BOUNDED GENERATION AND SECOND BOUNDED COHOMOLOGY OF WREATH PRODUCTS

IGOR V. EROVENKO, NIKOLAY NIKOLOV, AND B. SURY

ABSTRACT. We show that the (standard restricted) wreath product of groups is boundedly generated if and only if the bottom group is boundedly generated and the top group is finite. We also establish a criterion for triviality of the singular part of second bounded cohomology of wreath products.

1. INTRODUCTION

Wreath products of groups (for definitions and notation see §2) naturally arise in the study of Sylow subgroups of appropriate symmetric groups. They also often provide examples of certain groups with rather unexpected properties. The goal of this paper is to investigate bounded generation and bounded cohomology of (standard restricted) wreath products of groups.

An abstract group G is said to have *bounded generation* if there exist (not necessarily distinct) elements $g_1, \dots, g_k \in G$ such that $G = \langle g_1 \rangle \cdots \langle g_k \rangle$, where $\langle g_i \rangle$ is the cyclic subgroup generated by g_i. Even though defined as a simple combinatorial notion, bounded generation turns out to imply a number of remarkable structural properties:

- the pro-p completion of a boundedly generated group is a p-adic analytic group for every prime p [4, 13];
- if a boundedly generated group G has property (FAb), then it has only finitely many inequivalent completely reducible representations in every dimension over any field (see [14, 20, 21] for representations in characteristic zero, and [1] for arbitrary characteristic);
- if G is a boundedly generated S-arithmetic subgroup of an absolutely simple simply connected algebraic group over a number field, then G has the congruence subgroup property [15, 19];
- bounded generation can be used to find explicit Kazhdan constants [11, 22].

We establish the following criterion for bounded generation of wreath products.

Theorem 1.1 *If A and B are groups then $A \wr B$ has bounded generation if and only if A has bounded generation and B is finite.*

We remark that the question of bounded generation of complete wreath products is trivial: if B is finite, then the complete wreath product is the same as the restricted wreath product, and if B is infinite, then the complete wreath product $A \,\mathrm{Wr}\, B$ is not finitely generated, hence cannot be boundedly generated.

Bounded cohomology $H_b^*(G)$ of a group G (we will be considering only cohomology with coefficients in the additive group of reals $\mathbb{R}$ with trivial action, so in our notations for cohomology the coefficient module will be omitted) is defined using the complex

$$\cdots \longleftarrow C_b^{n+1}(G) \xleftarrow{\delta_b^n} C_b^n(G) \longleftarrow \cdots \longleftarrow C_b^2(G) \xleftarrow{\delta_b^1} C_b^1(G) \xleftarrow{\delta_b^0=0} \mathbb{R} \xleftarrow{\delta_b^{-1}=0} 0$$

of bounded cochains $f\colon G\times\cdots\times G\to\mathbb{R}$, and $\delta_b^n=\delta^n|_{C_b^n(G)}$ is the bounded differential operator. Since $H_b^0(G)=\mathbb{R}$ and $H_b^1(G)=0$ for any group G, investigation of bounded cohomology starts in dimension 2. One observes that $H_b^2(G)$ contains a subspace $H_{b,2}^2(G)$ (called the singular part of the second bounded cohomology group), which has a simple algebraic description in terms of quasicharacters and pseudocharacters, and the quotient space $H_b^2(G)/H_{b,2}^2(G)$ is canonically isomorphic to the bounded part of the ordinary cohomology group $H^2(G)$. For background on bounded cohomology of groups see [6], for bounded cohomology of topological spaces see [7]. Special interest in $H_{b,2}^2$ is motivated in part by its connections with other structural properties of groups such as commutator length [2] and bounded generation [6]. In particular, it is important to know when $H_{b,2}^2$ vanishes.

We recall that a function $F\colon G\to\mathbb{R}$ is called a *quasicharacter* (another name used in the recent literature is *quasimorphism*) if there exists a constant $C_F\geqslant 0$ such that

$$|F(xy)-F(x)-F(y)|\leqslant C_F \quad \text{for all } x,y\in G.$$

A function $f\colon G\to\mathbb{R}$ is called a *pseudocharacter* (or a *homogeneous quasimorphism*) if f is a quasicharacter and in addition $f(g^n)=nf(g)$ for all $g\in G$ and $n\in\mathbb{Z}$. The notions of a quasicharacter and a pseudocharacter originally arose from the questions of stability of solutions of functional equations [8, 9, 10] and continuous representations of groups [12]. Recently, some surprising applications of quasicharacters and pseudocharacters in symplectic geometry were found [3, 5, 18].

We will use the following notation:

- $X(G)$ is the space of additive characters $G\to\mathbb{R}$;
- $QX(G)$ is the space of quasicharacters;
- $PX(G)$ is the space of pseudocharacters;
- $B(G)$ is the space of bounded functions.

Then

$$H_{b,2}^2(G)\cong QX(G)/(X(G)\oplus B(G))\cong PX(G)/X(G) \tag{1}$$

as vector spaces [6, Proposition 3.2 and Theorem 3.5]. We establish the following criterion for triviality of $H_{b,2}^2$ of wreath products.

Theorem 1.2 $H_{b,2}^2(A\wr B)=0$ *if and only if the following conditions hold:*

(i) $H_{b,2}^2(B)=0$;

(ii) $H_{b,2}^2(A)=0$ *or* B *is infinite.*

2. Preliminaries

Wreath products are defined in the context of permutation groups when a group A acts on a set X and a group B acts on a set Y. We will consider the so-called *standard* wreath products, in which case the groups A and B act on themselves via right regular representations. Moreover, we will work with *restricted* standard wreath products, which are defined as follows. We will use some notations and terminology from [16].

Let $A^{(B)}$ be the direct sum of copies of A indexed by elements of B (for the *complete* wreath product one takes the direct product). We will represent elements of the group $A^{(B)}$ as tuples $\mathbf{a} = (a_b)_{b\in B}$ and will refer to $a_b \in A$ as the *coordinate* of $\mathbf{a}$ at $b \in B$. The set

$$\sigma(\mathbf{a}) = \{b \in B \mid a_b \neq 1\} \subseteq B$$

is the *support* of $\mathbf{a}$; notice that $\sigma(\mathbf{a})$ is finite for every $\mathbf{a} \in A^{(B)}$, and define the *length* of $\mathbf{a}$ by $\ell(\mathbf{a}) = |\sigma(\mathbf{a})|$.

The (standard restricted) wreath product of A and B, denoted by $A \wr B$, is the semidirect product of $A^{(B)}$ and B with the action of B on $A^{(B)}$ given by

$$ {}^{b_0}\mathbf{a} = (c_b)_{b\in B}, \quad \text{where } c_b = a_{bb_0^{-1}}. \tag{2}$$

The group A is called the *bottom* group, the group B is called the *top* group, and the group $A^{(B)}$ is called the *base* group.

An element $\mathbf{a} \in A^{(B)}$ with the property $\sigma(\mathbf{a}) = \{b\}$ will be denoted by $\mathbf{a}_b$, in other words, the only nontrivial coordinate of $\mathbf{a}_b$ is a_b. When it is important to emphasize that a particular element $a_i \in A$ is the coordinate of $\mathbf{a}_b$ at b, we will slightly abuse notation and write $[a_i]_b$ for $\mathbf{a}_b$. In this notation, every element $\mathbf{a}$ of $A^{(B)}$ can be written in the form

$$\mathbf{a} = \mathbf{a}_{b_1}\mathbf{a}_{b_2}\cdots\ \mathbf{a}_{b_s} = [a_{b_1}]_{b_1}[a_{b_2}]_{b_2}\cdots[a_{b_s}]_{b_s},$$

where $b_1, b_2, \ldots, b_s$ are *distinct* elements of B; observe that $s = \ell(\mathbf{a})$. If we identify elements of B with their copies in $A \wr B$, then (2) yields the following relation in the wreath product:

$$b_0\mathbf{a}_b = [a_b]_{bb_0}b_0, \quad \text{where } b_0, b \in B,\ a_b \in A.$$

We will represent elements of the wreath product $A \wr B$ as products $\mathbf{a}b$, where $\mathbf{a} \in A^{(B)}$ is an element of the base group and $b \in B$ is an element of the top group.

We now list some well-known facts about pseudocharacters that will be used in the proof of Theorem 1.2.

Lemma 2.1 *Any pseudocharacter is constant on conjugacy classes; a bounded pseudocharacter is trivial.*

Proof. Let f be a pseudocharacter on a group G and suppose that $f(yxy^{-1}) - f(x) = \alpha \neq 0$ for some $x, y \in G$. Then the difference $f(yx^ny^{-1}) - f(x^n) = n\alpha$ is unbounded when $n \to \infty$. On the other hand,

$$|f(yx^ny^{-1}) - f(x^n)| = |f(yx^ny^{-1}) - f(y) - f(x^n) - f(y^{-1})| \leqslant 2C_f,$$

a contradiction. The second assertion is obvious. □

Lemma 2.2 *If f is a pseudocharacter on a group G and $x_1, \dots, x_n$ are pairwise commuting elements of G, then*

$$f(x_1 \cdots x_n) = f(x_1) + \cdots + f(x_n).$$

Proof. Let $\alpha = f(x_1x_2) - f(x_1) - f(x_2)$. Then for any positive integer n,

$$|n\alpha| = |nf(x_1x_2) - nf(x_1) - nf(x_2)| = |f(x_1^n x_2^n) - f(x_1^n) - f(x_2^n)| \leqslant C_f$$

which implies $\alpha = 0$. The general case follows by induction on n. □

Remark. Of course, the result follows from the general fact that bounded cohomology of amenable groups vanishes, but we chose to give a short elementary proof.

Next, we will need the following standard facts about bounded generation for the proof of Theorem 1.1.

Lemma 2.3 *Let G be a group and H be its subgroup.*

(i) *If H has finite index in G then bounded generation of G is equivalent to that of H.*
(ii) *If G has bounded generation then so does any homomorphic image of G.*
(iii) *If H is a normal subgroup of G and both H and G/H have bounded generation then so does G.*

Proof. The only fact that is not immediate from the definition is that bounded generation of G implies that of its subgroup H of finite index. Suppose that $G = \langle g_1 \rangle \cdots \langle g_n \rangle$. Since every subgroup of finite index contains a normal subgroup of finite index, it suffices to prove our claim assuming in addition that H is normal in G.

An arbitrary element $h \in H$ can be written in the form $h = g_1^{r_1} \cdots g_n^{r_n}$ for some $r_1, \dots, r_n \in \mathbb{Z}$. Say, $[G : H] = m$ and for $i = 1, \dots, n$ write $r_i = e_i + ma_i$ with $0 \leqslant e_i < m$. Since H is normal, we have $h_i := g_i^m \in H$. In this notation,

$$\begin{aligned} h &= g_1^{r_1} \cdots g_n^{r_n} = g_1^{e_1} h_1^{a_1} g_2^{e_2} h_2^{a_2} \cdots g_n^{e_n} h_n^{a_n} \\ &= g_1^{e_1} \cdots g_n^{e_n} \left(\prod_{i=1}^{n-1} [(g_{i+1}^{e_{i+1}} \cdots g_n^{e_n})^{-1} h_i (g_{i+1}^{e_{i+1}} \cdots g_n^{e_n})]^{a_i} \right) h_n^{a_n}. \end{aligned} \tag{3}$$

We now introduce the following finite set

$$\Lambda = \{ g_1^{e_1} \cdots g_n^{e_n} \mid 0 \leqslant e_i < m \}.$$

Then it follows from (3) that

$$H = \left(\prod_{y \in \Lambda \cap H} \langle y \rangle \right) \cdot \prod_{i=1}^{n} \left(\prod_{x \in \Lambda} \langle x^{-1} h_i x \rangle \right),$$

so H has bounded generation. □

Finally, we will need the following result from [17].

Theorem 2.4 *Suppose that a group G is a union of n (left or right) cosets of its subgroups $H_1, \dots, H_k$. Then one of the subgroups H_i must have index at most n in G.*

Corollary 2.5 *Let G be a group and $H_1, \dots, H_k$ be subgroups of infinite index in G. Then for every integer n there exist n elements $a_1, \dots, a_n$ in G such that the set $\{a_1, \dots, a_n\}$ cannot be covered by fewer than n (left or right) cosets of $H_1, \dots, H_k$.*

Proof. We will construct elements $a_1, \dots, a_n$ no two of which are in the same left or right coset of any H_i by induction on n. This is trivial for $n = 1$. Suppose that we have found $a_1, \dots, a_m$ with the above property. Since the subgroups $H_1, \dots, H_k$ have infinite index in G, Theorem 2.4 implies

$$G \neq \bigcup \{a_j H_i,\ H_i a_j \mid j = 1, \dots, m,\ i = 1, \dots, k\}.$$

Now take any element of G outside the right hand side and call it a_{m+1}. □

3. Proof of Theorem 1.1

If B is finite, then the base group $A^{(B)}$ has finite index in the wreath product $A \wr B$ and thus bounded generation of $A \wr B$ is equivalent to that of $A^{(B)}$ (Lemma 2.3). On the other hand, $A^{(B)}$ is a direct sum of finitely many copies of A, hence it has bounded generation if and only if A does. We have reduced the proof of Theorem 1.1 to the proof of the following statement.

Theorem 3.1 *If A is a nontrivial group and B is an infinite group, then the wreath product $A \wr B$ is not boundedly generated.*

Assume on the contrary that $A \wr B$ is boundedly generated: $A \wr B = C_1 \cdots C_k$ where $C_i = \langle \mathbf{a}_i b_i \rangle$ is a cyclic subgroup generated by $\mathbf{a}_i b_i \in A \wr B$. Let $B_i = \langle b_i \rangle$ be the cyclic subgroup of B generated by b_i, $1 \leqslant i \leqslant k$; observe that $B = B_1 \cdots B_k$.

Lemma 3.2 *The group B is virtually cyclic.*

Proof. Assume the contrary; then all subgroups $B_1, \dots, B_k$ have infinite index in B. Let $N = k \sum_{i=1}^{k} \ell(\mathbf{a}_i)$. By Corollary 2.5 there is a finite subset S of B which is not covered by any collection of N cosets of the following finite set of subgroups of B

$$\mathcal{B} = \left\{ x B_i x^{-1} \;\middle|\; x \in \bigcup_{j=1}^{k} \sigma(\mathbf{a}_j),\ i = 1, \dots, k \right\}.$$

Let $\mathbf{d}$ be an element of $A^{(B)}$ whose support contains the set S. We have

$$\mathbf{d} = \prod_{i=1}^{k} (\mathbf{a}_i b_i)^{n_i} \tag{4}$$

for some integers $n_i \in \mathbb{Z}$, $1 \leqslant i \leqslant k$. Write $(\mathbf{a}_i b_i)^{n_i} = \mathbf{e}_i b_i^{n_i}$, where

$$\mathbf{e}_i = \begin{cases} (\mathbf{a}_i) \cdot ({}^{b_i}\mathbf{a}_i) \cdot ({}^{b_i^2}\mathbf{a}_i) \cdots ({}^{b_i^{n_i-1}}\mathbf{a}_i) & \text{if } n_i > 0, \\ ({}^{b_i^{-1}}\mathbf{a}_i^{-1}) \cdot ({}^{b_i^{-2}}\mathbf{a}_i^{-1}) \cdots ({}^{b_i^{n_i}}\mathbf{a}_i^{-1}) & \text{if } n_i < 0. \end{cases}$$

It follows that the support $\sigma(\mathbf{e}_i)$ of $\mathbf{e}_i$ is contained in the union of the left cosets $\{xB_i \mid x \in \sigma(\mathbf{a}_j),\ i,j = 1,\dots,k\}$ of $B_1,\dots,B_k$. On the other hand, (4) gives

$$\mathbf{d} = (\mathbf{e}_1)\cdot({}^{p_1}\mathbf{e}_2)\cdot({}^{p_2}\mathbf{e}_3)\cdots({}^{p_{k-1}}\mathbf{e}_k), \quad \text{where } p_j = b_1^{n_1}\cdots b_j^{n_j},$$

which shows that the support of $\mathbf{d}$ is contained in the union of at most N right cosets $xB_ip_j = (xB_ix^{-1})xp_j$ of the subgroups $xB_ix^{-1} \in \mathcal{B}$. This is a contradiction. Thus one of the subgroups B_i has finite index in B and so B is a virtually cyclic group. □

Lemma 3.3 *It suffices to prove that $A \wr \mathbb{Z}$ is not boundedly generated.*

Proof. Since $\mathbb{Z}$ is a subgroup of finite index of B, the wreath product $A \wr \mathbb{Z}$ is a quotient of a subgroup of finite index of $A \wr B$. Our claim now follows from Lemma 2.3. □

From now on we assume that B is an infinite cyclic group and we will simply index the coordinates of elements $\mathbf{a} \in A^{(B)}$ by integers; the generator z of B then acts on $A^{(B)}$ as the shift $i \mapsto i+1$ of the coordinates. In this new notation we have the assumption that $A \wr B = C_1 \cdots C_k$, where $C_i = \langle \mathbf{a}_i z^{t_i}\rangle$, $t_i \in \mathbb{Z}$, $1 \leqslant i \leqslant k$.

Lemma 3.4 *The group A is finite.*

Proof. We let J be the subset of $\{1,2,\dots,k\}$ consisting of those i for which $t_i \neq 0$, also let I be the complement of J in $\{1,2,\dots,k\}$; observe that $J \neq \varnothing$. If $i \in I$, then the power $(\mathbf{a}_i z^{t_i})^{\alpha_i}$, $\alpha_i \in \mathbb{Z}$, is simply $\mathbf{a}_i^{\alpha_i}$. If $i \in J$, then the power $(\mathbf{a}_i z^{t_i})^{\alpha_i}$ is a product of the following element $\mathbf{a}$ of the base group

$$\mathbf{a} = \begin{cases} (\mathbf{a}_i)\cdot({}^{z^{t_i}}\mathbf{a}_i)\cdot({}^{z^{2t_i}}\mathbf{a}_i)\cdots({}^{z^{(\alpha_i-1)t_i}}\mathbf{a}_i) & \text{if } \alpha_i > 0,\\ ({}^{z^{-t_i}}\mathbf{a}_i^{-1})\cdot({}^{z^{-2t_i}}\mathbf{a}_i^{-1})\cdots({}^{z^{\alpha_i t_i}}\mathbf{a}_i^{-1}) & \text{if } \alpha_i < 0 \end{cases} \tag{5}$$

and the element $z^{\alpha_i t_i}$ of the top group. If $|\alpha_i|$ is large enough then $\mathbf{a}_i$ and ${}^{z^{\alpha_i}}\mathbf{a}_i$ have disjoint support since $\sigma({}^{z^{\alpha_i}}\mathbf{a}_i) = \alpha_i + \sigma(\mathbf{a}_i)$. It follows that each coordinate of the elements in (5) is a product of boundedly many coordinates of $\mathbf{a}_i$. Therefore there is a constant M_i which depends only on $\mathbf{a}_i$ and t_i, but not on α_i, such that the coordinates of the elements in (5) take at most M_i values in A.

Since we assume that $A \wr B = C_1 \cdots C_k$, every element of the base group $A^{(B)}$ is a product of at most k of some B-conjugates of elements as in (5) and at most k of some B-conjugates of elements of the form $\mathbf{a}_i^{\alpha_i}$. Notice that any B-conjugate ${}^{z^{\beta_i}}\mathbf{a}_i^{\alpha_i}$ has support of size $\ell(\mathbf{a}_i)$, so the total support of B-conjugates of such elements corresponding to $i \in I$ has size at most $\sum_{i=1}^{k} \ell(\mathbf{a}_i)$. If we take an element $\mathbf{a}$ of $A^{(B)}$ of length $\ell(\mathbf{a}) > \sum_{i=1}^{k} \ell(\mathbf{a}_i)$, then at least one of its coordinates has to be a product of coordinates of elements of the form (5) corresponding to $i \in J$. But such product can take at most $\prod_{i\in J} M_i$ values in A. It follows that A cannot have more than $\prod_{i\in J} M_i$ elements. □

Remark. One can also conclude that A must be finite in the original set-up, without the assumption that B is infinite cyclic. If we similarly partition the set

$\{1, 2, \ldots, k\}$ into two subsets I (consisting of those i for which b_i has finite order) and J (consisting of those i for which b_i has infinite order), then the support of all B-conjugates of elements corresponding to I is bounded, while coordinates of B-conjugates of elements corresponding to J take a bounded number of values in A.

We have now reduced Theorem 3.1 to the following case: A is finite and B is infinite cyclic. Define the *width* of $\mathbf{a} \in A^{(B)}$, denoted $w(\mathbf{a})$, as the difference between the largest and the smallest element of the support of $\mathbf{a}$ and let $L = \max\{w(\mathbf{a}_1), \ldots, w(\mathbf{a}_k)\}$. For a large positive integer M let $\pi\colon A^{(B)} \to A^M$ be the projection onto the coordinates $1, 2, \ldots, M$:

$$\pi\left((a_i)_{i\in\mathbb{Z}}\right) = (a_1, \ldots, a_M).$$

Take an arbitrary element $\mathbf{a}z^t \in A \wr B$ with $w(\mathbf{a}) \leqslant L$ and $t \neq 0$. For an integer β_1, a positive integer β_2, and $\epsilon \in \{\pm 1\}$, consider the element

$$\mathbf{g}_{\beta_1,\beta_2,\epsilon} = ({}^{z^{\beta_1}}\mathbf{a}) \cdot ({}^{z^{\beta_1+\epsilon t}}\mathbf{a}) \cdot ({}^{z^{\beta_1+2\epsilon t}}\mathbf{a}) \cdots ({}^{z^{\beta_1+\beta_2\epsilon t}}\mathbf{a}).$$

Let $u_i \in \mathbb{Z}$ be the position of the first nontrivial coordinate of the element ${}^{z^{\beta_1+\epsilon i t}}\mathbf{a}$, $0 \leqslant i \leqslant \beta_2$. More explicitly, assuming $\epsilon = 1$, $u_i = u_0 + it$ and

$$\sigma\left({}^{z^{\beta_1+\epsilon i t}}\mathbf{a}\right) \subseteq \{u_0 + it, u_0 + 1 + it, \ldots, u_0 + L + it\}.$$

The number of possible projections of $\mathbf{g}_{\beta_1,\beta_2,\epsilon}$ as β_1, β_2, ϵ vary depends only on $\mathbf{a}$, t, and the coordinates whose positions are between 1 and M. More precisely, since u_i determines the element ${}^{z^{\beta_1+\epsilon i t}}\mathbf{a}$, once $\mathbf{a}$ and $t \neq 0$ are fixed, the projection $\pi\left(\mathbf{g}_{\beta_1,\beta_2,\epsilon}\right)$ is completely determined by the smallest and the largest of the positions $u_0, u_1, \ldots, u_{\beta_2}$ which lie in the interval $[-(L-1), M]$. We conclude that there are at most $(M+L)^2$ possibilities for the projection $\pi\left(\mathbf{g}_{\beta_1,\beta_2,\epsilon}\right)$ as β_1 ranges over $\mathbb{Z}$, β_2 ranges over $\mathbb{N}$, and ϵ is fixed as either 1 or -1.

As observed earlier, every element of $A^{(B)}$ is a product of at most k of some B-conjugates of elements of the following three types:

$$(6)\quad (\mathbf{a}_i) \cdot ({}^{z^{t_i}}\mathbf{a}_i) \cdots ({}^{z^{(\alpha_i-1)t_i}}\mathbf{a}_i), \qquad ({}^{z^{-t_i}}\mathbf{a}_i^{-1}) \cdot ({}^{z^{-2t_i}}\mathbf{a}_i^{-1}) \cdots ({}^{z^{\alpha_i t_i}}\mathbf{a}_i^{-1}), \qquad \mathbf{a}_i^{\alpha_i}.$$

We have just established that there are at most $(M+L)^2$ possibilities for the projections onto A^M for each of the elements of the first two types in (6). On the other hand, the B-conjugates of the elements of the third type have only $\ell(\mathbf{a}_i)$ nontrivial coordinates, which are a shift of the nontrivial coordinates of $\mathbf{a}_i$. To count the number of possible projections of such elements, we notice that by varying the coordinates we obtain at most $|A|^{\ell(\mathbf{a}_i)}$ combinations, and by shifting the position of the first nontrivial coordinate (which can take any value between $-(L-1)$ and M) we obtain at most $(M+L)$ possibilities for each combination of coordinates. It follows that the projections of the elements of the third type from (6) can take at most $(M+L)|A|^{\ell(\mathbf{a}_i)}$ values in A^M.

Putting all of this together, we see that the product of k B-conjugates of elements as in (6) can have at most

$$\left((M+L)^2\right)^k \cdot \left((M+L)|A|^D\right)^k$$

values in its projection under π, where $D = \max\{\ell(\mathbf{a}_1), \dots, \ell(\mathbf{a}_k)\}$. This number grows polynomially in M when L, D, k, and $|A|$ are fixed. On the other hand, $|A|^M$ grows exponentially with M since $|A| > 1$. So for large enough M we will not be able to achieve all the choices for the coordinates $1, 2, \dots, M$ with a product of k cyclic subgroups C_i. This contradiction completes the proof of Theorem 3.1.

Remark. The proof of Theorem 3.1 can be adapted to other types of permutation actions including that of $SL_n(\mathbb{O}_S)$ on $\mathbb{O}_S^n$ for the ring $\mathbb{O}_S$ of S-integers in a number field.

4. Proof of Theorem 1.2

Suppose that $H^2_{b,2}(A \wr B) = 0$. We begin by showing that (i) must hold.

Lemma 4.1 $\dim H^2_{b,2}(A \wr B) \geqslant \dim H^2_{b,2}(B)$.

Proof. Let $f_1, \dots, f_n$ be pseudocharacters of B linearly independent modulo characters. For each $i = 1, \dots, n$ define a function F_i on $A \wr B$ by

$$F_i(\mathbf{a}b) = f_i(b),$$

where $\mathbf{a} \in A^{(B)}$ and $b \in B$. Then

$$F_i((\mathbf{a}b)^n) = F_i\left((\mathbf{a}) \cdot ({}^{b}\mathbf{a}) \cdots ({}^{b^{n-1}}\mathbf{a}) \cdot b^n\right) = f_i(b^n) = nf_i(b) = nF_i(\mathbf{a}b)$$

and

$$|F_i\left((\mathbf{a}_1 b_1)(\mathbf{a}_2 b_2)\right) - F_i(\mathbf{a}_1 b_1) - F_i(\mathbf{a}_2 b_2)| = |f_i(b_1 b_2) - f_i(b_1) - f_i(b_2)| \leqslant C_{f_i}.$$

Therefore, $F_1, \dots, F_n$ are pseudocharacters on $A \wr B$ which are linearly independent modulo characters of $A \wr B$, whence our claim. □

Condition (ii) must hold in view of the following.

Lemma 4.2 *If B is finite, then* $\dim H^2_{b,2}(A \wr B) \geqslant \dim H^2_{b,2}(A)$.

Proof. Given pseudocharacters $f_1, \dots, f_n$ on A linearly independent modulo characters, define functions F_i, $1 \leqslant i \leqslant n$, on $A \wr B$ as follows:

$$F_i\left([a_1]_{b_1} \cdots [a_s]_{b_s} b\right) = f_i(a_1) + \dots + f_i(a_s).$$

Suppose that $|B| = m$ and let $a_1, \dots, a_s$, $c_1, \dots, c_t$ be arbitrary elements of A, $b_1, \dots, b_s$ be distinct elements of B, $d_1, \dots, d_t$ be distinct elements of B, and u, v be arbitrary elements of B. Then

$$\begin{aligned} &|F_i\left(([a_1]_{b_1} \cdots [a_s]_{b_s} u)([c_1]_{d_1} \cdots [c_t]_{d_t} v)\right) - F_i\left([a_1]_{b_1} \cdots [a_s]_{b_s} u\right) \\ &\qquad\qquad - F_i\left([c_1]_{d_1} \cdots [c_t]_{d_t} v\right)| \\ &= |F_i\left([a_1]_{b_1} \cdots [a_s]_{b_s} [c_1]_{d_1 u} \cdots [c_t]_{d_t u} uv\right) - F_i\left([a_1]_{b_1} \cdots [a_s]_{b_s} u\right) \\ &\qquad\qquad - F_i\left([c_1]_{d_1} \cdots [c_t]_{d_t} v\right)| \\ &= \left| \sum_{b_k = d_j u} \left(f_i(a_k c_j) - f_i(a_k) - f_i(c_j)\right) \right| \leqslant m C_{f_i}, \end{aligned}$$

which shows that F_i is an unbounded quasicharacter of $A \wr B$ with constant mC_{f_i}. It follows from (1) that there is a bounded function G_i on $A \wr B$ such that $F_i + G_i$ is a pseudocharacter of $A \wr B$. Note that the restriction of $F_i + G_i$ to the coordinate at position 1 of $A^{(B)}$ is a pseudocharacter of A which differs from f_i by a bounded function, hence coincides with f_i by Lemma 2.1. Thus the pseudocharacters $F_1 + G_1, \ldots, F_n + G_n$ are linearly independent modulo characters of $A \wr B$. □

Now it remains to show that (i) and (ii) imply $H^2_{b,2}(A \wr B) = 0$. We begin with a couple of observations.

Lemma 4.3 *If $F \in PX(A \wr B)$, then $F([a]_{b_1}) = F([a]_{b_2})$ for all b_1, $b_2 \in B$ and all $a \in A$.*

Proof. Every pseudocharacter is constant on conjugacy classes (Lemma 2.1) and $[a]_{b_2} = (b_1^{-1}b_2)[a]_{b_1}(b_1^{-1}b_2)^{-1}$. □

Lemma 4.4 *If $H^2_{b,2}(A) = 0$, then $H^2_{b,2}(A^{(B)}) = 0$.*

Proof. Let $F \in PX(A^{(B)})$ and take an arbitrary element $\mathbf{a} \in A^{(B)}$. If $\sigma(\mathbf{a}) = \{b_1, \ldots, b_s\}$, then $\mathbf{a} = \mathbf{a}_{b_1} \cdots \mathbf{a}_{b_s}$ and by Lemma 2.2,

$$F(\mathbf{a}_{b_1} \cdots \mathbf{a}_{b_s}) = F(\mathbf{a}_{b_1}) + \cdots + F(\mathbf{a}_{b_s}).$$

Since $H^2_{b,2}(A) = 0$, the restriction of F to every coordinate of $A^{(B)}$ is a character of A, whence F is a character of $A^{(B)}$. □

We now continue with the proof of the theorem.

Lemma 4.5 *If $H^2_{b,2}(A) = 0$ and $H^2_{b,2}(B) = 0$, then $H^2_{b,2}(A \wr B) = 0$.*

Proof. If $F \in PX(A \wr B)$, then by Lemma 4.4, the restriction $F|_{A^{(B)}}$ is a character of $A^{(B)}$; also $F|_B$ is a character of B. To prove that F is a character of the wreath product $A \wr B$, it thus remains to show that

$$F(\mathbf{a}b) = F(\mathbf{a}) + F(b) \quad \text{for all } \mathbf{a} \in A^{(B)},\ b \in B.$$

Let $\alpha = F(\mathbf{a}b) - F(\mathbf{a}) - F(b)$. Then for any positive integer n, we have

$$\begin{aligned} |n\alpha| &= |nF(\mathbf{a}b) - nF(\mathbf{a}) - nF(b)| \\ &= \left| F\left((\mathbf{a}) \cdot ({}^{b}\mathbf{a}) \cdots ({}^{b^{n-1}}\mathbf{a}) \cdot b^n \right) - nF(\mathbf{a}) - F(b^n) \right| \\ &\leqslant \left| F\left((\mathbf{a}) \cdot ({}^{b}\mathbf{a}) \cdots ({}^{b^{n-1}}\mathbf{a}) \cdot b^n \right) - F\left((\mathbf{a}) \cdot ({}^{b}\mathbf{a}) \cdots ({}^{b^{n-1}}\mathbf{a}) \right) - F(b^n) \right| \\ &\qquad + \left| F\left((\mathbf{a}) \cdot ({}^{b}\mathbf{a}) \cdots ({}^{b^{n-1}}\mathbf{a}) \right) - nF(\mathbf{a}) \right| \\ &\leqslant C_F + \left| F(\mathbf{a}) + F\left({}^{b}\mathbf{a}\right) + \cdots + F\left({}^{b^{n-1}}\mathbf{a}\right) - nF(\mathbf{a}) \right| \\ &= C_F \end{aligned}$$

which shows that $\alpha = 0$. □

Remark. One can also derive the result of Lemma 4.5 from the observation that if N and K are subgroups of G with N normal such that $G = NK$ and $H^2_{b,2}(N) = H^2_{b,2}(K) = 0$, then $H^2_{b,2}(G) = 0$. The proof is identical to that of the lemma.

The next lemma completes the proof of Theorem 1.2.

Lemma 4.6 *If $H^2_{b,2}(B) = 0$ and B is infinite, then $H^2_{b,2}(A \wr B) = 0$.*

Proof. Let $F \in PX(A \wr B)$. Proof of Lemma 4.5 shows that in order to establish that F is a character of $A \wr B$, it suffices to show that F is a character of $A^{(B)}$. Lemma 4.3 implies there exists a pseudocharacter f of A such that the restriction of F to every coordinate in $A^{(B)}$ is f, i.e.,

$$F([a]_b) = f(a) \quad \text{for all } a \in A,\ b \in B.$$

If $b_1, \dots, b_s$ are distinct element of B, then Lemma 2.2 implies

$$F([a_1]_{b_1} \cdots [a_s]_{b_s}) = f(a_1) + \cdots + f(a_s)$$

for arbitrary elements $a_1, \dots, a_s \in A$. Therefore, to prove that F is a character of $A^{(B)}$, it suffices to show that f is a character of A. Suppose that f is not a character of A; then there exist $a_1,\ a_2 \in A$ such that

$$\alpha = f(a_1a_2) - f(a_1) - f(a_2) \neq 0.$$

Choose an infinite sequence $\{b_i\}$ of distinct elements of B. Then

$$\begin{aligned} &|F\left(([a_1]_{b_1} \cdots [a_1]_{b_n})([a_2]_{b_1} \cdots [a_2]_{b_n})\right) - F\left([a_1]_{b_1} \cdots [a_1]_{b_n}\right) - F\left([a_2]_{b_1} \cdots [a_2]_{b_n}\right)| \\ &\quad = |F\left([a_1a_2]_{b_1} \cdots [a_1a_2]_{b_n}\right) - F\left([a_1]_{b_1} \cdots [a_1]_{b_n}\right) - F\left([a_2]_{b_1} \cdots [a_2]_{b_n}\right)| \\ &\quad = |nf(a_1a_2) - nf(a_1) - nf(a_2)| = |n\alpha| \to \infty \quad \text{as } n \to \infty \end{aligned}$$

On the other hand, it is bounded by C_F, a contradiction. □

`Acknowledgement.` This work was begun during the third author's visit to the University of North Carolina at Greensboro and was completed after his visit to the Imperial College London. He would like to thank both these institutions for their excellent hospitality.

References

[1] M. Abért, A. Lubotzky, L. Pyber, Bounded generation and linear groups, *Inernat. J. Algebra Comput.* **13** (2003), no. 4, 401–413.

[2] Ch. Bavard, Longueur stable des commutateurs, *Enseign. Math.* **37** (1991), no. 1–2, 109–150.

[3] P. Biran, M. Entov, L. Polterovich, Calabi quasimorphisms for the symplectic ball, *Commun. Contemp. Math.* **6** (2004), no. 5, 793–802.

[4] J.D. Dixon, M.P.F du Sautoy, A. Mann, Analytic pro-p Groups, London Math. Soc. Lecture Note Series, **157**, Cambridge Univ. Press, Cambridge, 1991.

[5] M. Entov and L. Polterovich, Calabi quasimorphism and quantum homology, *Int. Math. Res. Not.* (2003), no. 30, 1635–1676.

[6] R.I. Grigorchuk, Some results on bounded cohomology, *London Math. Soc. Lecture Note Ser.* **204** (1995), 111–163.

[7] M. Gromov, Volume and bounded cohomology, *Inst. Hautes Études Sci. Publ. Math.* **56** (1982), 5–99.

[8] D.H. Hyers, On the stability of the linear functional equation, *Proc. Nat. Acad. Sci. USA* **27** (1941), 222–224.

[9] D.H. Hyers and S.M. Ulam, On approximate isometries, *Bull. Amer. Math. Soc.* **51** (1945), 288–292.

[10] D.H. Hyers and S.M. Ulam, Approximate isometries of the space of continuous functions, *Ann. of Math.* **48** (1947), 285–289.

[11] M. Kassabov, Kazhdan constants for $\mathrm{SL}_n(\mathbb{Z})$, *Internat. J. Algebra Comput.* **15** (2005), no. 5–6, 971–995.

[12] D. Kazhdan, On ε-representations, *Israel J. Math.* **43** (1982), no. 4, 315–323.

[13] M. Lazard, Groupes analytiques p-adiques, *Inst. Hautes Études Sci. Publ. Math.* **26** (1965), 389–603.

[14] A. Lubotzky, Dimension function for discrete groups, *London Math. Soc. Lecture Note Ser.* **121** (1986), 254–262.

[15] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995), no. 2, 267–295.

[16] J.D.P. Meldrum, Wreath Products of Groups and Semigroups, Pitman Monographs and Surveys in Pure and Applied Mathematics, 74. Longman, Harlow, 1995.

[17] B.H. Neumann, Groups covered by permutable subsets, *J. London Math. Soc.* **29** (1954), 236–248.

[18] Y. Ostrover, Calabi quasi-morphisms for some non-monotone symplectic manifolds, *Algebr. Geom. Topol.* **6** (2006), 405–434.

[19] V.P. Platonov and A.S. Rapinchuk, Abstract properties of S-arithmetic groups and the congruence problem, *Russian Acad. Sci. Izv. Math.* **40** (1993), no. 3, 455–476.

[20] A.S. Rapinchuk, Representations of groups of finite width, *Dokl. Akad. Nauk SSSR* **315** (1990), 536–540.

[21] A.S. Rapinchuk, On SS-rigid groups and A. Weil's criterion for local rigidity, *Manuscripta Math.* **97** (1998), no. 4, 529–543.

[22] Y. Shalom, Bounded generation and Kazhdan's property (T), *Inst. Hautes Études Sci. Publ. Math.* **90** (1999), 145–168.

Department of Mathematics and Statistics, University of North Carolina at Greensboro, Greensboro NC 27402, USA

E-mail address: `igor@uncg.edu`

Department of Mathematics, Imperial College, London, SW7 2AZ, UK

E-mail address: `n.nikolov@imperial.ac.uk`

Stat–Math Unit, Indian Statistical Institute, 8th Mile Mysore Rd, Bangalore 560 059, India

E-mail address: `sury@isibang.ac.in`