Invariable generation of iterated wreath products of cyclic groups

Publisher:
Springer Verlag

Published version:
DOI: 10.1007/s13366-016-0326-2

INVARIABLE GENERATION OF ITERATED WREATH PRODUCTS OF CYCLIC GROUPS

ANDREA LUCCHINI

ABSTRACT. Given a sequence $\{C_i\}_{i\in\mathbb{N}}$ of cyclic groups of prime orders, let Γ_∞ be the inverse limit of the iterated wreath products $C_m \wr \cdots \wr C_2 \wr C_1$. We prove that the profinite group Γ_∞ is not topologically finitely invariably generated.

1. Introduction

Let $\{G_i\}_{i\in\mathbb{N}}$ be a sequence of finite groups and let $X_m = G_m \wr \cdots \wr G_2 \wr G_1$ be the iterated wreath product of the first m groups, where at each step the permutation action which is considered is the regular one. The infinitely iterated wreath product is the inverse limit

$$X_\infty = \varprojlim_m X_m = \varprojlim_m (G_m \wr \cdots \wr G_2 \wr G_1).$$

We consider the particular case when the groups G_i are all cyclic of prime order. Let $\{C_i\}_{i\in\mathbb{N}}$ be a sequence of finite cyclic groups and assume that $|C_i| = p_i$ is a prime for every i and let $\Gamma_\infty = \varprojlim_m C_m$. As it follows from the results presented in [1], [2] or [8], the profinite group Γ_∞ is (topologically) finitely generated if and only if there exists a positive integer d with the property that, for every prime p, the set $\Omega_p = \{n \in \mathbb{N} \mid p_n = p\}$ has size at most d. In particular it follows from [8, Corollary 2.4] that Γ_∞ is 2-generated if the primes p_n are all distinct.

We prove that the situation is completely different if we consider the "invariable generation". Following [5] we say that a subset S of a group G invariably generates G if $G = \langle s^{g(s)} \mid s \in S\rangle$ for each choice of $g(s) \in G$, $s \in S$. The notion of invariable generation occurs naturally for Galois groups, where elements are only given up to conjugacy. We also say that a group G is invariably generated if G is invariably generated by some subset S of G. A group G is invariably generated if and only if it cannot be covered by a union of conjugates of a proper subgroup, which amount to saying that in every transitive permutation representation of G on a set with more than one element there is a fixed-point-free element. Using this characterization, Wiegold [10] proved that the free group on two (or more) letters is not invariably generated. Kantor, Lubotzky and Shalev studied invariable generation in finite and infinite groups. For example in [6] they proved that every finite group G is invariably generated by at most $\log_2 |G|$ elements. In [7] they studied invariable generation of infinite groups, with emphasis on linear groups, proving that a finitely generated linear group is finitely invariably generated if and only if it is virtually soluble. When G is a profinite group, generation and invariable generation in G are interpreted topologically. Our main result is the following:

Partially supported by Università di Padova (Progetto di Ricerca di Ateneo: "Invariable generation of groups").

Theorem 1. *The profinite group Γ_∞ is not finitely invariably generated.*

In particular, if the primes p_i are pairwise distinct, Γ_∞ is 2-generated but not finitely invariably generated. The question whether a finitely generated prosoluble group is also finitely invariable generated was asked by Kantor, Lubotzky and Shalev in [7] and received a negative answer in [4]. Theorem 1 improves the results in [4], giving a concrete example of a 2-generated prosoluble group that is not finitely invariably generated.

2. Proof of Theorem 1

In all this section we will use the notation $G = \langle g_1, \dots, g_d \rangle_I$ to indicate that G is invariably generated by the elements $g_1, \dots, g_d$.

Lemma 2. *Let H be a group acting irreducibly and faithfully on an elementary abelian p-group V and for a positive integer u, consider the semidirect product $G = V^u \rtimes H$, where the action of H is diagonal on V^u, that is, H acts in the same way on each of the u direct factors. Suppose that $h_1, \dots, h_d$ invariably generate H and that $\mathrm{H}^1(H, V) = 0$ and let t be a positive integer with $t \le d$. There exist some elements $w_1, \dots, w_t \in V^u$ such that $h_1w_1, h_2w_2, \dots, h_tw_t, h_{t+1}, \dots, h_d$ invariably generate $V^u \rtimes H$ if and only if*

$$u \le \sum_{1 \le i \le t} \dim_{\mathrm{End}_H(V)} C_V(h_i).$$

Proof. Set $w_{t+1} = \cdots = w_d = (0, \dots, 0)$ and for every $i \in \{1, \dots, d\}$ assume $w_i = (w_{i,1}, \dots, w_{i,u})$. For $j \in \{1, \dots, u\}$, consider the vectors

$$r_j = (w_{1,j}, \dots, w_{d,j}) \in V^d.$$

By [3, Proposition 8], the elements $h_1w_1, h_2w_2, \dots, h_dw_d$ invariably generate $V^u \rtimes H$ if and only if the vectors $r_1, \dots, r_u$ are linearly independent modulo

$$W = \{(u_1, \dots, u_d) \in V^d \mid u_i \in [h_i, V],\ i = 1, \dots, d\}.$$

Now for every $j \in \{1, \dots, u\}$, let

$$\tilde{r}_j = (w_{1,j}, \dots, w_{t,j}) \in V^t$$

and let

$$\tilde{W} = \{(u_1, \dots, u_t) \in V^d \mid u_i \in [h_i, V],\ i = 1, \dots, t\}.$$

Since $w_{t+1} = \cdots = w_d = (0, \dots, 0)$, the vectors $r_1, \dots, r_u$ are linearly independent modulo W if and only if the vectors $\tilde{r}_1, \dots, \tilde{r}_u$ are linearly independent modulo $\tilde{W}$. In particular, there exist some elements $w_1, \dots, w_t \in V^t$ such that $h_1w_1, , \dots, h_tw_t, h_{t+1}, \dots, h_d$ invariably generate $V^u \rtimes H$ if and only if

$$u \le t \cdot \dim_{\mathrm{End}_H(V)} V - \dim \tilde{W} = \sum_i \dim_{\mathrm{End}_H(V)} C_V(h_i). \quad \square$$

Lemma 3. *Suppose that $G = N \rtimes H$ with N and H finite groups of coprime orders. Assume that $G = \langle g_1, \dots, g_d \rangle_I$. Let $g_1 = n_1h_1$ with $n_1 \in N$ and $h_1 \in H$. If $(|g_1|, |N|) = 1$, then $G = \langle h_1, g_2, \dots, g_d \rangle_I$.*

Proof. Let π be the set of the prime divisors of $|h_1|$. If $(|g_1|, |N|) = 1$, then g_1 belongs to a Hall π-subgroup of $N\langle h_1 \rangle$. Hence $g_1^n \in H$ for some $n \in N$ and consequently g_1 and h_1 are conjugated in G. But then $G = \langle g_1, g_2, \dots, g_d \rangle_I$ if and only if $G = \langle h_1, g_2, \dots, g_d \rangle_I$. $\square$

Lemma 4. *Let H be a finite soluble group, q be a prime not dividing $|H|$ and consider the wreath product $G = C_q \wr H$ with respect to the regular permutation representation of H. Assume that $H = \langle h_1, \dots, h_d \rangle_I$ and that there exist $r \leq d$ and $w_1, \dots, w_d$ in the base $W \cong C_q^{|H|}$ of this wreath product such that*

(1) $G = \langle h_1 w_1, \dots, h_d w_d \rangle_I$;

(2) q does not divide the order of $w_i h_i$ for every $i \in \{r+1, \dots, d\}$.

Then

$$1 \leq \sum_{1 \leq i \leq r} \frac{1}{|h_i|}.$$

Proof. Let F be the field of order q and consider the additive group W of the group algebra FH. Notice that G is isomorphic to the semidirect product $W \rtimes H$, where H acts on W by right multiplication. By Maschke's theorem,

$$W = V_1^{m_1} \oplus \cdots \oplus V_s^{m_s}$$

where the V_j are irreducible FH-modules no two of which are H-isomorphic. Let

$$F_i = \mathrm{End}_{FH} V_i, \quad r_i = |F_i : F|, \quad n_i = \dim_F V_i.$$

It follows from the Weddeburn Theorem that

$$W = FH \cong \mathrm{M}_{m_1}(F_1) \oplus \cdots \oplus \mathrm{M}_{m_s}(F_s),$$

where $\mathrm{M}_{m_i}(F_i)$ is the ring of the $m_i \times m_i$ matrices over F_i and that V_i is FH-isomorphic to a minimal ideal of $\mathrm{M}_{m_i}(F_i)$. In particular we have

$$m_i = \dim_{F_i} V_i = \frac{n_i}{r_i}$$

and consequently

$$|H| = \dim_F V = \sum_{1 \leq i \leq s} r_i \cdot m_i^2.$$

By Lemma 3, condition (2) implies that we may assume $w_{r+1} = \cdots = w_d = 0$. By [9, Lemma 1] we have $\mathrm{H}^1(H, V_j) = 0$, so we may apply Lemma 2 to the homomorphic image $V_j^{m_j} \rtimes H$. It follows that, for any j, we have

$$m_j \leq \sum_{1 \leq i \leq r} \dim_{F_j} C_{V_j}(h_i).$$

Multiplying by $r_j \cdot m_j$ we get

$$r_j \cdot m_j^2 \leq \sum_{i \leq i \leq r} r_j \cdot m_j \cdot \dim_{F_j} C_{V_j}(h_i) = \sum_{1 \leq i \leq r} m_j \cdot \dim_F C_{V_j}(h_i).$$

It follows that:

$$|H| = \sum_{1 \leq i \leq r} r_j \cdot m_j^2 \leq \sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} m_j \cdot \dim_F C_{V_j}(h_i) = \sum_{1 \leq i \leq r} \dim_F C_W(h_i).$$

On the other hand, by [4, Lemma 9],

$$\dim_F C_W(h_i) = \frac{|H|}{|h_i|}$$

and therefore

$$1 \leq \sum_{i=1}^{r} \frac{1}{|h_i|}.$$

□

Proof of Theorem 1. We may assume that for every prime p there are only finitely many indices n with $p_n = |C_n| = p$ (otherwise Γ_∞ is not finitely generated). This means in particular that the profinite order of Γ_∞ is divisible by infinitely many primes. Assume now by contradiction that there exist $g_1, \dots, g_d \in \Gamma_\infty$ with $\Gamma_\infty = \langle g_1, \dots, g_d \rangle_I$. From now on we will denote by Γ_m the iterated wreath product $C_m \wr \cdots \wr C_1$ and by $\pi_m : \Gamma_\infty \to \Gamma_m$ the natural projection from Γ_∞ to Γ_m. First we prove the following claim:
$(*)$ there exists $\mu \in \mathbb{N}$, such that $|\pi_\mu(g_i)| > d$ for every $i \in \{1, \dots, d\}$.
Indeed, suppose that $(*)$ is false. Up to reordering the indices, we may assume that there exists $r < d$ such that $|g_i| > d$ if and only if $i \le r$. In particular there exists m_1 such that

$$|\pi_n(g_i)| > d \text{ for every } n \ge m_1 \text{ and every } i \in \{1, \dots, r\}.$$

Using the fact that $|\Gamma_\infty|$ is divisible by infinitely many distinct primes, we are ensured that there exists a positive integer $m \ge m_1$ such that

$$p_{m+1} > d \quad \text{and} \quad p_n \ne p_{m+1} \text{ for every } n \le m.$$

For every i, let

$$x_i = \pi_{m+1}(g_i) \in \Gamma_{m+1} = C_{p_{m+1}} \wr \Gamma_m, \quad y_i = \pi_m(g_i) \in \Gamma_m.$$

We may write x_i in the form $x_i = y_i w_i$ where w_i is an element of the base $C_{p_{m+1}}^{|\Gamma_m|}$ of the wreath product $C_{p_{m+1}} \wr \Gamma_m$. If $i > r$, then $|g_i| < d$ and consequently p_{m+1} does not divide $|x_i|$. Since $\langle x_1, \dots, x_d \rangle_I = \Gamma_{m+1}$, we deduce from Lemma 4, that

$$1 \le \sum_{i=1}^{r} \frac{1}{|y_i|} < \frac{r}{d} \le \frac{d-1}{d},$$

a contradiction. Having proved $(*)$, we take now a positive integer k such that

$$k > \mu \quad \text{and} \quad p_n \ne p_{k+1} \text{ for every } n \le k.$$

We apply Lemma 4 to the wreath product $\Gamma_{k+1} = C_{p_{k+1}} \wr \Gamma_k$. Since $\Gamma_{k+1} = \langle \pi_{k+1}(g_1), \dots, \pi_{k+1}(g_d) \rangle_I$ we must have

$$1 \le \sum_{i=1}^{d} \frac{1}{|\pi_{k+1}(g_i)|} \le \sum_{i=1}^{d} \frac{1}{|\pi_\mu(g_i)|} < 1,$$

a contradiction. □

References

1. I. Bondarenko, Finite generation of iterated wreath products, Arch. Math. (Basel) 95 (2010), no. 4, 301-308.
2. E. Detomi and A. Lucchini, Characterization of finitely generated infinitely iterated wreath products, Forum Math. 25 (2013), no. 4, 867-886.
3. E. Detomi and A. Lucchini, Invariable generation with elements of coprime prime-power orders, J. Algebra 423 (2015), 683–701.
4. E. Detomi and A. Lucchini, Invariable generation of prosoluble groups, Israel J. Math. 211 (2016), no. 1, 481-491.
5. J. D. Dixon, Random sets which invariably generate the symmetric group, Discrete Math. 105 (1992) 25-39.
6. W. M. Kantor, A. Lubotzky and A. Shalev, Invariable generation and the Chebotarev invariant of a finite group, J. Algebra 348 (2011), 302–314.
7. W. M. Kantor, A. Lubotzky and A. Shalev, Invariable generation of infinite group, J. Algebra 421 (2015), 296310.

8. A. Lucchini, Generating wreath products, Arch. Math. (Basel) 62 (1994), no. 6, 481–490.
9. U. Stammbach, Cohomological characterisations of finite solvable and nilpotent groups, J. Pure Appl. Algebra 11 (1977/78), no. 1–3, 293–301.
10. J. Wiegold, Transitive groups with fixed-point-free permutations, Arch. Math. (Basel) 27 (1976), 473–475.

Andrea Lucchini, Università degli Studi di Padova, Dipartimento di Matematica "Tullio Levi-Civita", Via Trieste 63, 35121 Padova, Italy, email: lucchini@math.unipd.it