POSITIVE LAWS ON LARGE SETS OF GENERATORS: COUNTEREXAMPLES FOR INFINITELY GENERATED GROUPS

CRISTINA ACCIARRI and GUSTAVO A. FERNÁNDEZ-ALCOBER $^{\boxtimes}$

Communicated by E. A. O'Brien

Abstract

Shumyatsky and the second author proved that if G is a finitely generated residually finite p-group satisfying a law, then, for almost all primes p, the fact that a normal and commutator-closed set of generators satisfies a positive law implies that the whole of G also satisfies a (possibly different) positive law. In this paper, we construct a counterexample showing that the hypothesis of finite generation of the group G cannot be dispensed with.

2010 *Mathematics subject classification*: primary 20E99.

Keywords and phrases: positive laws, residually finite p-groups.

1. Introduction

A group word is called *positive* if it does not involve any inverses of the variables. If α and β are two different positive words, a subset T of a group G is said to satisfy the *positive law* $\alpha \equiv \beta$ if every substitution of elements of T for the variables gives the same value for α and for β. The *degree* of the law is the maximum of the lengths of the words α and β. A prominent positive law is the *Mal'cev law* $M_c(x, y)$ given by the relation $\alpha_c(x, y) \equiv \beta_c(x, y)$, where α_c and β_c are defined by $\alpha_0 = x$, $\beta_0 = y$, and the recursive relations

$$\alpha_c = \alpha_{c-1}\beta_{c-1} \quad \text{and} \quad \beta_c = \beta_{c-1}\alpha_{c-1}.$$

Thus $M_1(x, y)$ is the abelian law $xy \equiv yx$, and $M_2(x, y)$ is the law $xyyx \equiv yxxy$. Throughout this paper, when we speak about a Mal'cev law $M_c(x, y)$, we always assume that $c \geq 1$.

289

Every nilpotent group of class c satisfies the law $M_c(x, y)$, and an extension of a nilpotent group of class c by a group of finite exponent e satisfies the positive law $M_c(x^e, y^e)$. Mal'cev asked whether, conversely, a group that satisfies a positive law is nilpotent-by-(finite exponent). This question was answered in the negative by Olshanskii and Storozhev in [7]. However, the answer is positive for a large class of groups: Burns and Medvedev proved in [2] that *a locally graded group satisfying a positive law is nilpotent-by-(locally finite of finite exponent)*. (See also the paper [1] by Bajorska and Macedońska.)

An interesting question regarding positive laws is the following: under what conditions does a positive law on a set T of generators of a group G imply a (possibly different) positive law on the whole of G? This problem is inspired by the following particular but important case: is it true that a positive law on the set of all values of a word w in a group G implies a positive law on the verbal subgroup $w(G)$? One of the conditions that must be certainly fulfilled in the first question is that the set T of generators has to be large in some sense. For example, a free product $G = P * Q$ of two finite p-groups is generated by the set $T = P \cup Q$ that satisfies a positive law of the form $x^q \equiv 1$, where q is a power of p, but G does not satisfy a positive law unless $|P|, |Q| \le 2$. On the other hand, the set of values of a word is to some extent large; note that it is a normal subset and, on occasions, also commutator-closed (that is, closed under taking commutators of its elements). This happens, for example, with the simple commutators $[x_1, \ldots, x_m]$, and with the derived words.

Shumyatsky and the second author [4] considered the question of the previous paragraph in the realm of finitely generated residually finite p-groups. (By a residually finite p-group we mean a group in which the intersection of all the normal subgroups of finite p-power index is trivial. Thus we are not speaking about p-groups, that is groups all of whose elements have p-power order, that are at the same time residually finite.) One of their main results is the following: *for every n, there exists a finite set $P(n)$ of primes such that, if $p \notin P(n)$ and G is a finitely generated residually finite p-group that satisfies a law and can be generated by a normal and commutator-closed subset T satisfying a positive law of degree n, then G also satisfies a positive law.* Thus 'normal and commutator-closed' is a valid sense of largeness in the above setting (for example, for soluble residually finite p-groups), a fact that can be applied to several important instances of the problem for word values and verbal subgroups.

Our goal in this paper is to show that the hypothesis of finite generation of G cannot be dispensed with in the previous result. More precisely, we prove the following result.

THEOREM 1.1. *For every $c \ge 3$, there exists an infinitely generated metabelian group G with the following properties.*

(i)   *G is a residually finite p-group for all primes p.*

(ii)   *G can be generated by a commutator-closed normal subset T satisfying the positive law $M_c(x, y)$.*

(iii)   *G does not satisfy any positive laws.*

The main tool that is needed for the construction of this counterexample is to characterize when a union of cosets of an abelian normal subgroup satisfies a Mal′cev law, provided that the representatives of the cosets commute with each other. This is the goal of Section 2. Once this characterization is obtained, in Section 3 we proceed to construct the counterexample, and prove that our main theorem, Theorem 1.1, holds. It is noteworthy that the theory of monomial ideals in polynomial algebras plays an important role in the proof.

2. The Mal′cev law on unions of cosets of an abelian normal subgroup

If G is a group and A is an abelian normal subgroup of G, then every element $t \in G$ defines an automorphism of A by conjugation, which we denote by the same letter t. Since the set $\text{End}(A)$ of endomorphisms of A is a ring, we can combine these automorphisms with the operations of addition and composition, which we denote by juxtaposition.

We begin by determining when two elements in cosets tA and uA, with t and u commuting, satisfy a Mal′cev law.

LEMMA 2.1. *Let G be a group, and let A be an abelian normal subgroup of G. If $t, u \in G$ commute and $a, b \in A$, then the Mal′cev law $M_c(x, y)$ holds for the substitution $x = ta$, $y = ub$ if and only if*

$$a^{f_c(u,t)} = b^{f_c(t,u)},$$

where

$$f_c(X, Y) = (X - 1) \prod_{i=0}^{c-2} (X^{2^i} Y^{2^i} - 1).$$

PROOF. We define, for every $c \geq 1$, the word $w_c(x, y) = \beta_c(x, y)^{-1} \alpha_c(x, y)$. The lemma will be proved if we show that

$$w_c(ta, ub) = a^{f_c(u,t)} b^{-f_c(t,u)}.$$

We argue by induction on c. If $c = 1$, then

$$w_1(ta, ub) = (ubta)^{-1}(taub) = (utb^t a)^{-1}(tua^u b) = a^{u-1} b^{1-t},$$

and the result is true. Assume now that $c > 1$. Since

$$w_c = \beta_c^{-1} \alpha_c = \alpha_{c-1}^{-1} \beta_{c-1}^{-1} \alpha_{c-1} \beta_{c-1} = w_{c-1}^{\alpha_{c-1}} w_{c-1}^{-1},$$

it follows from the induction hypothesis that

$$w_c(ta, ub) = (a^{f_{c-1}(u,t)} b^{-f_{c-1}(t,u)})^{\alpha_{c-1}(ta,ub)} (a^{-f_{c-1}(u,t)} b^{f_{c-1}(t,u)}). \tag{2.1}$$

Now, since A is abelian, in order to calculate the conjugate in this last expression, we only need to know the value of $\alpha_{c-1}(ta, ub)$ modulo A. Since α_{c-1} has weight 2^{c-2} in both x and y, and t and u commute, it follows that

$$\alpha_{c-1}(ta, ub) \equiv \alpha_{c-1}(t, u) \equiv t^{2^{c-2}} u^{2^{c-2}} \mod A.$$

By putting this value into (2.1), we get

$$w_c(ta, ub) = a^{f_{c-1}(u,t)(t^{2^{c-2}}u^{2^{c-2}}-1)} b^{-f_{c-1}(t,u)(t^{2^{c-2}}u^{2^{c-2}}-1)},$$

which concludes the proof.   □

We now characterize when the unions of cosets of A that we are interested in satisfy a Mal′cev law.

THEOREM 2.2. *Let G be a group, and let A be an abelian normal subgroup of G. Consider a union of cosets $T = t_1 A \cup \cdots \cup t_n A \cup A$, where $t_1, \ldots, t_n$ commute with each other. Suppose that $t_1, \ldots, t_n$, as endomorphisms of A, satisfy the following conditions.*

(i) $(t_i - 1)^c = 0$ *when $i = 1, \ldots, n$.*
(ii) $(t_i - 1)(t_i t_j - 1)^{c-1} = 0$ *when $1 \leq i \neq j \leq n$.*

Then the subset T satisfies $M_c(x, y)$. Conversely, if T satisfies $M_c(x, y)$, and if G is nilpotent and A is torsion-free, then $t_1, \ldots, t_n$ satisfy conditions (i) and (ii) above.

PROOF. The law $M_c(x, y)$ holds in the subset T if and only if it holds for every substitution $x = ta$, $y = ub$, where $t, u \in \{1, t_1, \ldots, t_n\}$ and $a, b \in A$. By considering the case where $a = 1$ and b is arbitrary, it readily follows from Lemma 2.1 that T satisfies $M_c(x, y)$ if and only if $f_c(t, u)$ annihilates A for every $t, u \in \{1, t_1, \ldots, t_n\}$. Put differently, a necessary and sufficient condition for T to satisfy $M_c(x, y)$ is that the substitution $X \mapsto t_i$ in $f_c(X, 1)$ and $f_c(X, X)$, and the substitution $X \mapsto t_i$, $Y \mapsto t_j$ in $f_c(X, Y)$, where $i \neq j$, always induce the zero endomorphism of A.

Since

$$f_c(X, 1) = (X - 1)^c \prod_{i=1}^{c-2} (X^{2^i - 1} + \cdots + X + 1), \tag{2.2}$$

$$f_c(X, X) = f_c(X, 1) \prod_{i=0}^{c-2} (X^{2^i} + 1), \tag{2.3}$$

and

$$f_c(X, Y) = (X - 1)(XY - 1)^{c-1} \prod_{i=1}^{c-2} ((XY)^{2^i - 1} + \cdots + XY + 1), \tag{2.4}$$

it is clear that, if conditions (i) and (ii) of the statement hold, then T satisfies $M_c(x, y)$. This proves the first assertion of the theorem.

Conversely, suppose now that T satisfies $M_c(x, y)$, that G is nilpotent and that A is torsion-free. By (2.2), (2.3), and (2.4),

$$f_c(X, 1) = (X - 1)^c g_c(X), \quad f_c(X, X) = (X - 1)^c h_c(X), \tag{2.5}$$

and

$$f_c(X, Y) = (X - 1)(XY - 1)^{c-1} g_c(XY), \tag{2.6}$$

for some polynomials $g_c(X), h_c(X) \in \mathbb{Z}[X]$ that are coprime to $X - 1$. Now we claim that, for every polynomial $j(X) \in \mathbb{Z}[X]$ that is coprime to $X - 1$, and for every automorphism φ of A that is induced by conjugation by an element of G, the endomorphism $j(\varphi)$ is injective. Once this is proved, it follows from (2.5) and (2.6), and from the discussion in the first paragraph of the proof, that (i) and (ii) must hold.

Hence it only remains to prove the claim. Let k be the nilpotency class of G. Since $j(X)$ is coprime to $X - 1$, by using Bézout's identity in $\mathbb{Q}[X]$ we get an expression of the form

$$p(X)(X - 1)^k + q(X)j(X) = m, \tag{2.7}$$

where $p(X), q(X) \in \mathbb{Z}[X]$ and m is a positive integer. Now, G is nilpotent of class k and φ is induced by conjugation by an element of G, and so $(\varphi - 1)^k = 0$. By substituting φ for X in (2.7), it follows that $q(\varphi)j(\varphi) = m1_A$. Taking into account the fact that A is torsion-free, we conclude that $j(\varphi)$ is injective, as desired. $\qquad\square$

3. Construction of the counterexample

The key to our counterexample is the next lemma, where we show that for every $n \geq c$ there exists a nilpotent group G_n that can be generated by a normal and commutator-closed subset T_n satisfying $M_c(x, y)$, but nevertheless G_n does not satisfy any law $M_k(x, y)$ for $k \leq n$. Thus the 'distance' between the Mal'cev laws satisfied by T_n and G_n increases as n goes to infinity.

LEMMA 3.1. *Let $c \geq 3$ be a fixed integer. Then, for every $n \geq c$ there exists a finitely generated nilpotent torsion-free group $G_n = B_n \ltimes A_n$ with the following properties.*

(i) A_n *and* B_n *are abelian groups. Thus* G_n *is metabelian.*
(ii) B_n *can be generated by* n *elements* $t_1, \ldots, t_n$ *such that the subset* $T_n = t_1 A_n \cup \cdots \cup t_n A_n \cup A_n$ *satisfies the law* $M_c(x, y)$.
(iii) G_n *does not satisfy* $M_n(x, y)$. *More precisely, for every* $e \geq 1$, *the law* $M_n(x, y)$ *is not satisfied in the coset* $(t_1 \ldots t_n)^e A_n$.

PROOF. The idea of the proof is to put $A_n = \mathbb{Z}^d$ for some d (to be determined in the course of the proof), and to let $t_1, \ldots, t_n$ be commuting matrices in $\mathrm{GL}_d(\mathbb{Z})$ that fulfil the necessary conditions for T_n to satisfy $M_c(x, y)$, and for G_n not to satisfy $M_n(x, y)$. These are the conditions that can be read in Theorem 2.2. The matrices $t_1, \ldots, t_n$ will arise from the regular representation of an appropriate quotient of the algebra of polynomials $\mathbb{Q}[X_1, \ldots, X_n]$.

Consider the ideal

$$\mathfrak{a} = ((X_1 - 1)^c, \ldots, (X_n - 1)^c, (X_i - 1)(X_i X_j - 1)^{c-1} \mid 1 \leq i \neq j \leq n)$$

of $\mathbb{Q}[X_1, \ldots, X_n]$. Under the isomorphism $X_i \mapsto X_i + 1$, this ideal maps onto

$$\mathfrak{b} = (X_1^c, \ldots, X_n^c, X_i(X_i + X_j + X_i X_j)^{c-1} \mid 1 \leq i \neq j \leq n).$$

One can readily check that $\mathfrak{b}$ is contained in the monomial ideal

$$\mathfrak{c} = (X_1^{i_1} \cdots X_n^{i_n} \mid i_1 + \cdots + i_n = c \text{ and } i_j \geq 2 \text{ for some } j);$$

note that $c \geq 3$ is necessary for this. Also, if $\mathfrak{m}$ is the maximal ideal of $\mathbb{Q}[X_1, \ldots, X_n]$ generated by all the indeterminates $X_1, \ldots, X_n$, then $\mathfrak{m}^{n+1}$ is contained in $\mathfrak{c}$, since $n \geq c$.

Let $e \geq 1$ be an arbitrary integer. Since

$$(X_1 + 1)^e (X_2 + 1)^e \cdots (X_n + 1)^e - 1 \equiv e(X_1 + X_2 + \cdots + X_n) \quad \mod \mathfrak{m}^2,$$

it follows that

$$((X_1 + 1)^e (X_2 + 1)^e \cdots (X_n + 1)^e - 1)^n \equiv e^n (X_1 + X_2 + \cdots + X_n)^n \quad \mod \mathfrak{m}^{n+1}.$$

This last congruence also holds modulo $\mathfrak{c}$, since $\mathfrak{m}^{n+1} \subseteq \mathfrak{c}$. As a consequence,

$$((X_1 + 1)^e (X_2 + 1)^e \cdots (X_n + 1)^e - 1)^n \equiv e^n n! X_1 \cdots X_n \quad \mod \mathfrak{c}. \qquad (3.1)$$

On the other hand, by [3, Lemma 2, p. 67],

$$X_1 \cdots X_n \notin \mathfrak{c},$$

since $\mathfrak{c}$ is a monomial ideal and $X_1 \cdots X_n$ is not divisible by any of the generators in the definition of $\mathfrak{c}$. Thus, it follows from (3.1) that

$$((X_1 + 1)^e (X_2 + 1)^e \cdots (X_n + 1)^e - 1)^n \notin \mathfrak{c}. \qquad (3.2)$$

Now put $A = \mathbb{Q}[X_1, \ldots, X_n]/\mathfrak{c}$, and let d be the dimension of A as a $\mathbb{Q}$-vector space. The set

$$\mathcal{B} = \{X_1^{i_1} \cdots X_n^{i_n} + \mathfrak{c} \mid X_1^{i_1} \cdots X_n^{i_n} \text{ is not a multiple of a generator of } \mathfrak{c}\}$$

is a basis of A, by [3, Proposition 4, p. 229]. We order $\mathcal{B}$ first by total degree of the monomials, and then arbitrarily among monomials of the same degree. Let us consider the regular representation φ of A in $M_d(\mathbb{Q})$, where matrices are taken with respect to the basis $\mathcal{B}$, and put $t_i = \varphi(X_i + 1 + \mathfrak{c})$. Obviously, $t_1, \ldots, t_n$ commute with each other. Also, since the basis $\mathcal{B}$ consists only of monomials, and these are ordered according to their degree, the matrices t_i have only 0 and 1 entries, and are upper unitriangular. In other words, $t_i \in UT_d(\mathbb{Z})$, the group of upper unitriangular matrices over the integers.

Hence, we can consider the semidirect product $G_n = B_n \ltimes A_n$ of the groups $A_n = \mathbb{Z}^d$ and $B_n = \langle t_1, \ldots, t_n \rangle$, with respect to the natural action of B_n on A_n. Clearly, G_n satisfies (i). Since $UT_d(\mathbb{Z})$ is a torsion-free group (see [8, p. 128]), B_n is also torsion-free. Hence the same is true for G_n. On the other hand, since A_n and B_n are abelian, $\gamma_i(G_n) = [A_n, B_n, \overset{i-1}{\ldots}, B_n]$ for all $i \geq 1$ (see [6, Ch. 3, Lemma 15.2]). Since B_n is contained in the unitriangular group, it follows that G_n is a nilpotent group.

On the other hand, since X_i^c and $X_i(X_i + X_j + X_iX_j)^{c-1}$ lie in $\mathfrak{c}$, it follows readily that $(t_i - 1)^c = (t_i - 1)(t_it_j - 1)^{c-1} = 0$ for all $1 \le i \ne j \le n$. Also, as a consequence of (3.2), $(t_1^e \cdots t_n^e - 1)^n \ne 0$ for every $e \ge 1$. Thus we can conclude from Theorem 2.2 that T_n satisfies $M_c(x, y)$, and that $M_n(x, y)$ is never satisfied in a coset of the form $t_1^e \cdots t_n^e A_n$, where $e \ge 1$. $\square$

We are now ready to prove our main theorem, Theorem 1.1.

PROOF OF THEOREM 1.1 We use the same notation as in Lemma 3.1. We define G to be the restricted direct product $\prod_{n \ge c} G_n$. Note that G is metabelian. Since G_n is a finitely generated nilpotent torsion-free group, it is a residually finite p-group for all primes p, by a result of Gruenberg [5]. As a consequence, the same is true for G and (i) holds.

Since the direct product G is restricted and $G_n = \langle T_n \rangle$ for all n, it follows that the subset $T = \bigcup_{n \ge c} T_n$ generates G. By the definition of T_n, it is clear that it is a normal subset of G_n, and also commutator-closed. (Recall that $t_1, \ldots, t_n$ commute with each other.) As a consequence, T is commutator-closed and a normal subset of G. Also, since every T_n satisfies the law $M_c(x, y)$, so also does T: note that two elements from T_n and T_m, where $n \ne m$, commute. Thus we obtain (ii).

Finally, let us see that G cannot satisfy a positive law. Otherwise, by the result of Burns and Medvedev mentioned in the introduction, G has a normal nilpotent subgroup N such that G/N has finite exponent. Let k and e be the class of N and the exponent of G/N, respectively. Then the subgroup G_k^e satisfies the law $M_k(x, y)$ and, in particular, the same is true for the coset $(t_1 \cdots t_k)^e A_k^e$. Now, it follows from Theorem 2.2 that the endomorphism $(t_1^e \cdots t_k^e - 1)^k$ is zero on the abelian group A_k^e. Since A_k is a torsion-free group, $(t_1^e \cdots t_k^e - 1)^k$ is also zero as an endomorphism of A_k. This means that the coset $(t_1 \cdots t_k)^e A_k$ satisfies $M_k(x, y)$, which is a contradiction, according to part (iii) of Lemma 3.1. $\square$

References

[1]   B. Bajorska and O. Macedońska, 'On positive law problems in the class of locally graded groups', *Comm. Algebra* **32** (2004), 1841–1846.

[2]   R. G. Burns and Yu. Medvedev, 'Groups laws implying virtual nilpotence', *J. Aust. Math. Soc.* **74** (2003), 295–312.

[3]   D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, 2nd edn, Undergraduate Texts in Mathematics (Springer, Berlin–Heidelberg–New York, 1997).

[4]   G. A. Fernández-Alcober and P. Shumyatsky, 'Positive laws on word values in residually-p groups', Preprint, 2010.

[5]   K. W. Gruenberg, 'Residual properties of infinite soluble groups', *Proc. Lond. Math. Soc.* **7** (1957), 29–62.

[6]   B. Huppert, *Endliche Gruppen I*, Grundlehren der Mathematischen Wissenschaften, 134 (Springer, Berlin–Heidelberg–New York, 1967).

[7]   A. Yu. Olshanskii and A. Storozhev, 'A group variety defined by a semigroup law', *J. Aust. Math. Soc. (Series A)* **60** (1996), 225–259.

[8]   D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd edn, Graduate Texts in Mathematics, 80 (Springer, Berlin–Heidelberg–New York, 1996).

CRISTINA ACCIARRI, Dipartimento di Matematica Pura ed Applicata,
Università degli Studi dell'Aquila, I-67010 Coppito, L'Aquila, Italy
e-mail: acciarricristina@yahoo.it

GUSTAVO A. FERNÁNDEZ-ALCOBER, Matematika Saila,
Euskal Herriko Unibertsitatea, 48080 Bilbao, Spain
e-mail: gustavo.fernandez@ehu.es