^n \rtimes H^n)^\Psi = B^n \rtimes H^n$ contained in $(A^n)^\psi = B^n$. It follows that $A_i^\psi = B_j$ for some j. In particular, $A \cong B$ as groups.

If $A_1^\psi = B_1$, then consider that $[\prod_{i>1} A_i, H_1] = 1$ implies

$$\left[\prod_{i>1} A_i, H_1\right]^\Psi = \left[\prod_{i>1} A_i^\Psi, H_1^\Psi\right] = \left[\prod_{i>1} B_i, H_1^\Psi\right] = 1$$

thus $H_1^\Psi \leq C_{B^n \rtimes H^n}(\prod_{i>1} B_i)$. Moreover, $H_1^\Psi \leq B^n \rtimes H_1$ since the right part of the diagram (3.2) commutes, and therefore

$$H_1^\Psi \leq C_{B^n \rtimes H^n}\left(\prod_{i>1} B_i\right) \cap \left(B^n \rtimes H_1\right) \leq B_1 \rtimes H_1.$$

It follows that the following diagram commutes,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A_1 & \longrightarrow & A_1 \rtimes H_1 & \longrightarrow & H_1 & \longrightarrow & 1 \\ & & \big\downarrow \psi & & \big\downarrow \Psi & & \big\| & & \\ 1 & \longrightarrow & B_1 & \longrightarrow & B_1 \rtimes H_1 & \longrightarrow & H_1 & \longrightarrow & 1, \end{array}$$

and $A_1 \sim_{H_1} B_1$. Since the action of H on A and B is equal to the action of H_1 on A_1 and B_1 respectively, $A \sim_H B$ and we are done.

We are left with the case $A_1^{\psi} \neq B_1$; then there exists an index $j \neq 1$ such that $A_j^{\psi} = B_1$. Note that we cannot argue as above, since now $A_1^{\psi} \rtimes H_1^{\Psi}$ is contained in $B_1 B_j \rtimes H_1$ but not in $B_j \rtimes H_1$ and hence we cannot simply "restrict" the diagram (3.2) to one component.

Since the right part of the diagram (3.2) commutes, for every $h \in H_1$ there exist unique elements $b_i \in B$ such that $h^{\Psi} = (b_1, \dots, b_n)h$: we define the map $\beta : H_1 \mapsto B_1$ by sending h to the element $h^{\beta} = (b_1, 1 \dots, 1)$. Then $[H_1, A_j] = 1$ implies $[H_1^{\Psi}, B_1] = 1$ and hence $h^{\beta} h$ commutes with every element of B_1. It follows that the map $\Theta : A_j \rtimes H_1 \mapsto B_1 \rtimes H_1$ defined by $(a_j h)^{\Theta} = a_j^{\psi} h^{\beta} h$ is a well-defined homomorphism for which the following diagram is commutative,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A_j & \longrightarrow & A_j \rtimes H_1 & \longrightarrow & H_1 & \longrightarrow & 1 \\ & & \big\downarrow \psi & & \big\downarrow \Theta & & \big\| & & \\ 1 & \longrightarrow & B_1 & \longrightarrow & B_1 \rtimes H_1 & \longrightarrow & H_1 & \longrightarrow & 1, \end{array}$$

and hence $A_j \sim_{H_1} B_1$ (note that the action of H_1 on A_j is the trivial one and it is not equivalent to the action of H on A).

Now, by definition,

$$I_{H_1}(A_j) = \{x \in H_1 \mid x \text{ induces an inner automorphism on } A_j\} = H_1,$$

hence $A_j \sim_{H_1} B_1$ implies $I_{H_1}(B_1) = I_{H_1}(A_j) = H_1$. Then

$$I_W(B^n) = (I_H(B))^n = H^n,$$

and since $B^n \sim_W A^n$, we get $I_W(A^n) = I_w(B^n) = H^n$. Therefore we find that $I_H(A) = H = I_H(B)$. As we will see in the subsequent Lemma 3.2, from the facts that $I_H(A) = H = I_H(B)$ and that $A \cong B$ as groups, we get that A and B are H-equivalent to the same trivial H-group. By transitivity, it follows that $A \sim_H B$ and this gives the desired contradiction.

(4) Let A be a chief factor of H. Then $L \cong H/C_H(A)$ if A is non-abelian, $L \cong A \rtimes H/C_H(A)$ otherwise. Note that $C_W(A^n) \leq \bigcap_{i=1}^n C_W(A_i) \leq H^n$, as the action of K on the components is faithful. Hence $C_W(A^n) = C_H(A)^n$. Then $W/C_W(A^n) \cong (H/C_H(A)) \wr K$ and the result follows. □

Lemma 3.2. *Suppose A is a G-group with trivial center. If $I_G(A) = G$, then A is G-equivalent to the trivial G-group A^*, where $A^* = A$ as a group.*

Proof. This is a consequence of the definition (see the remark after Proposition 1.2 in [12]) and Theorem 11.4.10 in [23], but for the readers' convenience, we will sketch a direct proof.

As A has trivial center and $I_G(A) = G$, there is a homomorphism $f : G \mapsto A$ which send $g \in G$ to the element $f(g)$ in A such that $a^{f(g)} = a^g$ for every $a \in A$. Let A^* be the trivial G-group equal to A as a group. Now we define

$$\Phi : A^* \times G \to A \rtimes G,$$
$$(a, g) \mapsto af(g)^{-1}g.$$

Note that, by definition of f, for every $g \in G$ the element $f(g)^{-1}g$ centralizes the elements of A in $A \rtimes G$. Thus

$$\begin{aligned}((a_1, g_1)(a_2, g_2))^\Phi &= (a_1a_2, g_1g_2)^\Phi = a_1a_2f(g_1g_2)^{-1}g_1g_2 \\ &= a_1(a_2f(g_2)^{-1})(f(g_1)^{-1}g_1)g_2 \\ &= a_1(f(g_1)^{-1}g_1)(a_2f(g_2)^{-1})g_2 \\ &= (a_1, g_1)^\Phi(a_2, g_2)^\Phi,\end{aligned}$$

since $a_2f(g_2)^{-1} \in A$. This shows that Φ is a homomorphism. Then the following diagram is commutative,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A^* & \longrightarrow & A^* \times G & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow \Phi & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & A \rtimes G & \longrightarrow & G & \longrightarrow & 1, \end{array}$$

and we conclude that $A \sim_G A^*$. □

From now on, B will denote the base subgroup H^n of $W = H \wr K = B \rtimes K$. Let us fix a chief series of H passing through the derived subgroup H' of H

$$1 = N_t \lhd N_{t-1} \lhd \cdots \lhd N_{t'} = H' \lhd \cdots \lhd N_1 \lhd N_0 = H. \qquad (3.3)$$

Since every N_i^n is normal in W, we can refine the series $(N_i^n)_i$ to get a W-chief series of B passing through the derived subgroup B'

$$1 = M_{s_t} \lhd \cdots \lhd M_{s_{t'}} = N_{t'}^n = B' \lhd \cdots \lhd M_1 \lhd M_0 = B. \qquad (3.4)$$

For every prime p, let $d_p(H/H')$ be the minimal number of generators of the Sylow p-subgroup of H/H'. Note that $d_p(H/H') = h_{H/H'}(A)$ where A is a central non-Frattini chief-factor of H/H' of order p. Moreover, if $A = X/Y$ is a central non-Frattini (i.e., complemented) chief-factor of H, then X cannot be contained in H'; therefore

$$d_p(H/H') = h_H(\mathbb{F}_p) = h_{H/H'}(\mathbb{F}_p) \tag{3.5}$$

where $A \sim_H \mathbb{F}_p$ and $\mathbb{F}_p$ is the irreducible trivial $\mathbb{F}_p H$-module.

Proposition 3.3. *Suppose $M = M_i/M_{i+1}$ is a non-Frattini chief factor of the series* (3.4).

(1) *If $M_i \le B'$, then there is a non-Frattini chief factor $A = X/Y$ of the series* (3.3) *contained in H' such that $M = X^n/Y^n$. Moreover M is not W-equivalent to any chief factor of W/B', $\delta_W(M) = \delta_H(A)$ and $L_M \cong L_A \wr K$.*

(2) *If $B' \le M_{i+1} < M_i \le B$, then*

$$\delta_W(M) \le \delta_K(M) + d_p(H/H')r_K(M),$$

where p is the exponent of M.

(3) *If $B \le M_{i+1}$, and M is not equivalent to any W-chief factor of B/B', then the action of W on M induces an action of K on M, $\delta_W(M) = \delta_K(M)$ and the primitive monolithic group associated to M is the same in the two actions.*

Proof. (1) We first prove that the map $A = X/Y \mapsto A^n = X^n/Y^n$ gives a bijection between the set of non-Frattini chief factors of the series (3.3) contained in H' and the set of non-Frattini chief factors of the series (3.4) contained in B'.

Let $A = X/Y$ be a non-Frattini chief factor of the series (3.3) contained in H'. Note that the central complemented chief factors of (3.3) lie above H'. Then A is not central and hence, by Proposition 3.1, we have that A^n is a non-central chief factor of the series (3.4) contained in B'. Moreover, if U is a complement to A in H, then $U \wr K$ is a complement to A^n in W. This implies that the map is well defined.

To prove that the map is bijective, it is sufficient to show that if $A = N_i/N_{i+1}$ is a Frattini chief factor of H, then every chief factor X/Y of the series (3.4) with $N_{i+1}^n \le Y < X \le N_i^n$ is Frattini. We can assume $N_{i+1} = 1$; thus $A \le \operatorname{Frat} H$ and $A^n \le (\operatorname{Frat} H)^n = \operatorname{Frat} B \le \operatorname{Frat} W$ and we are done.

To prove that $\delta_H(A) = \delta_W(A^n)$ it is sufficient to show that A^n cannot be equivalent to any W-chief factor containing B', indeed, from Proposition 3.1, we already know there are $\delta_H(A)$ chief factors of (3.4) which are W-equivalent to A^n

inside B'. Assume, by contradiction, that $A^n \sim_W M = X/Y$ where $B' \le Y \le X \le W$. Then $I_W(A^n) = I_W(M)$. But, on one hand, $I_W(A^n) = (I_H(A))^n \le B$, on the other hand $I_W(M) = XC_W(X)$. This implies $X \le B$ and $I_W(M) = B$. In particular, as $B' \le Y$, M is centralized by B. Therefore the two factors A^n and M are abelian, the equivalence relation reduces to a W-isomorphism and hence A^n is centralized by B. It follows that A is a central factor of H, but this is a contradiction, since complemented central chief factors of (3.3) lie above H'.

Finally, by Proposition 3.1, we get that $L_M = L_A \wr K$.

(2) Set $\overline{H} = H/H'$ and note that $B \le C_W(M)$, hence the action of W on M induces an action of K on M. We follow the arguments of Lemma 2.1 in [15] and Lemma 4.1 in [16]. Since we are dealing with non-Frattini factors, we can assume that the Frattini subgroup of $\overline{H}$ is trivial. The Sylow p-subgroup $\overline{H}_p$ of $\overline{H}$ is a vector space of dimension $d = d_p(\overline{H})$ generated, say, by the elements $h_1, \dots, h_d$. Then the Sylow p-subgroup $\overline{H}_p^n$ of $\overline{H}^n$ is generated, as an $\mathbb{F}_p K$-module, by the elements $(h_i, 1, \dots, 1)$. In particular, $\overline{H}^n$ is the direct sum of d cyclic $\mathbb{F}_p K$-modules, and the number of complemented $\mathbb{F}_p K$-modules K-equivalent to M in $\overline{H}^n$ is at most $d_p(\overline{H}) r_K(M)$ where $r_K(M) = \dim_{\mathrm{End}_K(M)}(M)$ (see [15, Lemma 2.1]). It follows that $\delta_W(M) \le \delta_K(M) + d_p(\overline{H}) r_K(M)$.

(3) It is sufficient to note that $B \le C_W(M)$ and that, by the first part of the proposition, M cannot be equivalent to any chief factor contained in B'. □

Now we consider non-trivial W-modules (abelian W-groups) and the values of the function h_W on them.

Proposition 3.4. *Let p be a prime and M be a non-trivial irreducible $\mathbb{F}_p W$-module.*

(1) *If M is W-equivalent to a non-Frattini W-chief factor contained in B', then there exists a non-trivial irreducible $\mathbb{F}_p H$-module U such that $M \sim_W U^n$ and $h_W(M) \le \lceil \frac{h_H(U)-2}{n} \rceil + 2$.*

(2) *If M is W-equivalent to a non-Frattini W-chief factor of B/B', then we have $h_W(M) \le h_K(M) + d_p(H/H')$.*

(3) *If M is not W-equivalent to any non-Frattini W-chief factor of B but satisfies $\delta_W(M) = \delta_K(M) \ge 1$, then $h_W(M) = h_K(M)$.*

(4) *If $\delta_W(M) = 0$, then $h_W(M) \le 2$.*

Proof. (1) The first part follows from Propositions 3.3, the bound of $h_W(M)$ is proved in [16, step 2.5].

(2) Since M is W-equivalent to a chief factor of B/B', B centralizes M and hence $r_W(M) = r_K(M)$. Let $\overline{H} = H/H'$. From Proposition 3.3 we conclude

that $\delta_W(M) \le \delta_K(M) + d_p(\overline{H}) r_K(M)$. Moreover (see (1.2) in [16]),

$$\begin{aligned} s_W(M) &= \delta_W(M) + \dim_{\mathrm{End}_W(M)} H^1(W/C_W(M), M) \\ &\le \delta_K(M) + d_p(\overline{H}) r_K(M) + \dim_{\mathrm{End}_K(M)} H^1(K/C_K(M), M) \\ &= d_p(\overline{H}) r_K(M) + s_K(M). \end{aligned}$$

Therefore,

$$\begin{aligned} h_W(M) &= \left\lceil \frac{s_W(M)-1}{r_W(M)} \right\rceil + 2 \le \left\lceil \frac{d_p(\overline{H}) r_K(M) + s_K(M) - 1}{r_K(M)} \right\rceil + 2 \\ &\le h_K(M) + d_p(\overline{H}). \end{aligned}$$

(3) Since $\delta_W(M) = \delta_K(M) \ge 1$, it follows that M is not equivalent to any chief factor contained in B and hence B is contained in $R_W(A)$ where A is a chief factor W-equivalent to M (every minimal normal subgroup of $W/R_W(A)$ is W-equivalent to A). By the same arguments used to prove equation (2.1), it follows that $h_W(M) = h_{W/B}(M) = h_K(M)$.

(4) This is proved in Lemma 1.5 of [14]. □

4 Number of generators of wreath products

Let L be a monolithic primitive group with socle N. Let us denote by $P_L(d)$ (resp. $P_{L/N}(d)$) the probability of generating L (resp. L/N) with d elements, and, for $d \ge d(L)$, let

$$P_{L,N}(d) = P_L(d)/P_{L/N}(d).$$

When N is non-abelian, the formula given in [4] to evaluate $d(L_t)$ is the following:

Theorem 4.1 ([4, Theorem 2.7]). *Let L be a monolithic primitive group with non-abelian socle N and let $d \ge d(L)$. Then $d(L_t) \le d$ if and only if*

$$t \le \frac{P_{L,N}(d)|N|^d}{|C_{\mathrm{Aut}\, L}(L/N)|}.$$

In Theorem 1.1 in [19] it is proved that if $|N|$ is large enough and $d \ge 2$ random elements generate L modulo N, then these elements almost certainly generate L itself:

Theorem 4.2 ([19, Theorem 1.1]). *There exists a positive integer k_0 such that, if L is a monolithic primitive group with socle N and $|N| \ge k_0$, then for every $d \ge d(L)$ we have $P_{L,N}(d) \ge 1/2$.*

Proposition 4.3. *Let L be a monolithic primitive group with a non-abelian socle N, let K be a transitive group of degree n and set $L^* = L \wr K$. Assume that $|N|^n \geq k_0$. For every positive integer t and every integer $d \geq d(L^*/\operatorname{soc} L^*) - 2$, if $d(L_t) \leq d \cdot n$, then $d(L^*_t) \leq d + 2$.*

Proof. Since L_t can be generated by nd elements, by Theorem 4.1 we have that

$$t \leq \frac{P_{L,N}(nd)|N|^{nd}}{|C_{\operatorname{Aut} L}(L/N)|}.$$

As $N \leq C_{\operatorname{Aut} L}(L/N)$ and $P_{L,N}(nd) \leq 1$, we deduce $t \leq |N|^{nd-1}$.

Now, again by Theorem 4.1, to prove that $d(L^*_t) \leq d + 2$, it is sufficient to prove that

$$t \leq \frac{P_{L^*,M}(d+2)|M|^{d+2}}{|C^*|}$$

where $M = \operatorname{soc} L^*$ and $C^* = C_{\operatorname{Aut} L^*}(L^*/M)$. By assumption, we obtain that $d + 2 \geq \max(d(L^*/M), 2) = d(L^*)$, where the last equation follows from [18]. Moreover, we have that $|M| = |N|^n \geq k_0$. Thus we can apply Theorem 4.2 to get the inequality $P_{L^*,M}(d+2) \geq 1/2$. Moreover, if $N = S^a$, where S is a simple non-abelian group and a is a positive integer, from the proof of Lemma 1 in [5], $|C^*| \leq na|S|^{na-1}|\operatorname{Aut} S| \leq na|S|^{na+1}$. It follows that

$$\frac{P_{L^*,M}(d+2)|M|^{d+2}}{|C^*|} \geq \frac{1}{2} \cdot \frac{|M|^{d+2}}{na|S|^{na+1}}.$$

As $t \leq |N|^{nd-1}$ and $M = N^n$, it is sufficient to check that $\frac{|N|^{n(d+2)}}{2na|S|^{na+1}} \geq |N|^{nd-1}$, that is,

$$|N|^{2n+1} = |S|^{2na+a} \geq 2na|S|^{na+1},$$

and this follows from the fact that $|S| \geq 60$. □

Proposition 4.4. *Let K be a transitive permutation group of degree $n \geq \log_{60} k_0$, where k_0 is the constant defined in Theorem 4.2. Then*

$$d(H \wr K) \leq \max\left(d(H/H' \wr K), \left\lceil \frac{d(H)}{n} \right\rceil + 2\right).$$

Proof. Set $\overline{H} = H/H'$. When $W = H \wr K$ has an abelian generating chief factor, by Proposition 2.2 we have $d(G) = d(I_G)$, and then the result follows from Proposition 2.3:

$$\begin{aligned} d(W) = d(I_W) &= \max\left(d(I_{\overline{H}\wr K}), \left\lceil \frac{d(I_H) - 2}{n} \right\rceil + 2\right) \\ &\leq \max\left(d(\overline{H} \wr K), \left\lceil \frac{d(H)}{n} \right\rceil + 2\right). \end{aligned}$$

Now we assume that every generating chief factor is non-abelian and we argue by induction on $|H|$, the case $|H| = 1$ being obviously true. Let M be a non-abelian generating chief factor of the series (3.4). If M is not contained in B', then, by Proposition 3.3, M is a K-group such that $\delta_W(M) = \delta_K(M)$ and the crown-based power $L_{M,\delta_W(M)}$ is a homomorphic image of K. Therefore

$$d(W) = d(L_{M,\delta_W(M)}) \le d(K) \le d(\overline{H} \wr K)$$

and the result follows.

We are left with the case where M is a non-abelian chief factor contained in B'. From Proposition 3.3 we know that there exists a non-abelian chief factor N of the series (3.3) such that $\delta_W(M) = \delta_H(N)$ and $L_M \cong L_N \wr K$. Set $L = L_N$, $L^* = L \wr K$ and $\delta = \delta_H(N)$.

Let $d_0 = \max(d(\overline{H} \wr K), \lceil \frac{d(H)}{n} \rceil + 2)$; we want to apply Proposition 4.3 to prove that $d(W) = d(L^*_\delta) \le d_0$. As $|L/N| < |H|$, by induction we get

$$d(L/N \wr K) \le \max\left(d(L/L' \wr K), \left\lceil \frac{d(L/N)}{n} \right\rceil + 2 \right).$$

Since L/L' is a homomorphic image of $\overline{H}$ and $L^*/M = L/N \wr K$, we deduce that

$$d(L^*/M) = d(L/N \wr K) \le \max\left(d(\overline{H} \wr K), \left\lceil \frac{d(H)}{n} \right\rceil + 2 \right) = d_0.$$

Moreover, $d_0 \ge \lceil \frac{d(H)}{n} \rceil + 2$, i.e., $n(d_0 - 2) \ge d(H) \ge d(L_\delta)$. Also, the assumption $n \ge \log_{60} k_0$ gives $|N|^n \ge k_0$. Thus all the hypotheses of Proposition 4.3 are satisfied (for $d = d_0 - 2$) and we conclude that $d(W) = d(L^*_\delta) \le d_0$. □

The previous result reduces the problem of finding a bound to $d(W)$ to the case where H is an abelian group. Let

$$\rho_{K,H,p} = \max_M h_K(M) + d_p(H/H')$$

where the subscript M ranges over the set of non-trivial irreducible $\mathbb{F}_p K$-modules, with $\rho_{K,H,p} = 0$ if every irreducible $\mathbb{F}_p K$-module is trivial.

Proposition 4.5. *If H is abelian, then $d(H \wr K) \le \max_{p \mid |H|}(d(H \times K), \rho_{K,H,p})$.*

Proof. Let $W = H \wr K$ and let M be a generating chief factor for W.

If M is non-abelian, then M cannot be W-equivalent to any chief factor of $B = H^n$, hence $R_W(M) \ge B$ and $L_{M,\delta_W(M)}$ is a homomorphic image of K. It follows that

$$d(W) = d(L_{M,\delta_W(M)}) \le d(K) \le d(H \times K)$$

and we are done.

Now, let us assume that M is abelian. If M is central, by equation (3.5) it follows that $h_W(M) = h_{W/W'}(M) \le d(W/W') \le d(H \times K)$ since $W/[B,K] \cong H \times K$. Thus $d(W) = h_W(M) \le d(H \times K)$ and the result follows.

Then we are left with the case where M is non-central. By Proposition 3.4 (both (2) and (3)), $h_W(M) \le h_K(M) + d_p(H)$ and therefore

$$d(W) = h_W(M) \le \rho_{K,H,p}.$$

This completes the proof. □

5 Iterated wreath products

Note that if K is a permutation group of degree n, then $d(H) \le n \cdot d(H \wr K)$; indeed, given a set

$$\{g_i = (h_{i,1}, \dots, h_{i,n})k_i \mid h_{i,j} \in H,\, k_i \in K,\, i = 1, \dots, d\}$$

of generators for $H \wr K$, then the group H can be generated by the elements $\{h_{i,j} \mid j = 1, \dots, n,\, i = 1, \dots, d\}$. Moreover,

$$d(H \wr K) \ge d(H/H' \times K/K')$$

since $H/H' \times K/K'$ is a homomorphic image of $H \wr K$.

This shows the "only if" implication of Theorem 1.1. The other implication is proved in the following theorem.

Theorem 5.1. *Let $(G_i)_{i\in\mathbb{N}}$ be a sequence of transitive permutation groups of degree n_i. Let $\overline{G}_i = G_i/G_i'$ and denote by $W_m = G_m \wr \cdots \wr G_1$ the iterated permutational wreath product of the first m groups. Assume that there exist two integers c and d with*

(i) $d(\prod_{i=1}^{\infty} \overline{G}_i) = c$,

(ii) $d(G_i) \le d \cdot n_1 \cdots n_{i-1}$ *for every* $i > 1$.

Then, for $e = \max(d+2, d(W_{i_0}))$, where i_0 is the first index such that the degree $n_1 \cdots n_{i_0}$ of W_{i_0} is at least $\log_{60}(k_0)$, we get the following:

(1) *If M is a non-trivial irreducible $\mathbb{F}_p W_m$-module, where $m \ge i_0$, then*

$$h_{W_m}(M) \le e + d_p\left(\prod_{i=i_0}^{m} \overline{G}_i\right).$$

(2) $d(W_m) \le e + d(\prod_{i=i_0}^{m} \overline{G}_i)$ *for every* $m \ge i_0$.

(3) *The inverse limit of the iterated wreath products W_m is finitely generated and* $d(\varprojlim_m W_m) \le e + c$.

Proof. (1) We argue by induction on m. The case $m = i_0$, is trivial since

$$h_{W_{i_0}}(M) \le d(W_{i_0}) \le e.$$

So let $m > i_0$ and let M be a non-trivial irreducible $\mathbb{F}_p W_m$-module. By Proposition 3.4 applied to $W_m = G_m \wr_n W_{m-1}$, where $n = n_1 \cdots n_{m-1}$ is the degree of W_{m-1}, we get that either $h_{W_m}(M) \le \lceil \frac{h_{G_m}(U)-2}{n} \rceil + 2$ for an $\mathbb{F}_p G_m$-module U contained in G'_m, or $h_{W_m}(M) \le h_{W_{m-1}}(M) + d_p(\overline{G}_m)$; thus

$$h_{W_m}(M) \le \max\left(\left\lceil \frac{h_{G_m}(U) - 2}{n} \right\rceil + 2, h_{W_{m-1}}(M) + d_p(\overline{G}_m)\right).$$

Since $h_{G_m}(U) \le d(G_m) \le dn$ implies $\lceil \frac{h_{G_m}(U)-2}{n} \rceil + 2 \le d + 2$, and, by inductive hypothesis

$$h_{W_{m-1}}(M) \le e + d_p\left(\prod_{i=i_0}^{m-1} \overline{G}_i\right),$$

we get

$$h_{W_m}(M) \le \max\left(d + 2, e + d_p\left(\prod_{i=i_0}^{m-1} \overline{G}_i\right) + d_p(\overline{G}_m)\right) \le e + d_p\left(\prod_{i=i_0}^{m} \overline{G}_i\right).$$

(2) Again, we argue by induction on m, the case $m = i_0$ being trivial.

So let $m > i_0$, that is, $n = n_1 \cdots n_{m-1} > \log_{60}(k_0)$. Proposition 4.4 applied to $W_m = G_m \wr_n W_{m-1}$ gives

$$\begin{aligned} d(W_m) &\le \max\left(d(\overline{G}_m \wr W_{m-1}), \left\lceil \frac{d(G_m)}{n} \right\rceil + 2\right) \\ &\le \max\left(d(\overline{G}_m \wr W_{m-1}), d + 2\right). \end{aligned} \tag{5.1}$$

Then we apply Proposition 4.5 to have

$$d(\overline{G}_m \wr W_{m-1}) \le \max_{p \| \overline{G}_m|}\left(d(\overline{G}_m \times W_{m-1}), \rho_{W_{m-1},G_m,p}\right), \tag{5.2}$$

where

$$\rho_{W_{m-1},G_m,p} = \max_M \left(h_{W_{m-1}}(M)\right) + d_p(\overline{G}_m)$$

and M ranges over the set of non trivial irreducible $\mathbb{F}_p W_{m-1}$-modules, with

$$\rho_{W_{m-1},G_m,p} = 0$$

if every irreducible $\mathbb{F}_p W_{m-1}$-module is trivial. By part (1) of this theorem,

$$h_{W_{m-1}}(M) \le e + d_p\left(\prod_{i=i_0}^{m-1} \overline{G}_i\right),$$

and hence

$$\rho_{W_{m-1},G_m,p} \leq e + d_p\left(\prod_{i=i_0}^{m-1} \overline{G}_i\right) + d_p(\overline{G}_m) = e + d_p\left(\prod_{i=i_0}^{m} \overline{G}_i\right). \tag{5.3}$$

Moreover, note that a crown-based power homomorphic image of $\overline{G}_m \times W_{m-1}$ is either a homomorphic image of W_{m-1} or a homomorphic image of $\overline{G}_m \times \overline{W}_{m-1}$ (in the latter case it is associated to a central chief factor). This implies that

$$\begin{aligned} d(\overline{G}_m \times W_{m-1}) &\leq \max\Big(d(\overline{G}_m \times \overline{W}_{m-1}), d(W_{m-1})\Big) \\ &\leq \max\left(d\left(\prod_{i=1}^{m} \overline{G}_i\right), d(W_{m-1})\right). \end{aligned}$$

By inductive hypothesis, we get $d(W_{m-1}) \leq e + d(\prod_{i=i_0}^{m-1} \overline{G}_i)$, and therefore

$$\begin{aligned} d(\overline{G}_m \times W_{m-1}) &\leq \max\left(d\left(\prod_{i=1}^{m} \overline{G}_i\right), e + d\left(\prod_{i=i_0}^{m-1} \overline{G}_i\right)\right) \\ &\leq e + d\left(\prod_{i=i_0}^{m} \overline{G}_i\right). \end{aligned} \tag{5.4}$$

From (5.2), (5.3) and (5.4), we obtain that

$$\begin{aligned} d(\overline{G}_m \wr W_{m-1}) &\leq \max_{p \| |\overline{G}_m|} \Big(d(\overline{G}_m \times W_{m-1}), \rho_{W_{m-1},G_m,p}\Big) \\ &\leq \max_{p \| |\overline{G}_m|} \left(e + d\left(\prod_{i=i_0}^{m} \overline{G}_i\right), e + d_p\left(\prod_{i=i_0}^{m} \overline{G}_i\right)\right) \\ &\leq e + d\left(\prod_{i=i_0}^{m} \overline{G}_i\right). \end{aligned}$$

Since $d + 2 \leq e$, from (5.1) we conclude that

$$\begin{aligned} d(W_m) &\leq \max\Big(d(\overline{G}_m \wr W_{m-1}), d + 2\Big) \\ &\leq e + d\left(\prod_{i=i_0}^{m} \overline{G}_i\right). \end{aligned}$$

(3) This follows directly from (2) and the assumption that $d(\prod_{i=1}^{\infty} \overline{G}_i) = c$. Indeed, $d(W_m) \leq e + d(\prod_{i=i_0}^{m} \overline{G}_i) \leq e + c$ for every m, and the same bound applies to the generating number of their inverse limit. □

6 Probability of generating an iterated wreath product

Once we know that a profinite group G is finitely generated, it is natural to ask about the probability to find a set of generators for the group. A profinite group G is called *Positively Finitely Generated* (PFG) if there exists an integer $t \geq d(G)$ such that a randomly chosen t-tuple generates G with positive probability.

Note that it is possible to extend the definitions of G-equivalence and crowns to profinite groups (see [7]). Moreover, if G is finitely generated, then $\delta_G(A)$ is finite for every finite irreducible G-group A and in particular this holds for the chief factors of G (cf. [7, Theorem 12]). Recently, Jaikin-Zapirain and Pyber gave a characterization of PFG-groups in terms of non-abelian crowns:

Theorem 6.1 (Jaikin-Zapirain, Pyber [11]). *A finitely generated profinite group G is PFG if and only if there exists a constant c such that for every non-abelian chief factor A of G,*

$$\delta_G(A) \leq l(A)^c$$

where $l(A)$ is the minimal degree of a faithful transitive representation of A.

This statement allows us to characterize PFG infinitely iterated permutational wreath products.

Proposition 6.2. *Let $(G_i)_{i\in\mathbb{N}}$ be a sequence of transitive permutation groups of degree n_i. Assume that the inverse limit W_∞ of the iterated permutational wreath products $W_m = G_m \wr \cdots \wr G_1$ is finitely generated. Then W_∞ is PFG if and only if there exists a constant c such that for every non-abelian chief factor A of G_i and for every $i > 1$,*

$$\delta_{G_i}(A) \leq l(A)^{cn_1\cdots n_{i-1}}.$$

Proof. Let M be a non-abelian chief factor of $W = W_\infty$ such that $\delta_W(M) > 0$. Since $\delta_W(M)$ does not depend on the chosen chief series and is finite (Theorems 11 and 12 in [7]), we get $\delta_W(M) = \delta_{W_i}(M)$ for some i; let i be the smallest integer with this property. Without loss of generality we can assume $i > 1$. Since $\delta_{W_{i-1}}(M) < \delta_{W_i}(M)$, it follows that M is equivalent to a non-abelian chief factor of $B = G_i^n$, the base subgroup of $W_i = G_i \wr W_{i-1}$, where $n = n_1 \cdots n_{i-1}$ is the degree of W_{i-1}. In particular, M is equivalent to a non-abelian chief factor contained in B', and from Proposition 3.3 it follows that there exists a non-abelian chief factor A of G_i such that $M \sim_{W_i} A^n$ and $\delta_{W_i}(M) = \delta_{G_i}(A)$. Since $l(M) = l(A)^n$ (see Proposition 5.2.7 in [13] and the comments afterwards), the result follows from the characterization of PFG-groups given by Jaikin-Zapirain and Pyber (Theorem 6.1). □

Bibliography

[1] M. Bhattacharjee, The probability of generating certain profinite groups by two elements, *Israel J. Math.* **86** (1994), no. 1–3, 311–329.

[2] I. V. Bondarenko, Finite generation of iterated wreath products, *Arch. Math. (Basel)* **95** (2010), no. 4, 301–308.

[3] J. Cossey, K. W. Gruenberg and L. G. Kovács, The presentation rank of a direct product of finite groups, *J. Algebra* **28** (1974), 597–603.

[4] F. Dalla Volta and A. Lucchini, Finite groups that need more generators than any proper quotient, *J. Aust. Math. Soc. Ser. A* **64** (1998), 82–91.

[5] F. Dalla Volta and A. Lucchini, The smallest group with non-zero presentation rank, *J. Group Theory* **2** (1999), no. 2, 147–155.

[6] E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group, *J. Algebra* **265** (2003) 651–668.

[7] E. Detomi and A. Lucchini, Crowns in profinite groups and applications, in: *Noncommutative Algebra and Geometry*, pp. 47–62, Lecture Notes in Pure and Applied Mathematics 243, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[8] W. Gaschütz, Die Eulersche Funktion endlicher auflösbarer Gruppen, *Illinois J. Math.* **3** (1959), 469–476.

[9] R. I. Grigorchuk, Branch groups, *Math. Notes* **67** (2000), no. 5–6, 718–723.

[10] R. I. Grigorchuk, Solved and unsolved problems around one group, in: *Infinite Groups: Geometric, Combinatorial and Dynamical Aspects*, pp. 117–218, Progress in Mathematics 248, Birkhäuser-Verlag, Basel, 2005.

[11] A. Jaikin Zapirain and L. Pyber, Random generation of finite and profinite groups and group enumeration, *Ann. of Math. (2)* **173** (2011), 769–814.

[12] P. Jiménez-Seral and J. Lafuente, On complemented nonabelian chief factors of a finite group, *Israel J. Math.* **106** (1998), 177–188.

[13] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series 129, Cambridge University Press, Cambridge, 1990.

[14] A. Lucchini, Some questions on the number of generators of a finite group, *Rend. Semin. Mat. Univ. Padova* **83** (1990), 201–222.

[15] A. Lucchini, Generating wreath products, *Arch. Math. (Basel)* **62** (1994), no. 6, 481–490.

[16] A. Lucchini, Generating wreath products and their augmentation ideals, *Rend. Semin. Mat. Univ. Padova* **98** (1997), 67–87.

[17] A. Lucchini, A 2-generated just-infinite profinite group which is not positively generated, *Israel J. Math.* **141** (2004), 119–123.

[18] A. Lucchini and F. Menegazzo, Generators for finite groups with a unique minimal normal subgroup, *Rend. Semin. Mat. Univ. Padova* **98** (1997), 173–191.

[19] A. Lucchini and F. Morini, On the probability of generating finite groups with a unique minimal normal subgroup, *Pacific J. Math.* **203** (2002), no. 2, 429–440.

[20] P. Neumann, Some questions of Edjvet and Pride about infinite groups, *Illinois J. Math.* **30** (1986), no. 2, 301–316.

[21] M. Quick, Probabilistic generation of wreath products of non-abelian finite simple groups, *Comm. Algebra* **32** (2004), no. 12, 4753–4768.

[22] M. Quick, Probabilistic generation of wreath products of non-abelian finite simple groups, II. *Internat. J. Algebra Comput.* **16** (2006), no. 3, 493–503.

[23] D. J. S. Robinson, *A Course in the Theory of Groups*, Graduate Texts in Mathematics 80, Springer-Verlag, New York, Berlin, 1982.

[24] D. Segal, The finite images of finitely generated groups, *Proc. Lond. Math. Soc. (3)* **82** (2001), no. 3, 597–613.

[25] E. Zonta, *La probabilità di generazione nei gruppi finiti con un unico normale minimo*, Master thesis, University of Padova, 2011.

Received April 20, 2011; revised June 23, 2011.

Author information

Eloisa Detomi, Dipartimento di Matematica Pura ed Applicata, Università di Padova,
Via Trieste 63, 35121 Padova, Italy.
E-mail: detomi@math.unipd.it

Andrea Lucchini, Dipartimento di Matematica Pura ed Applicata, Università di Padova,
Via Trieste 63, 35121 Padova, Italy.
E-mail: lucchini@math.unipd.it