J. Group Theory **24** (2021), 453–466
DOI 10.1515/jgth-2020-0091

Metabelian groups: Full-rank presentations, randomness and Diophantine problems

Albert Garreta*, Leire Legarreta, Alexei Miasnikov and Denis Ovchinnikov

Communicated by Evgenii I. Khukhro

Abstract. We study metabelian groups G given by full rank finite presentations $\langle A \mid R\rangle_{\mathcal{M}}$ in the variety $\mathcal{M}$ of metabelian groups. We prove that G is a product of a free metabelian subgroup of rank $\max\{0, |A| - |R|\}$ and a virtually abelian normal subgroup, and that if $|R| \leq |A| - 2$, then the Diophantine problem of G is undecidable, while it is decidable if $|R| \geq |A|$. We further prove that if $|R| \leq |A| - 1$, then, in any direct decomposition of G, all factors, except one, are virtually abelian. Since finite presentations have full rank asymptotically almost surely, metabelian groups finitely presented in the variety of metabelian groups satisfy all the aforementioned properties asymptotically almost surely.

1 Introduction

In this paper, we study finitely generated metabelian groups G given by full rank finite presentations $G = \langle a_1, \dots, a_n \mid r_1, \dots, r_m\rangle_{\mathcal{M}}$ in the variety $\mathcal{M}$ of metabelian groups, random metabelian groups in the few relators model, and the Diophantine problem in such groups. Our research can be viewed as a natural continuation of the study of nilpotent groups admitting full rank presentations in [11]. Furthermore, some key results from [11] are also used here.

In what follows, we briefly describe our approach and the main contributions of the paper. The rest of the paper is devoted to proving the corresponding results.

1.1 Metabelian groups with full rank presentations

Let $A = \{a_1, \dots, a_n\}$ be a finite alphabet, $A^{-1} = \{a_1^{-1}, \dots, a_n^{-1}\}$, $A^{\pm 1} = A \cup A^{-1}$, $(A^{\pm 1})^*$ the set of all (finite) words in $A^{\pm 1}$, and $R = \{r_1, \dots, r_m\}$ a finite subset of $(A^{\pm})^*$. We fix this notation for the rest of the paper.

This work was supported by the Russian Science Foundation grant project 19-11-00209. Additionally, the first named author was supported by the ERC grant PCG-336983. The first and second named authors were supported by the Basque Government grant IT974-16, and by the Ministry of Economy, Industry and Competitiveness of the Spanish Government Grant MTM2017-86802-P.

A pair (A, R) is called a *finite presentation*; we denote it by

$$\langle A \mid R \rangle \quad \text{or} \quad \langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle.$$

If $\mathcal{V}$ is a variety or a quasivariety of groups (see [2, 20]), then a finite presentation $\langle A \mid R \rangle$ determines a group $G = F_{\mathcal{V}}(A)/\langle\langle R \rangle\rangle$, where $F_{\mathcal{V}}(A)$ is a free group in $\mathcal{V}$ with basis A and $\langle\langle R \rangle\rangle$ is the normal subgroup of $F_{\mathcal{V}}(A)$ generated by R. In this case, we write $G = \langle A \mid R \rangle_{\mathcal{V}}$. The *relation matrix* $M(A, R)$ of the presentation $\langle A \mid R \rangle$ is an $m \times n$ integral matrix whose (i, j)-th entry is the sum of the exponents of the a_j's that occur in r_i. It was introduced by Magnus in [17] (see also [16, Chapter II.3] for its ties to relation modules in groups). The number $d = |A| - |R|$, if non-negative, is called the *deficiency* of the presentation $\langle A \mid R \rangle$ (see [16, Chapter II.2] for a short survey on groups with positive deficiency). The matrix $M(A, R)$ has *full rank* if its rank is equal to $\min\{|A|, |R|\}$, i.e., it is the maximum possible.

We showed in [11] that if a finitely generated nilpotent group G admits a full-rank presentation, then G is either virtually free nilpotent (provided the deficiency $d \geq 2$), or virtually cyclic (if $d = 1$), or finite (if $d \leq 0$).

Groups given in the variety $\mathcal{M}$ of all metabelian groups by full rank presentations also have a rather restricted structure, as witnessed by the following result.

Theorem 1.1. *Let G be a metabelian group given by a full-rank presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$. Then there exist two finitely generated subgroups H and K of G such that*

(1) *H is a free metabelian group of rank* $\max(|A| - |R|, 0)$,

(2) *K is a virtually abelian group with $|R|$ generators, and its normal closure $L = K^G$ in G is again virtually abelian,*

(3) $G = \langle H, K \rangle = LH$.

Moreover, there is an algorithm that, given a presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$, finds a free basis for the subgroup H and a generating set in $|R|$ generators for the subgroup K.

The result above complements the Generalized Freiheitssatz for $\mathcal{M}$. In [23], Romanovskii proved that if a metabelian group G is given in the variety $\mathcal{M}$ by a finite presentation $\langle A \mid R \rangle_{\mathcal{M}}$ of deficiency $d \geq 1$, then there is a subset of generators $A_0 \subseteq A$ with $|A_0| = d$ which freely generates a free metabelian subgroup $H = \langle A_0 \rangle$. Theorem 1.1 shows that if the presentation $\langle A \mid R \rangle_{\mathcal{M}}$ has full rank, then there is a free metabelian of rank d subgroup H of G and, in addition, there are virtually abelian subgroups K and L as described in items (2) and (3) above

such that $G = HL$. Two remarks are in order here. First, the subgroup H in Theorem 1.1 is not necessarily equal to $\langle A_0 \rangle$ for a suitable $A_0 \subseteq A$ as in Romanovskii's result. However, for a given full rank presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$ of G, one can find algorithmically another full rank presentation of G, which is in Smith normal form (see Section 2.1), such that the subgroup H is, indeed, generated by a suitable $A_0 \subseteq A$ and K is generated by $A \setminus A_0$. Second, even if the presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$ is in Smith normal form, but it is not of full rank, then the subgroups K and L as in Theorem 1.1 may not necessarily exist (see details in Section 2.1).

In another direction, the authors showed in [11] that, in any direct decomposition of a nilpotent group G given in the nilpotent variety $\mathcal{N}_c$, $c \geq 2$, by a finite full rank presentation of deficiency ≥ 1, all but one of the direct factors are finite.

A similar result holds in the variety $\mathcal{M}$ as well.

Theorem 1.2. *Let G be a finitely generated metabelian group given by a full-rank presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$ such that $|R| \leq |A| - 1$. Then, in any direct decomposition of G, all but one of the direct factors are virtually abelian.*

1.2 Diophantine problems

In Section 3, we study the Diophantine problem in finitely generated metabelian groups given by full rank presentations. This is a continuation of research in [8,11].

Recall that the *Diophantine problem* in an algebraic structure $\mathcal{A}$, denoted $\mathcal{D}(\mathcal{A})$, is the task to determine whether or not a given finite system of equations with constants in $\mathcal{A}$ has a solution in $\mathcal{A}$. $\mathcal{D}(\mathcal{A})$ is *decidable* if there is an algorithm that, given a finite system S of equations with constants in $\mathcal{A}$, decides whether or not S has a solution in $\mathcal{A}$. Furthermore, $\mathcal{D}(\mathcal{A})$ is *reducible* to $\mathcal{D}(\mathcal{M})$ for another structure $\mathcal{M}$ if there is an algorithm that, for any finite system of equations S in $\mathcal{A}$, computes a finite system of equations $S_{\mathcal{M}}$ in $\mathcal{M}$ such that S has a solution in $\mathcal{A}$ if and only if $S_{\mathcal{M}}$ has a solution in $\mathcal{M}$.

Note that, due to the classical result of Davis, Putnam, Robinson and Matiyasevich, the Diophantine problem $\mathcal{D}(\mathbb{Z})$ in the ring of integers $\mathbb{Z}$ is undecidable [5, 19]. Hence, if $\mathcal{D}(\mathbb{Z})$ is reducible to $\mathcal{D}(\mathcal{M})$, then $\mathcal{D}(\mathcal{M})$ is also undecidable.

To prove that $\mathcal{D}(\mathcal{A})$ reduces to $\mathcal{D}(\mathcal{M})$ for some structures $\mathcal{A}$ and $\mathcal{M}$, it suffices to show that $\mathcal{A}$ is interpretable by equations (or *e-interpretable*) in $\mathcal{M}$. E-interpretability is a variation of the classical notion of first-order interpretability, where, instead of arbitrary first-order formulas, finite systems of equations are used as the interpreting formulas (see Definition 3.3 for details). The main relevant property of such interpretations is that if $\mathcal{A}$ is e-interpretable in $\mathcal{M}$, then $\mathcal{D}(\mathcal{A})$ is reducible to $\mathcal{D}(\mathcal{M})$ by a polynomial time many-to-one reduction (Karp reduction).

Theorem 1.3. *Let G be a metabelian group given by a full-rank presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$. Then the following hold.*

(1) *If $|R| \leq |A| - 2$, then the ring of integers $\mathbb{Z}$ is e-interpretable in G, and the Diophantine problem in G is undecidable.*

(2) *If $|R| \geq |A|$, then the Diophantine problem of G is decidable (in fact, the first-order theory of G is decidable).*

This result is analogous to that obtained for nilpotent groups in [11].

Remark 1.4. For the case of deficiency 1 (i.e., $m = n - 1$), decidability of the Diophantine problem over G remains an interesting open problem. The recent work [15] proves decidability of the Diophantine problem in

$$\mathrm{BS}(1, n) = \langle a_1, a_2 \mid a_1^{n-1} = [a_1, a_2] \rangle.$$

Also some deficiency-1 presentations define cyclic groups, which have decidable Diophantine problem [7].

Conjecture 1.5. *Let G be a metabelian group given by a full-rank presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$. If $|A| - |R| = 1$, then the Diophantine problem in G is decidable.*

1.3 Random finitely presented groups: the few-relations model

The first notion of *genericity* or a *random group* in the class of finitely presented groups is due to Gromov [12], where he introduced what is now known as the few relators model. A slightly different approach was suggested by Olshanskii [22] and Arzhantseva and Olshanskii [1].

Nowadays, the few relators model can be described as follows. Let m, n be fixed positive integers. Consider, in the notation above, the set $S(n, m)$ of all finite presentations $\langle A \mid R \rangle$ with $|A| = n$, $|R| = m$. For a given positive integer ℓ, consider a finite subset $S(n, m, \ell)$ of $S(n, m)$ which consists of all presentations $\langle A \mid R \rangle \in S(n, m)$, where each relator in R has length precisely ℓ. Now, for a given property of groups P, consider a subset $S_P(n, m, \ell)$ of $S(n, m, \ell)$ of all presentations $\langle A \mid R \rangle \in S(n, m, \ell)$ which define groups that satisfy P. The property P is termed (n, m)-*generic* if

$$\lim_{\ell \to \infty} \frac{|S_P(n, m, \ell)|}{|S(n, m, \ell)|} = 1.$$

Here $|X|$ denotes the cardinality of a set X. In this event, we also say sometimes that P holds for $\langle A \mid R \rangle$ *asymptotically almost surely as* $\ell \to \infty$.

In the book [12], Gromov stated that the group property of being hyperbolic is (n,m)-generic for all n and m. Later, Olshanskii [22] and Champetier [3] gave rigorous proofs of this result. We refer to [21] for a survey on random finitely presented groups and to Kapovich and Schupp [14] on group theoretic models of randomness and genericity.

Observe that the few relators model described above concerns classical finitely presented groups. However, this approach can be utilized as well for finitely presented groups in any fixed variety of groups $\mathcal{V}$, in particular, for finitely generated metabelian groups given in the variety $\mathcal{M}$ of all metabelian groups by finite presentations $\langle A \mid R\rangle_{\mathcal{M}}$. Note that every finitely generated group in $\mathcal{M}$ has a finite presentation in $\mathcal{M}$.

For the variety of nilpotent groups $\mathcal{N}_c$ (of a fixed nilpotency class c), this approach has been studied recently in [4, 11]. Other models of randomness for the groups in $\mathcal{N}_c$ can be found in [6,8]. To the best of our knowledge, there is no study of random metabelian groups (in any model) prior to this paper.

The following result is fundamental to our approach.

Theorem 1.6 ([11]). *Let R be a set of m words of length ℓ in an alphabet*

$$A^{\pm 1} = \{a_1^{\pm 1}, \dots, a_n^{\pm 1}\},$$

i.e., each word is obtained by successively concatenating randomly chosen letters from $A^{\pm 1}$ with uniform probability. Then $M(A,R)$ has full rank (that is, $\operatorname{rank}(M(A,R)) = \min\{n,m\}$*) asymptotically almost surely as $\ell \to \infty$.*

Corollary 1.7. *Let $\langle A \mid R\rangle = \langle a_1, \dots, a_n \mid r_1, \dots, r_m\rangle$ be a presentation where all relators r_i have length $\ell > 0$. Then the presentation $\langle A \mid R\rangle$ has full rank asymptotically almost surely as ℓ tends to infinity.*

One of the main appeals of full-rank presentations is that they occur asymptotically almost surely in the few-relators model for random groups in any variety $\mathcal{V}$, in particular, in the variety $\mathcal{M}$. Hence, random metabelian groups (in the few relators model) have full rank presentations asymptotically almost surely. Therefore, all the properties described above for metabelian groups given by full rank presentations are generic in the class of finitely presented metabelian groups. We refer to Section 4 for precise statements of the results.

2 Structural properties of metabelian groups given by full-rank presentations

Throughout the paper, we use the following notation. We denote by $\mathcal{N}_c$ and $\mathcal{M}$ the families of nilpotent groups of nilpotency class at most c, and of metabelian

groups, respectively. In general, we refer to books [16, 24] for the standard facts and notation in group theory and to [20] for basic notions regarding varieties.

2.1 A variation of the Generalized Freiheitssatz

In this section, we obtain some structural results on full rank metabelian groups, in particular, Theorem 1.1. To prove this theorem, we need some results on presentations in Smith normal form.

Recall (see, for example, [26]) that an integer matrix $A = (a_{ij})$ is in *Smith normal form* if there is some integer $r \geq 0$ such that the entries $d_i = a_{ii}$, $1 \leq i \leq r$, are positive, A has no other nonzero entries, and d_i divides d_{i+1} for $1 \leq i < r$.

Definition 2.1. A finite presentation $\langle A \mid R \rangle$ is said to be in *Smith normal form* if the relation matrix $M(A, R)$ is in Smith normal form.

Proposition 2.2. *For any finite presentation $\langle A \mid R \rangle$, there exists a finite presentation in Smith normal form $\langle A' \mid R' \rangle$, with*

$$|A| = |A'|, \quad |R| = |R'| \quad \textit{and} \quad \operatorname{rank}(M(A, R)) = \operatorname{rank}(M(A', R')),$$

such that, for any variety $\mathcal{V}$, the groups $G = \langle A \mid R \rangle_{\mathcal{V}}$ and $G' = \langle A' \mid R' \rangle_{\mathcal{V}}$ are isomorphic. Moreover, such a presentation $\langle A' \mid R' \rangle$ and an isomorphism $G \to G'$ can be found algorithmically.

Proof. The presentation $\langle A' \mid R' \rangle$ can be obtained by repeatedly applying Nielsen transformations on the tuples A and R. Indeed, note that such a Nielsen transformation has the effect in the relation matrix $M(A, R)$ of adding or subtracting two columns or two rows, respectively. It is known (see [26]) that one can find a finite sequence of elementary row and column operations that transforms $M(A, R)$ into its Smith normal form. Performing the corresponding Nielsen transformation on $\langle A \mid R \rangle$, one gets the required presentation $\langle A' \mid R' \rangle$. The details of this procedure can be found in [11]. □

The complexity of finding a presentation in Smith normal form and other algorithmic considerations regarding full-rank presentations and presentations in Smith normal form will be studied in upcoming work.

Lemma 2.3. *Let G be a metabelian group given by a full-rank presentation in Smith normal form,*

$$G = \langle A \mid R \rangle_{\mathcal{M}} = \langle a_1, \ldots, a_n \mid a_1^{\alpha_1} = c_1, \ldots, a_m^{\alpha_m} = c_m \rangle_{\mathcal{M}},$$

where $c_i \in [F(A), F(A)]$, $\alpha_i \in \mathbb{Z} \setminus \{0\}$ for all $i = 1, \ldots, m$, and $m \leq n$. Then the following holds.

(1) *$K = \langle a_1, \ldots, a_m \rangle$ is a virtually abelian group, and its normal closure $L = K^G$ in G is again virtually abelian.*

(2) *$H = \langle a_{m+1}, \ldots, a_n \rangle$ is a free metabelian group of rank $n - m$.*

(3) *$G = \langle H, K \rangle = HL$.*

Proof. We show first that $K = \langle a_1, \ldots, a_m \rangle$ is virtually abelian. Note that $K \cap G'$ is abelian. Set $N = \alpha_1 \cdots \alpha_m$. Then, for all $g \in K$, one has $g^N \in K \cap G'$. Hence, $K/K \cap G'$ is finite, so K is virtually abelian. Similarly, for $L = K^G$, the subgroup $L \cap G'$ is normal in L and abelian. The quotient $L/L \cap G'$ is abelian, of period N, and finitely generated (since $L = K(L \cap G')$), hence finite. It follows that L is abelian-by-(finite abelian). Note that L might not be finitely generated.

Now we show that $\langle a_{m+1}, \ldots, a_n \rangle$ is a free metabelian group of rank $n - m$. Assume that $n - m \geq 2$. By Romanovskii's aforementioned result [23] (see the discussion after the statement of Theorem 1.1), we know that there exists a subset $A_1 \subseteq A$ with $|A_1| = |A| - |R|$ such that $\langle A_1 \rangle$ is free metabelian freely generated by A_1. We claim that $A_1 = \{a_{m+1}, \ldots, a_n\}$. Indeed, otherwise, there exists $a_i \in A_1$ such that $a_i^t \in G'$ for some $t \in \mathbb{Z} \smallsetminus \{0\}$. Note that $|A_1| \geq 2$, so there is $a_j \in A_1$ with $i \neq j$. It follows then that $[a_i^t, [a_i, a_j]] = 1$, a contradiction with the fact that A_1 freely generates $\langle A_1 \rangle$ as a free metabelian group.

If $n - m = 1$, then the map $a_n \to 1$ and $a_i \to 0$ for all $i = 1, \ldots, n-1$ gives rise to a homomorphism $G \to \mathbb{Z}$. Hence, a_n has infinite order in G, and $\langle a_n \rangle$ is a free metabelian group of rank 1. We note in passing that, in the case when $m = n - 1$, the element of A that generates an infinite cyclic group (i.e., a free metabelian group of rank 1) is not necessarily unique, e.g., in

$$\mathrm{BS}(1, n) \cong \langle a_1, a_2 \mid a_1^{n-1} = [a_1, a_2] \rangle,$$

both a_1 and a_2 generate an infinite cyclic subgroup. □

Proof of Theorem 1.1. Let G be a metabelian group given by a full-rank presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$. By Proposition 2.2, one can find algorithmically another presentation $\langle A' \mid R' \rangle_{\mathcal{M}} = \langle a_1', \ldots, a_n' \mid r_1', \ldots, r_m' \rangle_{\mathcal{M}}$ of G which is in Smith normal form.

If $m \leq n$, then Lemma 2.3 applied to the presentation $\langle A', \mid R' \rangle$ gives subgroups H and K with the required properties. From these, we obtain the required subgroups in G by inverting the isomorphism $\langle A \mid R \rangle = \langle A' \mid R \rangle$.

On the other hand, if $m > n$, then G is a quotient of the full-rank metabelian group with zero deficiency $G_1 = \langle a_1', \ldots, a_n' \mid r_1', \ldots, r_n' \rangle$ (since $M(A', R')$ is in Smith normal form, this is a full-rank presentation), and by the previous case, it follows that G_1 is virtually abelian. Since G is a quotient of G_1, G is also virtually abelian. □

Remark 2.4. Note that if the presentation in Lemma 2.3 is in Smith normal form, but not of full rank, then, by the Generalized Freiheitssatz [23], the free subgroup $H = \langle A_0 \rangle$ of G exists, but there might not exist corresponding subgroups K and L for H. Indeed, let

$$G = \langle a_1, a_2, a_3, a_4 \mid [a_1, a_3] = 1,\ [a_2, a_4] = 1 \rangle.$$

Then a_3, a_4 generate a free metabelian group of rank 2, but G/H^G is free metabelian of rank 2, so there is not a virtually abelian subgroup L such that $G = HL$.

Remark 2.5. Finally, note that Theorem 1.1 or Lemma 2.3 may not reveal fully the structure of G and how it is related to the subgroups H and K. For example, consider

$$G = \langle a_1, a_2, a_3, a_4 \mid a_1^m = [a_1, a_3],\ a_2^k = [a_2, a_4] \rangle.$$

Lemma 2.3 tells us that $\langle a_3, a_4 \rangle$ is freely generated by a_3, a_4 and $\langle a_1, a_2 \rangle$ is a virtually abelian group. On the other hand, it is easy to check that

$$\langle a_1, a_3 \rangle \cong \mathrm{BS}(1, m+1), \quad \langle a_2, a_4 \rangle \cong \mathrm{BS}(1, k+1),$$

and G is the free metabelian product of two Baumslag–Solitar groups, which is not clear directly from the decomposition $G = HL$.

2.2 Direct decompositions

In this section, we prove our main result on direct decomposition of metabelian groups given by full rank presentations, Theorem 1.2. We denote the terms of the lower central series of a group G by $\gamma_i(G)$, $i = 1, \ldots,$ where $\gamma_1(G) = G$ and $\gamma_{i+1}(G) = [G, \gamma_i(G)]$ for all $i \geq 1$.

Proof of Theorem 1.2. We showed in [11] that if H is a finitely generated nilpotent group of class $c \geq 2$ given by a finite full rank presentation $H = \langle A \mid R \rangle_{\mathcal{N}_c}$ with $|R| \leq |A| - 1$, then, in any direct decomposition of H, all but one of the direct factors are finite. We will use this fact in our proof. Now let G be a finitely generated metabelian group given by a full-rank presentation $G = \langle A \mid R \rangle_{\mathcal{M}}$ such that $|R| \leq |A| - 1$. Assume $G = G_1 \times \cdots \times G_k$ for some $k \geq 2$ and some subgroups G_i, $i = 1, \ldots, k$. Let π be the natural projection of G onto $H = G/\gamma_3(G)$. The quotient H admits the full-rank presentation $\langle A \mid R \rangle_{\mathcal{N}_2}$, so, by the result mentioned above, all but one, say $\pi(G_k)$, of the groups $\pi(G_1), \ldots, \pi(G_k)$ are finite. Hence, $\ker \pi \cap G_i$ has finite index in G_i for all $i = 1, \ldots, k-1$. However, $\ker \pi$ is abelian since $\ker \pi = \gamma_3(G) \leq [G, G]$. □

3 Diophantine problem

3.1 Diophantine problem and e-interpretability

In this section, we introduce the technique of interpretability by systems of equations. It is nothing other than the classical model-theoretic technique of interpretability (see [13, 18]), restricted to systems of equations (equivalently, positive existential formulas without disjunctions). In [9, 10], we used this technique to study the Diophantine problem in different classes of solvable groups and rings.

In what follows, we often use non-cursive boldface letters to denote tuples of elements: e.g. $\mathbf{a} = (a_1, \dots, a_n)$. Furthermore, we always assume that equations may contain constants from the algebraic structure in which they are considered.

Definition 3.1. A set $D \subset M^m$ is called *definable by systems of equations* in $\mathcal{M}$, or *e-definable* in $\mathcal{M}$, if there exists a finite system of equations, say

$$\Sigma_D(x_1, \dots, x_m, y_1, \dots, y_k),$$

in the language of $\mathcal{M}$ such that, for any tuple $\mathbf{a} \in M^m$, one has that $\mathbf{a} \in D$ if and only if the system $\Sigma_D(\mathbf{a}, \mathbf{y})$ on variables $\mathbf{y}$ has a solution in $\mathcal{M}$. In this case, Σ_D is said to *e-define* D in $\mathcal{M}$.

Remark 3.2. Observe that, in the notation above, if $D \subset M^m$ is e-definable, then it is definable in $\mathcal{M}$ by the formula $\exists \mathbf{y} \Sigma_D(\mathbf{x}, \mathbf{y})$. Such formulas are called *positive primitive*, or pp-formulas. Hence, e-definable subsets are sometimes called pp-definable. On the other hand, in number theory, such sets are usually referred to as Diophantine. And yet, in algebraic geometry, they can be described as projections of algebraic sets.

Definition 3.3. An algebraic structure $\mathcal{A} = (A; f, \dots, r, \dots, c, \dots)$ is called *e-interpretable* in another algebraic structure $\mathcal{M}$ if there exists $n \in \mathbb{N}$, a subset $D \subseteq \mathcal{M}^n$ and an onto map (called the *interpreting* map) $\phi \colon D \twoheadrightarrow \mathcal{A}$ such that the following holds.

(1) D is e-definable in $\mathcal{M}$.

(2) For every function $f = f(x_1, \dots, x_n)$ in the language of $\mathcal{A}$, the preimage by ϕ of the graph of f, i.e., the set $\{(x_1, \dots, x_k, x_{k+1}) \mid \phi(x_{k+1}) = f(x_1, \dots, x_k)\}$, is e-definable in $\mathcal{M}$.

(3) For every relation r in the language of $\mathcal{A}$, and also for the equality relation $=$ in $\mathcal{A}$, the preimage by ϕ of the graph of r is e-definable in $\mathcal{M}$.

The following result is a fundamental property of e-interpretability. Intuitively, it states that if $\mathcal{A}$ is e-interpretable in $\mathcal{M}$, then any system of equations in $\mathcal{A}$ can be "encoded" as a system of equations in $\mathcal{M}$.

Lemma 3.4. *Let $\mathcal{A}$ be e-interpretable in $\mathcal{M}$ with an interpreting map $\phi\colon D \twoheadrightarrow \mathcal{A}$ (in the notation of Definition* 3.3*). Then, for every finite system of equations $S(\mathbf{x})$ in $\mathcal{A}$, there exists a finite system of equations $S^*(\mathbf{y}, \mathbf{z})$ in $\mathcal{M}$ such that if $(\mathbf{b}, \mathbf{c})$ is a solution to $S^*(\mathbf{y}, \mathbf{z})$ in $\mathcal{M}$, then $\mathbf{b} \in D$ and $\phi(\mathbf{b})$ is a solution to $S(\mathbf{x})$ in $\mathcal{A}$. Moreover, any solution $\mathbf{a}$ to $S(\mathbf{x})$ in $\mathcal{A}$ arises in this way, i.e., $\mathbf{a} = \phi(\mathbf{b})$ for some solution $(\mathbf{b}, \mathbf{c})$ to $S^*(\mathbf{y}, \mathbf{z})$ in $\mathcal{M}$ for some $i = 1, \ldots, k$. Furthermore, there is a polynomial time algorithm that constructs the system $S^*(\mathbf{y}, \mathbf{z})$ when given a system $S(\mathbf{x})$.*

The proof of this result can be obtained by following step by step the proof of [13, Theorem 5.3.2], which states that an analogue of the above holds when $\mathcal{A}$ is interpretable by first-order formulas in $\mathcal{M}$. One needs to replace all first-order formulas by systems of equations.

Now we state two key consequences of Lemma 3.4.

Corollary 3.5. *If $\mathcal{A}$ is e-interpretable in $\mathcal{M}$, then $\mathcal{D}(\mathcal{A})$ is reducible to $\mathcal{D}(\mathcal{M})$. Consequently, if $\mathcal{D}(\mathcal{A})$ is undecidable, then $\mathcal{D}(\mathcal{M})$ is undecidable as well.*

Corollary 3.6. *E-interpretability is a transitive relation, i.e., if $\mathcal{A}_1$ is e-interpretable in $\mathcal{A}_2$, and $\mathcal{A}_2$ is e-interpretable in $\mathcal{A}_3$, then $\mathcal{A}_1$ is e-interpretable in $\mathcal{A}_3$.*

The following is a key property of e-interpretability that is used below.

Proposition 3.7 ([10]). *Let H be a normal subgroup of a group G. If H is e-definable in G (as a set), then the natural map $\pi\colon G \to G/H$ is an e-interpretation of G/H in G. Consequently, $\mathcal{D}(G/H)$ is reducible to $\mathcal{D}(G)$.*

3.2 The Diophantine problem in metabelian groups given by full rank presentations

We next discuss the Diophantine problem in metabelian groups admitting a full-rank presentation. We will need the following result regarding the same problem in nilpotent groups.

Theorem 3.8 ([11]). *Let G be a finitely generated nonabelian nilpotent group admitting a full rank presentation of deficiency at least* 2 *(i.e., there are at least two more generators than relations). Then the ring of integers $\mathbb{Z}$ is e-interpretable in G, and in particular, the Diophantine problem of G is undecidable.*

Next we recall the definition of (finite) verbal width. This notion is conveniently related to definability by equations, as we see in Proposition 3.9.

Let $w = w(x_1, \dots, x_m)$ be a word on an alphabet of variables and its inverses $\{x_1, \dots, x_m\}^{\pm 1}$. The *w-verbal subgroup* of a group G is defined as

$$w(G) = \langle w(g_1, \dots, g_m) \mid g_i \in G \rangle,$$

and G is said to have *finite w-width* if there exists an integer n such that every $g \in w(G)$ can be expressed as a product of at most n elements of the form $w(g_1, \dots, g_m)^{\pm 1}$. Hence, $w(G)$ is e-definable in G through the equation

$$x = \prod_{i=1}^{n} w(y_{i1}, \dots, y_{im}) w(z_{i1}, \dots, z_{im})^{-1}$$

on variables x and $\{y_{ij}, z_{ij} \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$.

Proposition 3.9. *Let G be a group, and let H be a normal verbal subgroup of G with finite verbal width. Then the quotient G/H is e-interpretable in G.*

Proof. By the argument above, the subgroup H is e-definable in G. Now the result follows from Proposition 3.7. □

Proof of Theorem 1.3. Let $G = \langle A \mid R \rangle_{\mathcal{M}}$ be a full rank presentation of a metabelian group G. To prove (1), note first that, since $\gamma_3(G) \geq [G', G']$, the 2-nilpotent quotient $G/\gamma_3(G)$ admits a presentation $\langle A \mid R \rangle_{\mathcal{N}_2}$ in the variety $\mathcal{N}_2$ of nilpotent groups of class at most 2. In particular, the group $G/\gamma_3(G)$ has a full-rank presentation of deficiency at least 2. By Theorem 3.8, the ring $\mathbb{Z}$ is e-interpretable in $G/\gamma_3(G)$. It is known that, in a finitely generated metabelian group, any verbal subgroup has finite width [25]; in particular, the subgroup $\gamma_3(G)$ has finite width in G. Hence, by Proposition 3.9, the group $G/\gamma_3(G)$ is e-interpretable in G. It follows from transitivity of e-interpretations that $\mathbb{Z}$ is e-interpretable in G, so the Diophantine problem in G is undecidable.

To prove the second statement of the theorem, observe that if $|R| \geq |A|$, then, by Theorem 1.1, the group G is virtually abelian. Hence, the Diophantine problem in G is decidable (see [7]). □

4 Random metabelian groups

In this section, we study random metabelian groups in the few-relators model. More precisely, we consider group presentations

$$G = \langle a_1, \dots, a_n \mid r_1, \dots, r_m \rangle_{\mathcal{M}} = \langle A \mid R \rangle_{\mathcal{M}}$$

in the variety of metabelian groups $\mathcal{M}$, where the set of generators $A=\{a_1,\dots,a_n\}$ is fixed, the number of relations m is also fixed, and R is a set of m words of length ℓ in the alphabet $A^{\pm 1}$ chosen randomly and uniformly, as explained in Section 1.3. We then study the asymptotic properties of G as ℓ tends to infinity.

As mentioned in the introduction, the key observation here is that, due to Theorem 1.6, a finite presentation in the variety of all groups (hence, any variety) has full rank asymptotically almost surely.

Theorem 4.1. *Let $n, m \in \mathbb{N}$, and let G be a finitely generated metabelian group given by a presentation $\langle A \mid R\rangle_{\mathcal{M}} = \langle a_1,\dots,a_n \mid r_1,\dots,r_m\rangle_{\mathcal{M}}$, where all relators r_i have length ℓ. Then the following holds asymptotically almost surely as $\ell \to \infty$: there exist two finitely generated subgroups H and K of G such that*

(1) *H is a free metabelian group of rank* $\max(|A|-|R|,0)$,

(2) *K is a virtually abelian group with $|R|$ generators, and its normal closure $L = K^G$ in G is again virtually abelian,*

(3) *$G = \langle H, K\rangle = LH$.*

Moreover, there is an algorithm that, given a presentation $G = \langle A \mid R\rangle_{\mathcal{M}}$, finds a free basis for the subgroup H and a generating set in $|R|$ generators for the subgroup K.

Proof. The result follows from Theorems 1.6 and 1.1. □

Theorem 4.2. *Let $n, m \in \mathbb{N}$, and let G be a finitely generated metabelian group given by a presentation $\langle A \mid R\rangle_{\mathcal{M}} = \langle a_1,\dots,a_n \mid r_1,\dots,r_m\rangle_{\mathcal{M}}$, where all relators r_i have length ℓ. Then the following hold asymptotically almost surely as $\ell \to \infty$.*

(1) *If $|R| \le |A| - 2$, then the ring of integers $\mathbb{Z}$ is interpretable in G by systems of equations, and the Diophantine problem in G is undecidable.*

(2) *If $|R| \ge |A|$, then the Diophantine problem of G is decidable (in fact, the first-order theory of G is decidable).*

Proof. The result follows from Theorems 1.6 and 1.3. □

Theorem 4.3. *Let $n, m \in \mathbb{N}$, and let G be a finitely generated metabelian group given by a presentation $\langle A \mid R\rangle_{\mathcal{M}} = \langle a_1,\dots,a_n \mid r_1,\dots,r_m\rangle_{\mathcal{M}}$, where all relators r_i have length ℓ. Assume $n \ge m-1$. Then the following holds asymptotically almost surely as $\ell \to \infty$: in any direct decomposition of G, all but one of the direct factors are virtually abelian.*

Proof. The result follows from Theorems 1.6 and 1.2. □

Acknowledgments. We are grateful to the anonymous referee who very carefully read this work and whose comments helped improve its presentation.

Bibliography

[1] G. N. Arzhantseva and A. Y. Ol'shanskiĭ, The class of groups all of whose subgroups with lesser number of generators are free is generic, *Math. Notes* **59** (1996), no. 4, 350–355.

[2] S. Burris and H. P. Sankappanavar, *A Course in Universal Algebra*, Grad. Texts in Math. 78, Springer, New York, 1981.

[3] C. Champetier, Propriétés statistiques des groupes de présentation finie, *Adv. Math.* **116** (1995), no. 2, 197–262.

[4] M. Cordes, M. Duchin, Y. Duong, M.-C. Ho and A. P. Sánchez, Random nilpotent groups I, *Int. Math. Res. Not. IMRN* **2018** (2018), no. 7, 1921–1953.

[5] M. Davis, H. Putnam and J. Robinson, The decision problem for exponential diophantine equations, *Ann. of Math. (2)* **74** (1961), 425–436.

[6] K. Delp, T. Dymarz and A. Schaffer-Cohen, A matrix model for random nilpotent groups, *Int. Math. Res. Not. IMRN* **2019** (2019), no. 1, 201–230.

[7] J. L. Eršov, Elementary group theories, *Dokl. Akad. Nauk SSSR* **203** (1972), 1240–1243.

[8] A. Garreta, A. Miasnikov and D. Ovchinnikov, Random nilpotent groups, polycyclic presentations, and Diophantine problems, *Groups Complex. Cryptol.* **9** (2017), no. 2, 99–115.

[9] A. Garreta, A. Miasnikov and D. Ovchinnikov, Diophantine problems in rings and algebras: Undecidability and reductions to rings of algebraic integers, preprint (2018), `https://arxiv.org/abs/1805.02573`.

[10] A. Garreta, A. Miasnikov and D. Ovchinnikov, Diophantine problems in solvable groups, *Bull. Math. Sci.* **10** (2020), no. 1, Article ID 2050005.

[11] A. Garreta, A. Miasnikov and D. Ovchinnikov, Full rank presentations and nilpotent groups: Structure, Diophantine problem, and genericity, *J. Algebra* **556** (2020), 1–34.

[12] M. Gromov, Hyperbolic groups, in: *Essays in Group Theory*, Math. Sci. Res. Inst. Publ. 8, Springer, New York (1987), 75–263.

[13] W. Hodges, *Model Theory*, Encyclopedia Math. Appl. 42, Cambridge University, Cambridge, 1993.

[14] I. Kapovich and P. Schupp, On group-theoretic models of randomness and genericity, *Groups Geom. Dyn.* **2** (2008), no. 3, 383–404.

[15] O. Kharlampovich, L. López and A. Myasnikov, The Diophantine problem in some metabelian groups, *Math. Comp.* **89** (2020), no. 325, 2507–2519.

[16] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer, Berlin, 1977.

[17] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*, Dover, Mineola, 2004.

[18] D. Marker, *Model Theory. An Introduction*, Grad. Texts in Math. 217, Springer, New York, 2002.

[19] J. V. Matijasevič, The Diophantineness of enumerable sets, *Dokl. Akad. Nauk SSSR* **191** (1970), 279–282.

[20] H. Neumann, *Varieties of Groups*, Springer, New York, 1967.

[21] Y. Ollivier, *A January 2005 Invitation to Random Groups*, Ensaios Mat. 10, Sociedade Brasileira de Matemática, Rio de Janeiro, 2005.

[22] A. Y. Ol'shanskii, Almost every group is hyperbolic, *Internat. J. Algebra Comput.* **2** (1992), no. 1, 1–17.

[23] N. S. Romanovskiĭ, Free subgroups of finitely-presented groups, *Algebra Logic* **16** (1977), no. 1, 62–68.

[24] D. Segal, *Polycyclic Groups*, Cambridge Tracts in Math. 82, Cambridge University, Cambridge, 1983.

[25] D. Segal, *Words: Notes on Verbal Width in Groups*, London Math. Soc. Lecture Note Ser. 361, Cambridge University, Cambridge, 2009.

[26] C. C. Sims, *Computation with Finitely Presented Groups*, Encyclopedia Math. Appl. 48, Cambridge University, Cambridge, 1994.

Received June 10, 2020; revised November 18, 2020.

Author information

Corresponding author:
Albert Garreta, Department of Mathematics,
University of the Basque Country, Leioa, Spain.
E-mail: garreta.a@gmail.com

Leire Legarreta, Department of Mathematics,
University of the Basque Country, Bilbao, Spain.
E-mail: leire.legarreta@ehu.eus

Alexei Miasnikov, Department of Mathematical Sciences,
Stevens Institute of Technology, Hoboken, NJ 07030, USA.
E-mail: amiasnikov@gmail.com

Denis Ovchinnikov, Department of Mathematical Sciences,
Stevens Institute of Technology, Hoboken, NJ 07030, USA.
E-mail: dovchinn@stevens.edu