6-2020

Model Theory of Groups and Monoids

Laura M. Lopez Cruz
The Graduate Center, City University of New York

Model Theory of Monoids and Groups

by

Laura López Cruz

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2020

This manuscript has been read and accepted by the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

Olga Kharlampovich

Date
Chair of Examining Committee

Ara Basmajian

Date
Executive Officer

Olga Kharlampovich
Ilya Kapovich
Vladimir Shpilrain
Supervisory Committee

The City University of New York

Abstract

Model Theory of Monoids and Groups

by

Laura López Cruz

Advisor: Olga Kharlampovich

We first show that arithmetic is bi-interpretable (with parameters) with the free monoid and with partially commutative monoids with trivial center. This bi-interpretability implies that these monoids have the QFA property and that finitely generated submonoids of these monoids are definable. Moreover, we show that any recursively enumerable language in a finite alphabet X with two or more generators is definable in the free monoid. We also show that for metabelian Baumslag-Solitar groups and for a family of metabelian restricted wreath products of the form $A \wr \mathbb{Z}$, the Diophantine Problem is decidable. That is, we provide an algorithm that decides whether or not a given system of equations in these groups has a solution.

Acknowledgements

I would like to thank Olga Kharlampovich for her mentorship and support these past five years. It was a pleasure working with a brilliant and inspiring mathematician. I would like to thank my friends and colleagues Chris and Dan for sharing their ideas and most importantly, for their unconditional friendship.

Contents

Chapter 1

Introduction

The first-order theory of an algebraic structure can reveal many of its intrinsic properties. For instance, knowing the definable sets of a group can give you insight into the structure of its automorphism group, since automorphisms preserve definable sets. If a theory has quantifier elimination to quantifier-free formulas, then any model of the theory has the property that all of its substructures are elementarily equivalent to it and therefore, they share many first-order properties.

It is therefore useful to study which sets and properties are definable in the theory of an algebraic structure. Many algebraic properties can be described using the language of first-order logic. For instance, in the language of groups, being nilpotent, abelian, finite, and torsion-free are all first-order definable. One can also define the center, the centralizer of finite subsets (with constants), and the set of all commutators of a group. However, there is no way to express that a subgroup, or the group itself, is finitely generated. Moreover, the definability of certain properties depends on the structure. The rank of a finitely generated abelian group is definable, yet it is not definable in the theory of a free group. The set of bases is definable for the free group F_2, but it is not definable for F_n when $n > 2$ [KM13].

For a given structure $\mathcal{G}$, one can also ask whether the theory of $\mathcal{G}$, $Th(\mathcal{G})$, (with or without constants), is decidable. That is, is there an algorithm that, given a sentence in the language of the structure, can determine whether or not the sentence belongs to $Th(\mathcal{G})$? There are many examples of decidable and undecidable theories, as we will see below. Interestingly, algebraic structures with undecidable theory tend to share many other first-order properties, and the same is true for structures with decidable theory. For instance, groups with decidable theory are usually stable, do not have many definable sets, and the theory is not rigid (it does not classify the structure up to isomorphism). Structures with undecidable theory typically are rich in definable sets and the theory is QFA.

Mathematicians are also interested in the decidability of the positive existential theory of a structure. This is the subset of the first-order theory (with constants) consisting of sentences of the form $\exists x_1, \dots x_n\, t(x_1, \dots, x_n) = s(x_1, \dots, x_n)$, where $t(x_1, \dots, x_n)$ and $s(x_1, \dots, x_n)$ are terms in the language of the structure. The decidability of the positive existential theory of an algebraic structure $\mathcal{G}$ is equivalent to the decidability of the Diophantine problem for $\mathcal{G}$ (also called Generalized Hilbert's tenth problem); that is, is there an algorithm to determine if a given finite system of equations has a solution? For those structures with decidable Diophantine problem, one can also ask to describe the sets of solutions of the system.

The original version of Hilbert's tenth problem was the Diophantine problem for the ring of integers, $\mathbb{Z}$. The first steps towards solving the problem were taken by Davis, Putnam, and Robinson [Dav96], who showed that recursively enumerable sets can be represented in exponential Diophantine form; that is, for a recursively enumerable set $W \subseteq \mathbb{N}$, there is an expression P such that

$$x \in W \longleftrightarrow \exists x_1, \ldots, x_n \, P(x, x_1, \ldots, x_n, 2^{x_1}, \ldots, 2^{x_n}) = 0,$$

where $x_1, \ldots, x_n$ range through $\mathbb{N}$.

Building on their work, Matisyasevich proved in 1970 [Mat71b] that the relation $\{(x, y) | y = 2^x\}$ is Diophantine, and thus one can define recursively enumerable sets with polynomials. That is, for a recursively enumerable set

W, there is a polynomial P such that

$$x \in W \longleftrightarrow \exists x_1, \dots, x_n \, P(x, x_1, \dots, x_n) = 0,$$

This result, and the fact that some recursively enumerable sets are not recursive (for instance, the halting problem), implied the undecidability of Peano arithmetic and in particular, of Hilbert's tenth problem.

In this thesis, the structures we study are monoids and groups. Below, we mention some results on the model theory of these structures.

1.1 Arithmetic and "rich" structures

In 1925, Kurt Gödel showed that the theory of the ring of natural numbers, Peano arithmetic (PA), is incomplete. Implicit in his proof was the fact that PA is undecidable; that is, there is no algorithm that can decide whether a sentence in the language of rings is true or not about the natural numbers. PA has been studied thoroughly and a lot is known about its models. In this thesis, we will focus on the standard model of PA, which we will often refer to as arithmetic and denote by $\mathbb{N}$.

An interesting question to ask is whether an algebraic structure shares first-order properties with arithmetic. The ring of natural numbers is a "rich" structure, in the sense that it has many definable subsets. Yuri Matisyasevich proved in [Mat71a] that all recursively enumerable sets in the ring of natural numbers are Diophantine and therefore, definable. In fact, the first order theory of the natural numbers has the expressive power of its weak second order theory, in which you can quantify over finite subsets. Moreover, arithmetic is quasi-finitely axiomatizable (QFA), so a single first-order sentence in the language of ring theory characterizes the structure up to isomorphism (in the class of finitely generated structures). Thus, while the first order theory of arithmetic is undecidable, it captures a lot of information about $\mathbb{N}$.

The ring of integers, denoted by $\mathbb{Z}$, is also a "rich" structure. In 1770, Lagrange proved the Four Squares Theorem, which says that any natural number is the sum of the squares of four integers. It follows from this result that $\mathbb{N}$ is definable in $\mathbb{Z}$. Since $\mathbb{N}$ is a definable subset of $\mathbb{Z}$, it is certainly interpretable in $\mathbb{Z}$. It follows from this and Matisyasevich's result [Mat71b] that the two rings are in fact bi-interpretable and therefore in a sense, logically equivalent.

Structures that are bi-interpretable with arithmetic also have the QFA property [Nie07] and the property that recursively enumerable sets are definable. These structures are also prime, homogeneous, and have undecidable, non-stable first order theory. Moreover, if two structures are bi-interpretable without parameters (or with parameter sets C, D, respectively) then their groups of automorphisms (or groups of automorphisms fixing C, D, respectively, pointwise) are isomorphic [Mar06]. Thus, constructing a bi-interpretation between a structure $\mathcal{G}$ and arithmetic is a useful tool to study the elementary theory of $\mathcal{G}$.

In 1946, Quine proved that the free non-abelian semigroup of rank $m \geq 2$ is bi-interpretable (with constants) with arithmetic [Qui46]. It follows from this that the first order theory (with constants) of the free semigroup is undecidable. In Section 2.3.2 , we give an alternate proof of this result by constructing a bi-interpretation of the free monoid with the list superstructure $S(\mathbb{N}, \mathbb{N})$ of $\mathbb{N}$. This structure is known to be bi-interpretable with $\mathbb{N}$ and its first-order theory has the expressive power of the weak second order theory of $\mathbb{N}$ (see for example [RR67], [Coo17]). We also show that the rank of the free monoid is definable, and moreover, we show that non-trivial free partially commutative monoids with trivial center are also bi-interpretable (with the standard generating set as parameters) with arithmetic. It was proven by Dumev [Dur73], [Dur95] and Marchenkov [Mar82] that the $\forall\exists$-theory of the free semigroup is also undecidable.

The free monoid behaves differently to arithmetic when it comes to equations. The study of equations in the free semigroup began with Markov in the 60s, who conjectured that the problem of solvability of equations in the free semigroup might be reduced to Hilbert's Tenth Problem. Later, his student Hmelevskii [Hme71] disproved his conjecture and constructed an algorithm to solve equations in three unknowns and moreover, to solve systems of equations, each of which contains at most two variables. Makanin proved in [Mak77] the decidability of finite a system of arbitrary equations in the free semigroup, which he showed reduces to the decidability of a single equation. In general, the decidability of a single equation and the decidability of a system of equations are two fundamentally different problems. For instance, single equations are decidable in the Heisenberg group, whereas systems of equations are undecidable [DLS15].

1.2 Non-abelian free groups

In contrast, the free non-abelian group is not a "rich" structure. In fact, it exhibits almost the opposite behavior of the free monoid. The only definable subgroups are cyclic subgroups, which are defined as the centralizers of elements of the group. Proper verbal subgroups have infinite width and therefore are not definable [KM13]. Moreover, primitive elements are not definable for a free group of rank $m > 2$.

In 1945, Tarski conjectured two propositions about free groups, which were formalized as follows:

1. Any two non-abelian free groups are elementarily equivalent, regardless of their rank.

2. The theory of all non-abelian free groups is decidable.

Tarski was never explicit about the origin of these conjectures, but it's believed that they originated from two observations of the free group. The first is that many properties of the free group, in particular the description of its elements, are independent of the rank of the group. For instance, all elements have infinite order, and the only abelian subgroups are infinite cyclic subgroups. The second follows from the Reidemeister-Schreier process, and it's the fact that F_m can be embedded into F_n for any $m, n \geq 2$, $m < n$, and additionally, $F_\omega \leq F_m \leq F_\omega$ for any m, where F_ω is the free group of countably infinite rank.

The first steps towards proving these conjectures was due to Vaught, who was a student of Tarski's. He showed that the conjectures are true for free groups of infinte rank by using what is now known as the Taski-Vaught test. The next significant progress was due to Merzljakov [Mer66], who proved that all free groups have the same positive theory. In his proof, Merzljakov proved quantifier elimination arbitrary positive formula to boolean combinations of universal formulas, and these techniques served as a precursor to the eventual proofs of Tarski's conjectures.

The observation that all free groups are universally equivalent made it clear that the solution to Tarki's conjectures would involve the study of universally free groups. In the work of Gaglione and Spellman [GS93], Remenkislov [Rem89], and Chriswell [Chi76], it was shown that these are precisely the finitely generated fully residually free groups (later called limit groups by Sela [Sel01]. These include orientable surface groups of genus $g \geq 2$ and non-orientable surface groups of genus $g \geq 4$.

The solution to these problems, which came around 2006, involved the development of the theory of these fully residually free groups, along with Makanin-Razborov techniques for solving equations in free groups, and algebraic geometry over free groups (which Sela called Diophantine geometry). The first two conjectures were proven by Kharlampovich and Myasnikov [KM06], and independently by Sela [Sel09]. In their paper, Kharlampovich and Myasnikov also proved the second conjecture: that the first-order theory of the free group (with constants) is decidable.

The study of the Diophantine problem for the free group was integral in the solution to Tarski's conjectures. Lyndon provided one of the first results in [Lyn60a], [Lyn60b], where he showed the decidability of equations over free groups in one variable. Moreover, he provided a description of the solutions, which he showed can be defined by a finite system of what he called "parametric words". Lorents [Lor68] later extended this result to systems of equations in one variable. Chriswell and Remeslennikov [CR00] gave a description of solution sets of these systems as the set of homomorphisms from the coordinate group of irreducible algebraic sets to a free group. Following the work of Hmelevskii, Yu Ozhigov [Ozh83] showed the decidability of the Diophantine problem for systems of equations in two variables and provided a description of the solutions.

Malcev [Mal62] described the solution set of the equation $zxyx^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ using the group of automorphisms of the coordinate group of equations and minimal solutions. Makanin had a major breakthrough in the 1980s, when he proved the decidability of arbitrary systems of equations over free groups [Mak83]. He created the Makanin process, an extremely useful technique for working with equations in the free group. Based on Makanin's algorithm, Razborov [81] provided a description of the sets of solutions to systems of equations in free groups via what is now called Makanin-Razaborov diagrams. Kharlampovich and Miasnikov [KM96], [KM98] described solutions in terms of NTQ groups. Later, Kharlampovich, Lysenokov, Myasnikov and Touikan [Kha+10] showed that solving quadratic equations over free groups is NP-complete.

Most of the results for free groups are true for all torsion-free hyperbolic groups. The elementary theory is decidable, stable [Sel13], and there is effective quantifier elimination to $\forall\exists$-formulas. Cyclic subgroups are the only definable subgroups. Sela [Sel09] provided an algorithm to determine whether two torsion-free hyperbolic groups are elementarily equivalent, and moreover, showed that hyperbolicity is a first-order invariant.

In some sense, the theory of the free group does not "say" much about the free group. Unlike the free monoid, one cannot define the rank of a free group with a first-order sentence, and more so, one cannot distinguish a free group from certain surface groups. Thus, the "freeness" of the group is not captured in the first-order theory. However, the theory is decidable, complete, stable, and has quantifier elimination. This give and take is very common in the model theory of algebraic structures.

1.3 Solvable groups

Free solvable groups exhibit a different behavior from free groups. Rogers, Smith, and Solitar showed in [RSS86] that free solvable groups of different finite ranks have different $\forall\exists\forall$-theories, and therefore are not elementarily equivalent. In fact, they show that the class of free solvable groups is first-order rigid; that is, two free solvable groups are elementarily equivalent if and only if they are isomorphic. The same is true for free nilpotent groups and free abelian groups of finite rank, and for partially commutative metabelian groups [GT09]. Oger [Oge91] showed that two finitely generated nilpotent groups G and H are elementarily equivalent if and only if $G \times \mathbb{Z} \cong H \times \mathbb{Z}$.

Abelian groups behave quite nicely. The elementary theory is decidable; this follows from Szmielew's results [Szm55], where she determined invariants that characterize abelian groups up to elementary equivalence. The theory has quantifier elimination to positive primitive formulas; this quantifier elimination is effective if the group has decidable index problem. The theory is stable, and the definable subsets are boolean combinations of cosets of normal subgroups.

Another interesting class of solvable groups, whose behavior is closer to that of arithmetic, is the class of metabelian Baumslag-Solitar groups. These groups have the presentation $B(1,n) = \langle a, b | a^{-1}ba = b^n \rangle$. When $n = 1$, the group $B(1,1) \cong \mathbb{Z}^2$. It was shown by Khelif [Khe07] that for $n \geq 2$, these groups are bi-interpretable (with constants) with arithmetic. Therefore, the theory of $B(1,n)$ (with constants) is undecidable, yet rich in definable subsets. A finitely generated group is elementarily equivalent to $B(1,n)$ if and only if it is isomorphic to $B(1,n)$. This result follows from the work of Nies [Nie07] and Khelif [Khe07], who showed that metabelian Baumslag-

Solitar groups have the QFA property. Moreover, a recent result [KM19] shows that the first-order theory of any one-relator group containing a solvable Baumslag-Solitar subgroup is undecidable because the subgroup is interpretable in the group.

Denote by $\mathcal{EP}_1$ the problem of solvability of one equation. Roman'kov showed that $\mathcal{EP}_1$ is undecidable even for the subclass of all split equations of the form $w(x_1, \ldots, x_n) = g$, where $w(x_1, \ldots, x_n)$ is a coefficient-free word and g is an element of the underlying group G that is a free nilpotent of class ≥ 9 [Rom77] (this bound was later reduced to ≥ 4 in [Rom79]) or G is a free metabelian non-abelian group [Rom79]. In [DLS15] the authors proved that $\mathcal{EP}_1$ is decidable in the Heisenberg group that is free nilpotent of rank 2 and class 2. But the Diophantine problem (denoted by $\mathcal{EP}$ in [DLS15]) is undecidable in any non-abelian free nilpotent group. Moreover, in a finitely generated metabelian group G given by a finite presentation in the variety $\mathcal{M}_2$ of metabelian groups, the Diophantine problem is undecidable asymptotically almost surely if the deficiency of the presentation is at least 2 [GMO16].

Noskov [Nos84] showed that the first-order theory of a finitely generated solvable group is decidable if and only if the group is virtually abelian. Since virtually abelian solvable groups have decidable first-order theory, the Diophantine problem is decidable. For non-virtually abelian solvable groups, the situation is different. In a recent result of Garreta, Miasnikov, and Ochvikinov [GMO18], it was shown that for a finitely generated non-virtually abelian nilpotent group G, there is a ring of algebraic integers $\mathcal{O}$ that is e-interpretable (interpretable by equations) in G, and so it follows that the Diophantine problem in G reduces to that of $\mathcal{O}$. There is a longstanding conjecture in number theory that the ring $\mathbb{Z}$ is Diophantine in any ring of algebraic integers $\mathcal{O}$, and therefore, the Diophantine problem in $\mathcal{O}$ is undecidable.

For any group G and any $i \geq 2$, the quotient $G/\gamma_i(G)$ is a nilpotent group. For a finitely generated metabelian group G, $\gamma_3(G)$ has finite width and is therefore definable in G. Therefore, the quotient $G/\gamma_3(G)$ is interpretable in G. If $G/\gamma_3(G)$ is non virtually abelian, then it follows from the previous result that one can interpret a ring of integers, and assuming the conjecture to be true, the Diophantine problem in $G/\gamma_3(G)$ is undecidable. This result can then be carried over to G by transitivity of e-interpretability.

The discussion above shows that finitely generated metabelian groups G with virtually abelian quotients $G/\gamma_3(G)$ present an especially interesting case in the study of equations in metabelian groups. The groups $BS(1,k)$ and wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group and $\mathbb{Z}$ is an infinite cyclic group, are the typical examples of such groups. In Chapter 3, we show that equations in these groups are decidable, and thus we provide first examples of non-virtually abelian finitely generated metabelian groups with decidable Diophantine problem.

1.4 One relator groups and monoids

One relator groups often appear in combinatorial and geometric group theory and have been studied extensively. They also come up in topology as the fundamental groups of surfaces. In 1931, Magnus [Mag30] showed that all one relator groups can be broken down into the Magnus hierarchy. He later provided an algorithm to solve the word problem in one relator groups [Mag32].

An interesting class of one-relator groups is the class of Baumslag-Solitar groups $B(m,n) = \langle a, b | a^{-1}b^m a = b^n \rangle$. When $m \neq 1$, these groups are not metabelian. These groups were introduced in [BS62] by Baumslag and Solitar as the first examples of one-relator non-Hopfian groups and have since then been found to have many remarkable properties. Moldavanski classified Baumslag-Solitar groups up to existential and elementary theory [Mol91]. Adding to Moldavanski's work, Casals-Ruiz and Kazachkov showed in [CK12] that for the groups $BS(m,n)$ and $BS(l,k)$, the following properties are equivalent:

1. either $k = \pm m$ and $l = \pm n$ or $k = \pm n$ and $l = \pm m$
2. $BS(m, n)$ and $BS(l, k)$ are elementarily equivalent
3. $BS(m, n)$ and $BS(l, k)$ are isomorphic

In a recent result of Garreta and Grey [GG19], they provide a family of one relator monoids with decidable Diophantine problem.

1.5 Outline of results

Our main theorem in Chapter 2 is the following:

Theorem 3. *1. The list superstructure of* $\mathbb{N}$, $S(\mathbb{N}, \mathbb{N})$, *and the free monoid,* $\mathbb{M}_X$, *are bi-interpretable with parameters in* X *uniformly in* X.

2. If a non-trivial partially commutative monoid A_Γ *has trivial center, then* $S(\mathbb{N}, \mathbb{N})$ *and* A_Γ *are bi-interpretable with the standard generating set (vertices* V *of* Γ*) as parameters.*

Since $S(\mathbb{N}, \mathbb{N})$ and $\mathbb{N}$ are bi-interpretable without parameters, it immediately follows that $\mathbb{M}_X$ and A_Γ are bi-interpretable with parameters with $\mathbb{N}$ (Corollary 4).

Moreover, in Chapter 2 we provide a family of one-relator monoids in which $\mathbb{N}$ is interpretable. These results give us interesting corollaries. For instance, the monoids in which one can interpret $\mathbb{N}$ have undecidable first-order theory. We also show that any structure $\mathcal{G}$ that is bi-interpretable with arithmetic is bi-interpretable with its list superstructure, $S(\mathcal{G}, \mathbb{N})$. Moreover, we show that for the free monoid and partially commutative monoids with trivial center and for any $k \in \mathbb{N}$, there exists a single formula that defines finitely generated submonoids with k generators. Finally, we show that these monoids do not have quantifier elimination to boolean combinations of Σ_n and Π_n formulas for any n. These results are published in [KL19].

In Chapter 3, we prove the following:

Theorem 8. *The Diophantine Problem in $BS(1,k)$ is decidable.*

Theorem 11. *The Diophantine problem is decidable in $A \wr \mathbb{Z}$, where A is a finitely generated abelian group.*

We use techniques from linear algebra to reduce most of the systems to linear systems of equations and provide two partial algorithms, one which halts if there is a solution to the system and one which halts if there is no solution. These results can be found in our article [KLM19] which has recently been accepted in Mathematics of Computation.

Chapter 2

Arithmetic and the free monoid

2.1 Arithmetic and bi-interpretability

Let $\mathcal{B} = \langle B; \mathcal{L}(\mathcal{B})\rangle$ be an algebraic structure. A subset $A \subseteq B^n$ is said to be *definable* in $\mathcal{B}$ if there is a formula $\phi(x_1, \ldots, x_n)$ in $\mathcal{L}(\mathcal{B})$ such that $A = \{(b_1, \ldots, b_n) \in B^n \mid \mathcal{B} \models \phi(b_1, \ldots, b_n)\}$. For example, in any group one can define the center of the group with the formula $\phi(x) : \forall y(xy = yx)$.

A property of a structure is said to be *definable* if there is a sentence that describes that property. For instance, the property of being abelian can be defined by the sentence $\psi : \forall x \forall y(xy = yx)$. When we say that a subset (or a property) is *definable with parameters* $b_1, \cdots, b_n$, this means that the defining formula (or sentence) is a formula containing the constants $b_1, \cdots, b_n$ from the domain of $\mathcal{B}$. For example, the centralizer of an element g in a group G can be defined by the formula $\phi(y) : \forall y(gy = yg)$.

In general, it is a difficult problem to find which properties and subsets of a structure are definable. More often than not, one cannot simply construct a defining first-order formula, but merely prove one exists. If one is lucky enough, one can show that the structure is similar (or equivalent) to a structure whose first-order theory has been thoroughly studied and understood. An example of such a theory is Peano arithmetic. In the first part of this thesis, we show that the free monoid and partially commutative monoids with trivial center are similar to arithmetic.

Below, we will discuss interpretability and bi-interpretability, which are central to our study of the first-order theory of monoids. Moreover, we will discuss some model-theoretic properties of arithmetic that are passed down to structures that are bi-interpretable with $\mathbb{N}$.

2.1.1 Bi-interpretability

Definition 1. *Let $\mathcal{A} = \langle A, f, \ldots, R, \ldots, c, \ldots \rangle$ be an algebraic structure, where f, P, and c stand for functions, predicates, and constants. We say $\mathcal{A}$ is* ***interpretable*** *in another structure $\mathcal{B}$ if there is:*

- *a definable subset $A^* \subseteq B^n$*
- *an equivalence relation $\sim$ on A^*, definable in $\mathcal{B}$*

- *functions $f^*, \ldots$, relations $R^*, \ldots$, and constants $c^*, \ldots$ on the set $A^*/\sim$, all definable in $\mathcal{B}$*

such that the structure $\mathcal{A}^* = \langle A^*/\sim, f^*, \ldots, R^*, \ldots, c^*, \ldots \rangle$ is isomorphic to $\mathcal{A}$.

We say $\mathcal{A}$ is interpretable in $\mathcal{B}$ with parameters $b_1, \ldots, b_n \in B$ if the defining formulas used in the interpretation contain these constants. If the interpretation is without parameters, we say $\mathcal{A}$ is $\emptyset$-interpretable in $\mathcal{B}$. The interpretation of $\mathcal{A}$ in a class of structures $\mathscr{C}$ is said to be *uniform* if the formulas that interpret $\mathcal{A}$ in a structure $\mathcal{B}$ are the same for every structure $\mathcal{B} \in \mathscr{C}$. *Uniform interpretability with parameters* in a class $\mathscr{C}$ means that the formulas that interpret $\mathcal{A}$ in a structure $\mathcal{B}$ are the same for every structure $\mathcal{B} \in \mathscr{C}$ and the parameters in each such $\mathcal{B}$ come from subsets uniformly definable in $\mathscr{C}$.

If $\mathcal{A}$ is interpretable in $\mathcal{B}$, then in a sense, there is a copy of the structure $\mathcal{A}$ lying inside of $\mathcal{B}$. It is natural to conclude that all of the information (first-order properties, definable sets, etc.) in $Th(\mathcal{A})$ will be contained in $Th(\mathcal{B})$. The following lemma, which is a principle result on interpretability, says just that.

Lemma 1. *[Hod93] If $\mathcal{A}$ is interpretable in $\mathcal{B}$ with parameters $c_1, \ldots, c_n$,* *then for every formula $\psi(\bar{x})$ of $\mathcal{L}(\mathcal{A})$, one can effectively construct a formula $\psi^*(\bar{z}, c_1, \cdots, c_n)$ of $\mathcal{L}(\mathcal{B})$ such that for any $\bar{a} \in \mathcal{A}$, one has that $\mathcal{A} \models \psi(\bar{a})$ if and only if $\mathcal{B} \models [\psi(\bar{a})]^*$.*

Here, $[\psi(\bar{a})]^*$ denotes the interpretation of the formula $\psi(\bar{a})$. That is, the constants $a_1, \ldots, a_n$ in $\psi(\bar{x})$ are replaced by their interpretation in $\mathcal{B}$ along with any predicates, functions, and constants.

Lemma 1 shows that interpretability has many interesting applications.

Corollary 1. *Suppose $\mathcal{A}$ is $\emptyset$-interpretable in $\mathcal{B}$. If $Th(\mathcal{A})$ is undecidable, then $Th(\mathcal{B})$ is undecidable.*

Corollary 2. *[Ers+65] If $\mathbb{N}$ is interpretable in $\mathcal{B}$ (possibly with parameters) then $Th(\mathcal{B})$ is undecidable.*

Note that Corollary 2 is stronger than Corollary 1 since it is not required that $\mathbb{N}$ is interpretable in $\mathcal{B}$ without parameters.

If $\mathcal{A}$ is interpretable in $\mathcal{B}$ and $\mathcal{B}$ is interpretable in $\mathcal{A}$, we say that $\mathcal{A}$ and $\mathcal{B}$ are mutually interpretable. We now define the notion of bi-interpretability.

Definition 2. *Two algebraic structures $\mathcal{A}$ and $\mathcal{B}$ are said to be **bi-interpretable** if they satisfy the following conditions:*

- *$\mathcal{B}$ is interpretable in $\mathcal{A}$ as $\mathcal{B}^*$, $\mathcal{A}$ is interpretable in $\mathcal{B}$ as $\mathcal{A}^*$, which* *by transitivity implies that $\mathcal{A}$ is interpretable in itself as $\mathcal{A}^{**}$ and $\mathcal{B}$ in itself as $\mathcal{B}^{**}$.*

- *There is an isomorphism $\mathcal{A} \to \mathcal{A}^{**}$ definable in $\mathcal{A}$ and an isomorphism $\mathcal{B} \to \mathcal{B}^{**}$ definable in $\mathcal{B}$.*

If the defining formulas in the interpretation use parameters, we say $\mathcal{A}$ and $\mathcal{B}$ are bi-interpretable with parameters. Otherwise, we say $\mathcal{A}$ and $\mathcal{B}$ are $\emptyset$-bi-interpretable.

Note that bi-interpretability is a much stronger notion than mutual interpretability. The additional requirement that the isomorphisms $\mathcal{A} \to \mathcal{A}^{**}$ and $\mathcal{B} \to \mathcal{B}^{**}$ are definable suggests that in a sense, the interpretations $\mathcal{A}^*$ and $\mathcal{B}^*$ are reasonable and that the structures themselves can encode and decode them. There are examples of structures that are mutually interpretable but not bi-interpretable. For example, the Heisenberg group $UT_3(\mathbb{Z})$ of 3×3 unitriangular matrices with entries in $\mathbb{Z}$ is mutually interpretable with arithmetic [Mal60], but the two structures are not bi-interpretable [Khe07].

Lemma 1 also implies that structures that are bi-interpretable have essentially the same definable sets and maps. When two structures are bi-interpretable (or bi-interpretable with parameters), then their automorphism groups (or group of automorphisms fixing the parameters pointwise), are the same. Morevoer, many first-order properties, like stability, homogeneity, and finite axiomatization are preserved (we will define some of these terms later in the text). Thus, bi-interpretability can be seen as an equivalence relation between two structures of possibly different signatures.

2.1.2 Arithmetic

The ring of natural numbers, $\mathbb{N}$, has signature $\mathbb{N} = \langle N, +, \cdot, 0, 1\rangle$ and its theory is called Peano arithmetic. Kurt Gödel showed in 1925 that Peano arithmetic is incomplete; that is, there are theorems about the natural numbers that are not provable from the five postulates that axiomatize the theory. This, together with some results about computability, implied that the theory is also undecidable.

Nevertheless, arithmetic has many "good" properties. For instance, it is quasi-finitely axiomatizable. This means that, within the class of finitely generated structures, there is a single first-order sentence that can characterize $\mathbb{N}$ up to isomorphism.

Definition 3. *An infinite finitely generated structure $\mathcal{G}$ is* ***quasi-finitely axiomatizable*** *(QFA) if there is a first-order sentence $\phi \in \mathcal{L}(\mathcal{G})$ such that*

- $\mathcal{G} \models \phi$

- *if $\mathcal{H}$ is a finitely generated structure with the same signature as $\mathcal{G}$ and $\mathcal{H} \models \phi$, then $\mathcal{H} \cong \mathcal{G}$.*

There are many examples of QFA structures. For instance, the restricted wreath products $\mathbb{Z}_p \wr \mathbb{Z}$, with p prime, $UT_3(\mathbb{Z})$, and the subgroup of the group of permutations of $\mathbb{Z}$ generated by the successor function and transpositions, are all QFA groups. In fact, Nies [Nie07] showed that any structure that is bi-interpretable (possibly with parameters) with arithmetic is also QFA. Khelif [Khe07] showed that metabelian Baumslag-Solitar groups $B(1,n) = \langle a^{-1}ba = b^n \rangle$, with $n \geq 2$, are bi-interpretable with arithmetic and therefore QFA. He also showed that any free metabelian group of finite rank $n \geq 2$ is QFA.

A set $K \in \mathbb{N}$ is *recursive* if there is a recursive function $f : K \to \{0, 1\}$ such that $n \in K$ if and only if $f(n) = 1$. A set $K \subseteq \mathbb{N}$ is *recursively enumerable* if it is the range of a total recursive function. Matisyasevich [Mat71a] proved that recursively enumerable sets are definable in $\mathbb{N}$. In particular, he proved the following:

Proposition 1. *For any recursively enumerable set $R \subseteq \mathbb{N}^m$, there is a polynomial $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$ such that the equation $P(x_1, \ldots, x_n, a_1, \ldots, a_m) = 0$ has a solution if and only if $(a_1, \ldots, a_m) \in R$.*

This implies that any recursively enumerable set of natural numbers can be defined by a first order formula of the form $\phi(\bar{y}) : \exists x_1, \ldots, x_n \, P(\bar{x}, \bar{y}) = 0$. Sets satisfying this property are said to be Diophantine. The definable subsets of arithmetic defined by these existential formulas are therefore the recursively enumerable sets; these are also referred to as arithmetical sets.

Moreover, $\mathbb{N}$ is a prime model of Peano arithmetic. A structure $\mathcal{G}$ is *prime* if for any structure $\mathcal{H}$ such that $Th(\mathcal{G}) = Th(\mathcal{H})$, $\mathcal{G}$ elementary embeds into $\mathcal{H}$. If a theory has a prime model, then it is unique up to isomorphism. This property is also preserved under bi-interpretability.

Remark 1. *A structure $\mathcal{G}$ is prime if and only if the orbit of each tuple under the action of $Aut(\mathcal{G})$ is definable without parameters.*

2.1.3 The list superstructure of $\mathbb{N}$

Let $\mathcal{B}$ be an algebraic structure. The three-sorted structure $S(\mathcal{B}, \mathbb{N})$, termed the *list superstructure over* $\mathcal{B}$, is defined as

$$S(\mathcal{B}, \mathbb{N}) = \langle \mathcal{B}, S(B), \mathbb{N}, t(s, i, a), l(s), \frown, \in \rangle, \tag{2.1}$$

where $\mathbb{N} = \langle N; +, \cdot, 0, 1 \rangle$ is the standard arithmetic, $S(B)$ is the set of all finite sequences (tuples) of elements of B, $l : S(B) \to N$ is the length function which takes a sequence $s = (s_1, \ldots, s_n)$ to its length, n, and $t(x, y, z)$

is a predicate on $S(B) \times N \times B$ such that $t(s, i, a)$ holds in $S(\mathcal{B}, \mathbb{N})$ if and only if $s = (s_1, \ldots, s_n) \in S(B), i \in N, 1 \leq i \leq n$, and $a = s_i \in B$. This structure has the same expressive power as the weak second order theory of $\mathcal{B}$. In the weak second order logic, one can quantify not only over elements of the domain, but over finite subsets.

The list superstructure of $\mathbb{N}$ is denoted by $S(\mathbb{N}, \mathbb{N})$. The following Lemma is based on two facts: the first one is that there are effective codings of the set of all tuples of natural numbers such that the natural operations over the tuples are computable on their codes (see [Coo17], [RR67]); and the second is Matisyasevich's result that all computably enumerable predicates over natural numbers are $\emptyset$-definable in $\mathbb{N}$.

Lemma 2. *The list superstructure* $S(\mathbb{N}, \mathbb{N})$ *is* $\emptyset$*-interpretable in* $\mathbb{N}$*. Moreover,* $S(\mathbb{N}, \mathbb{N})$ *and* $\mathbb{N}$ *are bi-interpretable without parameters.*

Lemma 2 implies that Peano arithmetic contains the expressive power of the weak second order theory of $\mathbb{N}$. We will see in Section 2.3.2 that $\mathbb{M}_X$ also has this property as a consequence of bi-interpretability.

The result that $\mathbb{N}$ and $\mathbb{M}_X$ are bi-interpretable follows from Section 4 of Quine's paper [Qui46]. He showed that the structure $\langle N, +, \cdot, \uparrow, 0, 1\rangle$ is bi-interpretable with $\mathcal{C} = \langle C, \frown\rangle$ with two parameters from C. The first structure is the same as $\mathbb{N}$, with the additional predicate $x \uparrow y$, which means x^y. Since the predicate $z = x^y$ is computable and therefore definable in terms of addition and multiplication (see, for example, [Mat71a]) it can be removed from the signature. The second is a model of concatenation theory; C is the set of words on a finite generating set (with at least two elements) and $\frown$ is the concatenation operation. The free monoid and $\mathcal{C}$ are equivalent structures.

2.2 Interpretation of $\mathbb{N}$ in some classes of monoids

The signature of a monoid is $\langle \cdot, \emptyset \rangle$, where $\cdot$ is the multiplication operation and $\emptyset$ is the identity element. (The identity element is definable, thus it can be removed from the signature). We will use Quine's method from [Qui46], Section 3, to interpret $\mathbb{N} = \langle N, +, \cdot, 0, 1 \rangle$ in $\mathbb{M}_X = \langle M_X, \cdot, \emptyset \rangle$ and some other monoids with parameters.

Let G be a monoid containing elements x_1, x_2 and S be the set of non-trivial elements of G that can be represented by subwords of words in the set

$$\bar{S} = \{x_1^{i_1} x_2^{j_1} \cdots x_1^{i_k} x_2^{j_k} \ | i_1, \ldots, i_k \in \mathbb{N} - \{0\}, j_1, \ldots, j_k \in \{1, 2\}\}.$$

Lemma 3. $\mathbb{N}$ *is interpretable in any monoid* G *that contains two elements*

x_1 and x_2 such that

1. *x_1 generates a free cyclic submonoid $\langle x_1 \rangle$ that is definable;*

2. *S is definable;*

3. *Distinct words in $\bar{S}$ represent distinct elements. Let $\bar{w}$ be the word representing $w \in S$. If $v = u_1 u u_2$ and $v, u \in S$, then $u_1, u_2 \in S$ or empty and the equality $\bar{v} = \bar{u}_1 \bar{u} \bar{u}_2$ is graphical.*

The third assumption implies that both x_1 and x_2 are not divisors of 1; in particular, they are not invertible.

Proof. The set N can be interpreted as the centralizer of x_1, $C(x_1) = \{x_1^n \mid n \in \mathbb{N}\}$, which is defined by the formula $\theta(y, x_1) : x_1 y = y x_1$. One has to show that the operations $+$ and $\cdot$ and the constants 0 and 1 are intepretable. To interpret addition, we interpret the addition relation $\{(m, n, k) \mid m + n = k\}$ as the set of triples of the form $(x_1^n, x_1^m, x_1^{n+m})$ which can be defined by the formula $\phi(x, y, z)$: $xy = z$. Thus, we interpret the constant 0 in $\mathbb{N}$ as the empty word $\emptyset$, and it is easy to see $\emptyset$ is an identity element of the addition operation defined by ϕ. To interpret multiplication of $\mathbb{N}$, we show that set $\{(x_1^n, x_1^m, x_1^{nm})\}$ is definable. Given x_1^n, x_1^m, define w as

$$w(x_1^n, x_1^m) = x_2^2 x_1^{n+1} x_2 x_1^{m+1} x_2^2 x_1^n x_2 x_1^{2m+1} x_2^2 \dots x_2^2 x_1^2 x_2 x_1^{mn+1} x_2^2 \tag{2.2}$$

The element $w \in S$ is completely determined by the following conditions:

1) (head)$w = x_2^2 x_1^{n+1} x_2 x_1^{m+1} x_2^2 w_0$,

2) (recursion)If $w = w_1 x_2^2 w_2 x_2^2 w_3$ and $w_2 = v_1 x_2 v_2, v_1, v_2 \in \langle x_1 \rangle$, and $v_1 \neq x_1$ and $v_1 \neq x_1^2$, then $w_3 = v_3 x_2 v_4 x_2^2 w_4$, where $v_1 = v_3 x_1, v_4 = v_2 x_1^m$,

3) (tail) $w = w_4 x_2^2 x_1^2 x_2 v_5 x_2^2$ where $v_5 \in \langle x_1 \rangle$ or $w = x_2^2 x_1 x_2 x_1^{m+1} x_2^2$.

Conditions 1)–3) can be written in $\mathcal{L}_{\{x_1,x_2\}}$. Note that in condition 3), we take into account the case where $n = 0$, i.e. $x_1^n = \emptyset$. Let $\psi(x, y, w)$ be the formula defining $w(x, y)$, where $x, y \in C(x_1)$, then for $x = x_1^n, y = x_1^m$, we have $z = x_1^{nm}$ if and only if

$$\phi(x, y, z) :\ x, y, z \in \langle x_1 \rangle \wedge (\exists w\, \psi(x, y, w) \wedge (\exists w_4\, w = w_4 x_2^2 x_1^2 x_2 z x_1 x_2^2 \vee z = \emptyset)).$$

The identity element 1 in $\mathbb{N}$ can be interpreted as x_1. One can easily check that it is consistent with the interpretation of multiplication. □

The previous result implies that $\mathbb{N}$ is interpretable in many interesting monoids.

- A *Baumslag-Solitar monoid* is a monoid given by a presentation $\langle a, b | ab^k = b^m a\rangle$.

- *Partially commutative monoids* (also known as *trace monoids* or *right angled Artin monoids* are defined as follows:

  Given a finite graph Γ with the set of vertices V and edges E, we define such a monoid A_Γ by generators V and relations $v_1 v_2 = v_2 v_1$ for each pair of vertices $(v_1, v_2) \in E$.

Theorem 1. $\mathbb{N}$ *is interpretable (with parameters) in* $\mathbb{M}_X$ *and in the following classes of monoids:*

a) Baumslag-Solitar monoids with $k, m > 2$ (we do not need parameters for them)

b) Non-commutative partially commutative monoids.

c) One-relator monoids $G = \langle a, b, C | x = y\rangle$, where C is a non-empty alphabet, some letter of C appears in y and neither x nor y end with a (or one could consider the dual case).

Proof. a) We take $x_1 = a, x_2 = b$. The set S can be defined using the fact that both x_1 and x_2 are irreducible elements. Notice that elements a and b are definable, therefore we have interpretability without parameters.

b) We take $x_1 = v_1, x_2 = v_2$ such that Γ does not have an edge between v_1 and v_2. A non-trivial element is irreducible if it is not a product of two non-trivial elements. The cyclic submonoid $\langle x_1 \rangle$ is definable as the set consisting of the trivial element and non-trivial elements having only x_1 as their irreducible divisor. The set S can be defined using the fact that both x_1 and x_2 are irreducible elements. The generating set of A_Γ is definable as a set of irreducible elements. The submonoid generated by x_1, x_2 is free and an element in S cannot be represented as a word not in $\bar{S}$, therefore the third assumption is also satisfied.

Moreover, the free submonoid generated by x_1, x_2 is definable, hence the statement also follows from transitivity of interpretations.

c) In this case we can assume that the monoid is not free because for a free monoid all the assumptions of Lemma 3 are satisfied. The element a is irreducible. By the Freiheitssatz for one relator monoids, a, b generate a free submonoid since a letter from C appears in the relation. Note that since neither x nor y end in an a, we cannot create an a at the end of a word by applying relations and if ua, va are equal in G then u and v are equal in G (since the derivation from ua to va will never touch the final a).

We show by induction on word length that the centralizer of a is $\langle a \rangle$. If w commutes with a then from $aw = wa$ in G and by the above, we have that

w graphically ends in a, say $w = ua$. Then $aua = uaa$ in G. We deduce by right cancelling a, as discussed above, that $au = ua$ in G. By induction u is a power of a and hence w is a power of a.

If x contains some letters from C, then the submonoid generated by a, b is definable. If only y contains some $c \in C$ but b is contained in x and y, then we can interchange c and b. Suppose that x only contains b and maybe a and y only contains c and maybe a. Then $x \neq b, y \neq c$ because the monoid is not free. Therefore, b, c are irreducible. In this case we can replace b by bcb in the interpretation and in the definition of the set S. □

Corollary 3. *If G is a monoid from Theorem 1, then the first-order theory $Th(G)$ is undecidable.*

To eliminate parameters from the interpretation of $\mathbb{N}$ in $\mathbb{M}_X$ given in Lemma 3 we need the following lemma.

Lemma 4. *The relation $\{(x_2^s, x_1^s) \mid s \in \mathbb{N}\}$ is definable in $\mathbb{M}_X$ with parameters x_1, x_2.*

Proof. We begin by defining the set $\{x_2^s x_1^s \mid s \in \mathbb{N}\}$. Let $a = x_1x_2x_1x_2^2$.

The monomial $f = ax_2x_1a^2x_2^2x_1^2a^3 \cdots x_2^s x_1^s a^{s+1}$ satisfies the following conditions:

1) $f = ax_2x_1a^2g_3$ where g_3 does not begin with a

2) If $f = g_1\bar{a}g_2\bar{a}ag_3$ where $\bar{a} \in C(a)$, g_1 does not end in a, g_2 does not start or end with a and g_3 does not start with a, then $g_3 = x_2g_2x_1\bar{a}a^2g_4$ where g_4 does not start with a or $g_3 = \emptyset$.

3) $f = g_1\bar{a}u\bar{a}a$, where $a \in C(a)$, g_1 does not end in a and u does not begin or end with a and is not divisible by a.

Conditions 1)–3) can be written in $\mathcal{L}_{\{x_1,x_2\}}$ and uniquely define a word f, so let $\phi(x)$ be the formula defining all such words f, then the formula

$$\psi(x) : \exists f, g_1, g_1', b, x_1, x_2\ (\phi(f) \wedge f = g_1bxab \wedge g_1 \neq g_1'a \wedge x \neq x_1a \wedge x \neq ax_2 \wedge b \in C(a))$$

defines the set $\{x_2^s x_1^s \mid s \in \mathbb{N}\}$.

Now the following formula defines the set of pairs of the form (x_2^s, x_1^s):

$$Trans(x, y) : \exists z\, \psi(z) \wedge z = xy \wedge x \in C(x_2) \wedge y \in C(x_1) \qquad (2.3)$$

□

The basis X consists of all irreducible elements and therefore is definable in $\mathbb{M}_X$ by the formula $\theta(x) : \forall y \forall z\, (x = yz \implies y = \emptyset \vee z = \emptyset)$.

Theorem 2. $\mathbb{N}$ *is $\emptyset$-interpretable in* $\mathbb{M}_X$.

Proof. We will give a proof for $\mathbb{M}_X$. Denote by $\mathbb{N}_{x_i}$ the interpretation of $\mathbb{N}$ as $C(x_i)$, where x_i is an element of the basis X. The number m is interpreted as a pair (x_i^m, x_i). Lemma 3 implies that there is a definable isomorphism between $\mathbb{N}_{x_i}$ and $\mathbb{N}_{x_j}$ for any two elements x_i and x_j of the basis. Indeed, we can define pairs $(x_i^s, x_j^s), i \neq j$ where $1 \leq i, j \leq |X|$, without parameters with the following formula:

$$\phi(x, y) : \exists z_1, z_2 (z_1, z_2 \in X \wedge z_1 \neq z_2 \wedge Trans'(x, y)) \tag{2.4}$$

where $Trans'(x, y)$ is the formula $Trans(x, y)$ with any occurrences of x_1 and x_2 replaced by z_1 and z_2, respectively.

Thus we have a definable (without parameters) equivalence relation on the set of pairs (x_i^m, x_i) and factoring over this equivalence relation we identify all the structures $\mathbb{N}_{x_i}$ into one structure isomorphic to $\mathbb{N} = \langle N, +, \cdot, 0, 1\rangle$. Therefore $\mathbb{N} = \langle N, +, \cdot, 0, 1\rangle$ is $\emptyset$-interpretable in $\mathbb{M}_X$. □

Remark 2. *We can similarly prove $\emptyset$-interpretability of $\mathbb{N} = \langle N, +, \cdot, 0, 1\rangle$ in the non-commutative A_Γ.*

2.3 Bi-interpretability of $\mathbb{M}_X$ and some other monoids with $\mathbb{N}$

We have shown in the previous section that $\mathbb{N}$ is interpretable in a monoid G satisfying the assumptions of Lemma 3. Thus, by transitivity of interpretability, we have that $S(\mathbb{N}, \mathbb{N})$ is interpretable in G and, therefore, in $\mathbb{M}_X$.

In this section we will construct a direct interpretation of $S(\mathbb{N},\mathbb{N})$ in $\mathbb{M}_X$, which we will use in Section 2.3.2. The same technique also works for A_Γ without center.

Lemma 5. *$S(\mathbb{N},\mathbb{N})$ is $\emptyset$-interpretable in $\mathbb{M}_X$ and in any non-commutative A_Γ.*

Proof. We will give the proof for $\mathbb{M}_X$. Recall that the set $C(x_1) = \{x_1^n \mid n \in \mathbb{N}\}$ is interpretable in $\mathbb{M}_X$ with parameter x_1 and similarly $C(x_2)$ is interpretable with parameter x_2.

To interpret $S(\mathbb{N},\mathbb{N})$ in $\mathbb{M}_X$, we first interpret a tuple $t = (t_1, \ldots, t_m)$ in $S(N)$ with $m \geq 1$ as a word

$$w_t = x_1 x_2^{t_1+1} x_1^2 x_2^{t_2+1} \cdots x_1^m x_2^{t_m+1} \tag{2.5}$$

Note that any such word w_t is completely determined by t and the following conditions:

1) (head) $w_t = x_1 x_2 g_1$

2) (recursion) If $w_t = g_3 x_1^i g_4$ where $g_3 \neq g_3' x_1$, $g_4 = x_2 g_4'$, then $g_4 = g_5 x_1^{i+1} g_6$ where $g_5 \in C(x_2)$ and $g_6 = x_2 g_6'$, or $g_4 \in C(x_2)$.

3) (tail) $w_t = g_7 x_2$

Conditions 1)–3) are definable in $\mathcal{L}_{\{x_1,x_2\}}$, so there is a formula $w(x)$ defining the set of words w_t for $t \in S(N)$.

Next, we interpret the relations $\in$, $t(s,i,a)$, $l(s,n)$. The set of triples (w, x_1^i, x_1^a), where a is the i^{th} component of the tuple given by w, can be defined by the following formula, which says roughly that $x_1^i x_2^{a+1}$ is a subword of w:

$$\begin{aligned} t(x,y,z)\colon\ & w(x) \wedge y \in C(x_1) \wedge \\ & (\exists g_1, g_2, g_1', g_2', v\ \ x = g_1 y x_2 v g_2 \wedge g_1 \neq g_1' x_1 \wedge g_2 \neq x_2 g_2' \wedge \\ & v \in C(x_2) \wedge Trans(v,z)) \end{aligned}$$

The set of pairs (x_1^a, w) where a is a component of the tuple encoded in w, can be defined by the formula $In(x,y)\ :\ \exists z\, t(y,z,x)$. Finally, the length relation can be defined by the formula $l(x,y)\ :\ w(x) \wedge y \in C(x_1) \wedge \exists g_1, g_2, g_1'\, x = g_1 y g_2 \wedge g_1 \neq g_1' x_1 \wedge g_2 \in C(x_2)$.

Next we interpret the concatenation operation in $\mathbb{M}_X$. Suppose we have words w_1 and w_2 corresponding to the tuples $(t_1, \ldots, t_m)$ and $(p_1, \ldots, p_n)$ respectively. Let $w_2' = x_1^{m+1} x_2^{p_1+1} \cdots x_1^{m+n} x_2^{p_n+1}$. Then w_2' has the following properties:

1) (head)$w'_2 = x_1^{m+1}x_2g_1$, where m is the length of w_1

2) (recursion) If $w'_2 = g_2x_1^{m+i}g_3$ where $g_2 \neq g'_2x_1$ and $g_3 = x_2g'_3$, then $g_3 = x_2^{p_i+1}x_1^{m+i+1}g_4$, where $g_4 = x_2g'_4$, or $g_3 = x_2^{p_i+1}$.

3) (tail) $w'_2 = g_5x_2$

All of these properties are definable with parameters x_1, x_2, and with the formulas defining the interpretations of the length and position functions. Thus, there is a formula $\phi(x, y, z)$ such that $\mathbb{M}_X \models \phi(w_1, w_2, w'_2)$ if and only if w_1, w_2, w'_2 are as above. Now let t_3 be the concatenation of the tuples t_1 and t_2. Let the corresponding words be w_1, w_2, w_3 respectively. Then the formula $Concat(x, y, z)$: $\exists u\, \phi(x, y, u) \wedge z = xu$ defines concatenation uniformly in X, that is, $Concat(w_1, w_2, w_3)$ holds when $t_1 \frown t_2 = t_3$. Note that the use of x_1, x_2 in the interpretation is arbitrary; if instead of x_1, x_2 we take two $x_i, x_j \in X$, $i \neq j$, we just have to replace in the formula x_1, x_2 by x_i, x_j, respectively.

To eliminate parameters we can now, as in the proof of Theorem 2, define by a formula the equivalence relation identifying elements $w_t(x_i, x_j)$ for all pairs (x_i, x_j) of basis elements.

The proof for A_Γ is similar. □

2.3.1 Interpretation of $\mathbb{M}_X$ and other monoids in $S(\mathbb{N}, \mathbb{N})$

Let $X = \{x_1, \dots, x_n\}$. We interpret a monomial $x_{i_1} x_{i_2} \cdots x_{i_m} \in \mathbb{M}_X$ as the tuple $(i_1, i_2, \dots, i_m)$. Let $T = \{(t_1, \dots, t_m) \mid 1 \leq t_i \leq n,\ m \in \mathbb{N}\}$, then any element of T can be uniquely associated to a monomial in $\mathbb{M}_X$. So, $\mathbb{M}_X$ can be interpreted in $S(\mathbb{N}, \mathbb{N})$ as the set T. It is easy to see T is definable since the conditions $1 \leq t_i \leq n$ and $m \in \mathbb{N}$ can be written in the language of $S(\mathbb{N}, \mathbb{N})$. Multiplication in $\mathbb{M}_X$ can be interpreted as concatenation. So, $\mathbb{M}_X$ is $\emptyset$-interpretable in $S(\mathbb{N}, \mathbb{N})$.

Lemma 6. *If G is a monoid from Theorem 1, a), b) or a monoid with solvable word problem from c), then G is interpretable in $S(\mathbb{N}, \mathbb{N})$ and in $\mathbb{N}$.*

Proof. Notice that the word problem is solvable in monoids from a) and b). One can recursively enumerate all short-lex forms of elements in G and encode them as tuples in $\mathbb{N}$ the same way as this is done for $\mathbb{M}_X$. Multiplication is not just concatenation anymore, but the corresponding predicate is recursively enumerable and therefore definable in $S(\mathbb{N}, \mathbb{N})$. □

2.3.2 Bi-interpretation

Theorem 3. *1. $S(\mathbb{N}, \mathbb{N})$ and $\mathbb{M}_X$ are bi-interpretable with parameters in X uniformly in X.*

2. If a non-trivial partially commutative monoid A_Γ has trivial center, then $S(\mathbb{N},\mathbb{N})$ and A_Γ are bi-interpretable with the standard generating set (vertices V of Γ) as parameters.

1. We first will prove bi-interpretability of $S(\mathbb{N},\mathbb{N})$ and $\mathbb{M}_X$ uniformly in X. Since the bi-interpretability is with parameters, we will use the first interpretation of $\mathbb{M}_X$ from the proof of Lemma 3, in which we used x_1 and x_2 as parameters.

Denote by $\mathbb{M}_X^*$ the interpretation of $\mathbb{M}_X$ in $S(\mathbb{N},\mathbb{N})$, and by $S(\mathbb{N},\mathbb{N})^*$ the interpretation of $S(\mathbb{N},\mathbb{N})$ in $\mathbb{M}_X$. Denote the images of $\mathbb{M}_X$ and $S(\mathbb{N},\mathbb{N})$ in themselves by $\mathbb{M}_X^{**}$ and $S(\mathbb{N},\mathbb{N})^{**}$, respectively. To show bi-interpretability, it remains to show that the isomorphisms $S(\mathbb{N},\mathbb{N}) \to S(\mathbb{N},\mathbb{N})^{**}$ and $\mathbb{M}_X \to {\mathbb{M}_X}^{**}$ are definable in $S(\mathbb{N},\mathbb{N})$ and $\mathbb{M}_X$, respectively. The isomorphism $\psi : S(\mathbb{N},\mathbb{N}) \to S(\mathbb{N},\mathbb{N})^{**}$ is the composition of the map taking a tuple $t = (t_1,\dots,t_m) \mapsto w_t = x_1x_2^{t_1+1}\cdots x_1^m x_2^{t_m+1}$ and the map taking $M = x_{t_1}\cdots x_{t_m} \mapsto t_M = (t_1,\dots,t_m)$. So, $\psi(t) = (1,2,\dots,2) \frown (1,1,2,\dots,2) \frown \cdots \frown (1,\dots,1,2,\dots,2)$ where the i^{th} tuple has i 1's and t_i+1 2's. Since every recursively enumerable predicate is definable in $\mathbb{N}$ we have the following

Lemma 7. *The isomorphism $\phi : S(\mathbb{N},\mathbb{N}) \to S(\mathbb{N},\mathbb{N})^{**}$ mapping $t \mapsto t_{w_t}$ is $\emptyset$-definable in $S(\mathbb{N},\mathbb{N})$.*

To show that the isomorphism $\phi : \mathbb{M}_X \to \mathbb{M}_X{}^{**}$ is definable, note that this map is the composition of the map sending $x_{i_1} \cdots x_{i_m} \mapsto (i_1, \ldots, i_m)$ and the map sending $(i_1, \ldots, i_m) \mapsto x_1 x_2^{i_1+1} \cdots x_1^m x_2^{i_m+1}$. We will show that this isomorphism is definable with parameters in X. Recall that the set X is definable in $\mathbb{M}_X$.

We first define a relation $R = \{(x_1, x_1), (x_2, x_1^2), \ldots, (x_n, x_1^n)\}$ that pairs up the index of an element in X with its interpretation. In the language $\mathcal{L}_X$, this relation is certainly definable. We will call two elements x_i and x_1^i pairs.

Next, given a number $m \in \mathbb{N}$, we define an element $a_m \in \mathbb{M}_{\{x_1,x_2\}}$ by

$$a_m = x_2 x_1 x_2 x_1^2 x_2 x_1^3 \cdots x_2 x_1^m \tag{2.6}$$

Lemma 8. *The set of pairs $B = \{(a_m, x_1^m) \mid m \in \mathbb{N}, m > 0\}$ is definable in $\mathbb{M}_X$.*

Proof. The monomials a_m are completely determined by m and the following conditions:

1) (head) $a_m = x_2 x_1 x_2 u$

2) (recursion) If $a_m = u_1 x_2 v x_2 u_2$ with $v \in C(x_1), u_2 \neq x_1^m$, then $u_2 = v x_1 x_2 u_3$.

3) (tail) $a_m = u_4 x_2 x_1^m$

The conditions are definable in $\mathbb{M}_X$ in the language $\mathcal{L}_{\{x_1,x_2\}}$, so the relation B is definable in $\mathbb{M}_X$ with parameters x_1 and x_2. □

Lemma 9. *The isomorphism* $\phi : \mathbb{M}_X^{**} \to \mathbb{M}_X$ *sending* $w_M = x_1 x_2^{i_1+1} \cdots x_1^m x_2^{i_m+1} \mapsto M = x_{i_1} \cdots x_{i_m}$ *is definable in* $\mathbb{M}_X$ *with parameters in* X *uniformly in* X.

Proof. Recall that for a word $w_M = x_1 x_2^{i_1+1} \cdots x_1^m x_2^{i_m+1}$ we have defined a length relation and the position relation $t(s, i, a)$. Thus, for w_M let $a = a_m$, where m is the length of w_M, and define a word w as follows:

$$w = (ax_2a)x_{i_1}(a^2x_2^2a^2)x_{i_1}x_{i_2}(a^3x_2^3a^3)\cdots x_{i_1}x_{i_2}\cdots x_{i_m}(a^{m+1}x_2^{m+1}a^{m+1}) \quad (2.7)$$

The word w is completely determined by w_M and the following conditions:

1) (head) $w = (ax_2a)x_{i_1}(a^2x_2^2a^2)v_1$, where x_{i_1} is the pair of the first component of w_M.

2) (recursion) For any $j \in \mathbb{N}, 0 < j < m$, and for any $v_2, v_3, v_4 \in M$, if $w = v_2(\bar{a}x_2^j\bar{a})v_3(\bar{a}ax_2^{j+1}\bar{a}a)v_4$, where $\bar{a} \in C(a)$, v_2, v_3 do not end in a, v_3, v_4 do not start with a,
then $v_4 = v_3 x_{i_{j+1}}(\bar{a}a^2x_2^{j+2}\bar{a}a^2)v_5$, where v_5 does not begin with a, and $x_{i_{j+1}}$ is the pair of the $(j+1)'st$ component of w_M

3) (tail) $w = v_6(\bar{a}x_2^{m+1}\bar{a})$, where $\bar{a} \in C(a)$ and v_6 does not end with a.

Conditions 1)–3) are definable with parameters in X. Thus, there is a formula $\theta_0(x, z, X)$ such that $\theta_0(w_M, w, X)$ holds in $\mathbb{M}_X$ whenever w_M, w are as we defined them. Then the formula $\theta_1(x, y, X) : \exists z, y\, (\theta_0(x, z, X) \wedge z = u(\bar{a}x_2^m\bar{a})y(\bar{a}ax_2^{m+1}\bar{a}a) \wedge \forall u'\ (u \neq u'a))$ defines a pair (w_M, M) with parameters in X. □

The first statement of Theorem 3 is proved now.

To prove the second statement we need an analog of Lemma 9, but we have to make such an element $a = a_m$ that does not commute with any generator and the element w is uniquely defined by 1)–3) and w_M. If in Lemma 8 we replace any occurrence of x_2 in a_m by the product of all the generators in V except x_1, then the proof of Lemma 9 will work. This proves the second statement of Theorem 3 .

Corollary 4. $\mathbb{M}_X$ *and* $\mathbb{N}$ *are bi-interpretable with parameters* X *uniformly in* X.

This result gives us an interesting corollary.

The first-order theory of every structure $\mathcal{B}$ that is bi-interpretable with $\mathbb{N}$ has the same expressive power as the weak second order theory of $\mathcal{B}$. Namely, every statement about $\mathcal{B}$ that can be expressed in the weak second order logic of $\mathcal{B}$ can be expressed in the first-order logic.

Corollary 5. *If $\mathcal{B}$ and $\mathbb{N}$ are bi-interpretable, then $\mathcal{B}$ and $S(\mathcal{B},\mathbb{N})$ are bi-interpretable.*

Proof. Since $\mathcal{B}$ and $\mathbb{N}$ are bi-interpretable, we have that $S(\mathcal{B},\mathbb{N})$ and $S(\mathbb{N},\mathbb{N})$ are bi-interpretable. At the same time, $\mathbb{N}$ and $S(\mathbb{N},\mathbb{N})$ are bi-interpretable. Therefore $\mathcal{B}$ and $S(\mathcal{B},\mathbb{N})$ are bi-interpretable. □

Corollary 6. *$\mathbb{M}_X$ and $S(\mathbb{M}_X,\mathbb{N})$ are bi-interpretable with parameters X uniformly in X.*

Corollary 7. *A non-trivial A_Γ with trivial center and $S(A_\Gamma,\mathbb{N})$ are bi-interpretable with parameters V uniformly in V.*

2.4 Corollaries

We now discuss some corollaries of this bi-interpretation.

2.4.1 Definability of a submonoid

Consider now the submonoid of $\mathbb{M}_X$ generated by the elements $g_1,\dots,g_k$, that is, $\langle g_1,\dots,g_k\rangle$.

Theorem 4. *For any $k \in \mathbb{N}$, there is a formula $\psi(y, y_1, \ldots, y_k, X)$ such that $\psi(g, g_1, \ldots, g_k, X)$ holds in $\mathbb{M}_X$ if and only if $g \in \langle g_1, \ldots, g_k \rangle$.*

Such a formula also exists for any non-trivial A_Γ with trivial center.

We will give a proof for $\mathbb{M}_X$. We will use the fact that the structures $\mathbb{N}$ and $S(\mathbb{N}, \mathbb{N})$ are bi-interpretable with $\mathbb{M}_X$.

Recall from Lemma 2 that $S(\mathbb{N}, \mathbb{N})$ is $\emptyset$-interpretable in $\mathbb{N}$. We will refer to the interpretation in $\mathbb{N}$ of a finite sequence (tuple) in $S(N)$ as its code.

Proof of Theorem 4. Consider now $W = \langle g_1, \ldots, g_k \rangle$ and recall that each $g_i = x_{i_1} \cdots x_{i_m}$ has an interpretation in $S(\mathbb{N}, \mathbb{N})$ as the tuple $t_i = (i_1, \ldots, i_m)$, and this tuple in turn is interpreted as a code $n_i \in \mathbb{N}$. The set of words in $\langle g_1, \ldots, g_k \rangle$ can be recursively enumerated. Therefore the set of all tuples $(g_1, \ldots, g_k, g)$ such that $g \in \langle g_1, \ldots, g_k \rangle$ is also recursively enumerable. Therefore the set $W_k = \{(n_1, \ldots, n_k, s)\}$ of $k + 1$-tuples of codes of $(g_1, \ldots, g_k, g)$ in $\mathbb{N}$ is also recursively enumerable.

By Proposition 1, we have that the set W_k is Diophantine. So, there is a polynomial $P(x_1, \ldots, x_n, y_1, \ldots, y_k, z)$ with integer coefficients such that $P(x_1, \ldots, x_n, n_1, \ldots, n_k, s) = 0$ has a solution in $\mathbb{Z}$ if and only if $(n_1, \ldots, n_k, s) \in W_k$. Thus, the formula $\phi(y_1, \ldots, y_k, z) : \exists x_1, \ldots, x_n \, P(x_1, \ldots, x_n, y_1, \ldots, y_k, z) = 0$ defines W_k in $\mathbb{Z}$. Since $\mathbb{N}$ is definable in $\mathbb{Z}$, there is some formula $\phi'(y_1, \ldots, y_k, z)$ which defines W_k in $\mathbb{N}$.

To show that the set $S_k = \{(g_1, \ldots, g_k, g) \mid g \in \langle g_1, \ldots, g_k \rangle\}$ is definable in $\mathbb{M}_X$, we use the result in Lemma 9.

The formula $\phi'(y_1, \ldots, y_k, z)$ defines the set $W_k = \{(n_1, \ldots, n_k, s)\} \in \mathbb{N}^{k+1}$ where for each $1 \leq i \leq k$, n_i is the code of an element $g_i \in \mathbb{M}_X$ and s is the code of an element $g \in \langle g_1, \ldots, g_k \rangle$. Since $\mathbb{N}$ is $\emptyset$-interpretable in $\mathbb{M}_X$, by Lemma 1, there is a formula $\phi^*(y_1, \ldots, y_k, z, X)$ in $\mathbb{M}_X$ such that for any $n_1, \ldots, n_k, s \in \mathbb{N}$, $\mathbb{N} \models \phi'(n_1, \ldots, n_k, s)$ if and only if $\mathbb{M}_X \models \phi^*(n_1^*, \ldots, n_k^*, s^*, X)$, where $n_1^*, \ldots, n_k^*, s^*$ are the images of $n_1, \ldots, n_k, s$ in $\mathbb{M}_X$. By Lemma 9 the set of tuples $\{(n_1^*, \ldots, n_k^*, s^*, g_1, \ldots, g_k, g, \}$ is definable in $\mathbb{M}_X$ by some formula $\theta(n_1^*, \ldots, n_k^*, s^*, g_1, \ldots, g_k, g, X)$. Let

$$\psi(g_1, \ldots, g_k, g, X) =$$

$$\exists n_1^*, \ldots, n_k^*, s^*(\phi^*(n_1^*, \ldots, n_k^*, s^*, X) \wedge \theta(n_1^*, \ldots, n_k^*, s^*, g_1, \ldots, g_k, g, X)).$$

Then $\mathbb{N} \models \phi'(n_1, \ldots, n_k, s)$ if and only if $\mathbb{M}_X \models \psi(g_1, \ldots, g_k, g, X)$ if and only if $g \in \langle g_1, \ldots, g_k \rangle$, so we have our result.

Similarly one can prove the result for A_Γ without the center and the following result.

Theorem 5. *Every recursively enumerable language in the alphabet X is definable in $\mathbb{M}_X$.*

2.4.2 Isolation of Types, Homogeneity, and QFA property

Let $\mathcal{B}$ be an algebraic structure and $A \subseteq B$. A set p of $\mathcal{L}_A$-formulas in n free variables is called an *n-type* of $Th(\mathcal{B}, \{a\}_{a\in A})$ if $p \cup Th_A(\mathcal{B})$ is satisfiable. A type p is called *complete* if for each $\mathcal{L}_A$-formula ϕ with n free variables, either ϕ or $\neg\phi$ is in p. Moreover, p is said to be *realized* in $\mathcal{B}$ if there is some $\bar{b} \in B^n$ such that $\mathcal{B} \models \phi(\bar{b})$ for all $\phi \in p$. For a tuple $\bar{b} \in B^n$, the set $tp^{\mathcal{B}}(\bar{b}/A) = \{\phi(\bar{x}) \in \mathcal{L}_A \mid \mathcal{B} \models \phi(\bar{b})\}$ is a complete n-type.

A complete n-type p is isolated if there is a formula $\phi(\bar{x}) \in p$ such that for all $\mathcal{L}$-formulas $\psi(\bar{x}), \psi(\bar{x}) \in p$ if and only if $Th(\mathcal{B}) \models (\phi(\bar{x}) \implies \psi(\bar{x}))$. Moreover, $\mathcal{B}$ is called *atomic* over A if every type that is realized in $\mathcal{B}$ is isolated.

Remark 3. *Let $\mathcal{B}$ be a countable structure. Then $\mathcal{B}$ is atomic if for any $b \in B^m$, the orbit $Aut(\mathcal{B}) \cdot b$ is $\emptyset$-definable.*

A model is *homogeneous* if two finite tuples realize the same types if and only if they are automorphically equivalent. Every countable atomic model is homogeneous.

Theorem 6. *$\mathbb{M}_X$ is atomic and, therefore, homogeneous.*

Proof. Note that since the basis X of $\mathbb{M}_X$ is definable, any automorphism must send basis elements to basis elements. Morever, an automorphism is completely determined by where it sends the basis elements. Thus, the orbit of a word $w = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n} \in \mathbb{M}_X$ is the set of words $\{s = x_{\sigma(i_1)}^{e_1} \cdots x_{\sigma(i_n)}^{e_n}\}$ where σ is a permutation of the set $\{1, \ldots, n\}$. It is easy to see that this set is definable. For example, the orbit of a word $x_1^2 x_3 x_2 x_3$ can be defined by the formula $\phi(x) : \exists y_1, y_2, y_3 \in X \, (y_1 \neq y_2 \neq y_3 \wedge x = y_1^2 y_2 y_3 y_2)$. Similarly, we can show that the orbits of arbitrary tuples $\bar{b}$ of $\mathbb{M}_X$ are definable. Thus, $\mathbb{M}_X$ is atomic.

□

The same result is true for A_Γ without the center because the standard generating set is definable.

Remark 4. *If $|X| > 1$, then $\mathbb{M}_X$ is QFA and prime. A non-trivial A_Γ with trivial center is QFA and prime.*

This follows from Theorem 7.14 in [Nie07] and Corollary 4. Theorem 7.14 in [Nie07] says that a finitely generated structure $\mathcal{B}$ in a finite signature that is bi-interpretable with the integers (or with $\mathbb{N}$) is prime and QFA.

In contrast to this, recall that two non-abelian free groups of different ranks are elementarily equivalent, therefore the theory of non-abelian free groups is not QFA.

2.4.3 Quantifier elimination

In this section we will show that there is no quantifier elimination in the theory of any structure that is bi-interpretable with $\mathbb{N}$. In particular, there is no quantifier elimination in the theory of a free monoid of rank at least two.

Let $\mathcal{L}$ be a first-order language. Recall that a formula ϕ in $\mathcal{L}$ is in a prenex normal form if $\phi = Q_1y_1Q_2y_2\ldots Q_sy_s\phi_0(x_1,\ldots,x_m)$ where Q_i are quantifiers ($\forall$ or $\exists$), and ϕ_0 is a quantifier-free formula in $\mathcal{L}$. It is known that every formula in $\mathcal{L}$ is equivalent to a formula in prenex normal form. A formula $\phi = Q_1y_1Q_2y_2\ldots Q_sy_s\phi_0(x_1,\ldots,x_m)$ in prenex normal form is called a Σ_n formula if the sequence of quantifiers $Q_1Q_2\ldots Q_s$ begins with an existential quantifier $\exists$ and then alternates $n-1$ times between existential and universal quantifiers. Similarly, a formula ϕ as above is a Π_n formula if the sequence of quantifiers $Q_1Q_2\ldots Q_s$ begins with a universal quantifier $\forall$ and then alternates $n-1$ times between existential and universal quantifiers.

For a structure $\mathcal{B}$ in the language $\mathcal{L}$, denote by $\Sigma_n(\mathcal{B})$ (and $\Pi_n(\mathcal{B})$) the set of all subsets of B^m, $m \in \mathbb{N}$, definable in $\mathcal{B}$ by Σ_n (and Π_n) formulas $\phi(x_1,\ldots,x_m)$. Let $\Sigma_0(\mathcal{B}) = \Pi_0(\mathcal{B})$ be the set of all subsets definable in $\mathcal{B}$ by quantifier-free formulas. Clearly,

$$\Sigma_0(\mathcal{B}) \subseteq \Sigma_1(\mathcal{B}) \subseteq \ldots \subseteq \Sigma_n(\mathcal{B}) \subseteq \ldots$$

$$\Pi_0(\mathcal{B}) \subseteq \Pi_1(\mathcal{B}) \subseteq \ldots \subseteq \Pi_n(\mathcal{B}) \subseteq \ldots$$

The sets $\Sigma_n(\mathcal{B})$ and $\Pi_n(\mathcal{B})$ form the so-called *arithmetical hierarchy* over $\mathcal{B}$, denoted by $\mathcal{H}(\mathcal{B})$. It is easy to see that if $\Sigma_n(\mathcal{B}) = \Sigma_{n+1}(\mathcal{B})$ (or $\Pi_n(\mathcal{B}) = \Pi_{n+1}(\mathcal{B})$) for some $n \in \mathbb{N}$ then $\Sigma_m(\mathcal{B}) = \Sigma_{m+1}(\mathcal{B})$ and $\Pi_m(\mathcal{B}) = \Pi_{m+1}(\mathcal{B})$ for every natural $m \geq n$. We say that the hierarchy $\mathcal{H}(\mathcal{B})$ *collapses* if $\Sigma_n(\mathcal{B}) = \Sigma_{n+1}(\mathcal{B})$ for some $n \in \mathbb{N}$, otherwise it is called *proper*.

Theorem 7. *Let $\mathcal{B}$ be a structure in the language $\mathcal{L}$ that is bi-interpretable with $\mathbb{N}$. Then for any $n \in \mathbb{N}$, there is a formula ϕ_n in $\mathcal{L}$ such that the formula ϕ_n is not equivalent in $\mathcal{B}$ to any boolean combination of formulas from Π_n or Σ_n (with constants from B).*

Proof. Suppose, to the contrary, that for some $n \in \mathbb{N}$, any formula $\phi(x_1, \ldots, x_n)$ in the language $\mathcal{L}_\mathcal{B}$ is equivalent in $\mathcal{B}$ to some boolean combination $\phi'(\bar{x})$ of formulas from Π_n or Σ_n with constants from B. Take an arbitrary first-order formula $\psi(z_1, \ldots, z_n)$ in the language of $\mathbb{N}$, $\mathcal{L}_\mathbb{N}$. Since $\mathcal{B}$ is bi-interpretable with $\mathbb{N}$, the formula $\psi(\bar{z})$ can be rewritten as a formula $\phi(\bar{x})$ in $\mathcal{L}_\mathcal{B}$ such that for any values $\bar{a}$ of $\bar{z}$, $\mathbb{N} \models \psi(\bar{a}) \iff \mathcal{B} \models \phi(\bar{b})$, where $\bar{a} \to \bar{b}$ when

$\mathbb{N}$ is interpreted in $\mathcal{B}$. By our assumption, there is a formula $\phi'(\bar{x})$ in $\mathcal{L}_{\mathcal{B}}$ which is a boolean combination of formulas from Π_n or Σ_n, possibly with constants from B, such that $\phi(\bar{x})$ is equivalent to $\phi'(\bar{x})$ in $\mathcal{B}$. Since $\mathcal{B}$ is bi-interpretable with $\mathbb{N}$, there is a number m (which depends only on the bi-interpretation) such that $\phi'(\bar{x})$ can be rewritten into a formula $\psi'(\bar{z})$, which is a boolean combination of formulas from Π_{n+m} or Σ_{n+m} in $\mathcal{L}_{\mathbb{N}}$ such that $\mathbb{N} \models \psi'(\bar{a}) \Longleftrightarrow \mathcal{B} \models \phi'(\bar{b})$. It follows that $\psi(\bar{z})$ is equivalent to $\psi'(\bar{z})$ in $\mathbb{N}$, i.e., every formula ψ of the language of $\mathbb{N}$ is equivalent in $\mathbb{N}$ to some formula ψ' which is a boolean combination of formulas from Π_{n+m} in the language of $\mathbb{N}$. However, this is false since the arithmetical hierarchy in $\mathbb{N}$ is proper. It follows that our assumption is false, so the theorem holds. □

Corollary 8. *The hierarchy $\mathcal{H}(\mathbb{M}_X)$ is proper.*

Chapter 3

Equations in metabelian groups

The Diophantine problem (DP) for a group G, denoted $\mathcal{DP}(G)$, is the following: Given a finite system of equations in G, is there an algorithm that can determine whether the system has a solution or not? The decidability of $\mathcal{DP}(G)$ is equivalent to the decidability of the positive existential theory (with constants) of the group. Note that in the language of groups, positive existential sentences have the form

$$\exists x_1, \ldots, x_n \, \phi_0(x_1, \ldots, x_n, g_1, \ldots, g_m) = 1$$

where ϕ_0 is a product of the variables $x_1, \ldots, x_n$ and constants $g_1, \ldots g_m$ from G, and 1 is the identity element of the group. Deciding whether a sentence (or conjunction of sentences) of this form is true or false in G is equivalent to deciding whether a finite system of equations has a solution.

In the Sections 3.1 and 3.2 below, we show that the metabelian groups

$BS(1,k) = \langle a,b|a^{-1}ba = b^k\rangle$ for $k \geq 2$ and $A \wr \mathbb{Z}$, where A is a finitely generated abelian group, have decidable Diophantine problem. Moreover, with these algorithm we are able to describe the solution sets of these systems of equations.

Recall that a group G is metabelian if the commutator subgroup $[G,G]$ is abelian. The groups $BS(1,k)$ and $A \wr \mathbb{Z}$ are semidirect products of the form $G \rtimes \mathbb{Z}$. Both classes of groups are bi-interpretable with $\mathbb{N}$ and thus have undecidable first order theories. We will use techniques from linear algebra as well as results from the literature to prove the decidability of the Diophantine problems for these groups.

3.1 Diophantine Problem in $BS(1,k)$

Our first main result is the following:

Theorem 8. *The Diophantine Problem in $BS(1,k)$ is decidable.*

To prove the theorem we have to construct an algorithm that decides whether a finite system of equations in $BS(1,k)$ has a solution. Recall that the group $BS(1,k) = \langle a,b|a^{-1}ba = b^k\rangle$ is isomorphic to the group $\mathbb{Z}[1/k] \rtimes \mathbb{Z}$, where $\mathbb{Z}[1/k] \cong ncl(a)$ and $\mathbb{Z} \cong \langle b\rangle$, where

$$\mathbb{Z}[1/k] = \{zk^{-y}|z \in \mathbb{Z}, y \in \mathbb{N}\}$$

and the action of $\langle b\rangle$ on $\mathbb{Z}[1/k]$ is given by $b^{-1}ub = uk^{-1}$. Thus, we can think of elements in $BS(1,k)$ as pairs (zk^{-y}, r) where $z, r \in \mathbb{Z}, y \in \mathbb{N}$. The product is defined as

$$(z_1k^{-y_1}, r_1)(z_2k^{-y_2}, r_2) = (z_1k^{-y_1} + z_2k^{-(y_2+r_1)}, r_1 + r_2).$$

The inverse of an element (zk^{-y}, r) is $(-zk^{-y+r}, -r)$.

The following lemma reduces systems of equations in $BS(1,k)$ to systems of equations in $\mathbb{Z}$.

Lemma 10. *Any finite system of equations in $BS(1,k)$ is equivalent to a finite system of equations of the form*

$$\sum_i z_ik^{-y_i}(\sum_j \pm k^{\tau_{ij}(\bar{r})}) - \sum_t \gamma_t k^{\tau_t(\bar{r})} = 0 \tag{3.1}$$

and

$$\sum \beta_j r_j = \delta. \tag{3.2}$$

where $\tau_t(\bar{r}), \tau_{ij}(\bar{r}) = \sum_q \alpha_q r_q + c_q$ and where $\alpha_q, c_q, \delta, \gamma_t, \beta_j \in \mathbb{Z}$, $, z_i, r_i,$ are variables taking values in $\mathbb{Z}$ and y_i is a variable taking values in $\mathbb{N}$.

The product $z_ik^{-y_i}$ can be also considered as one variable in $\mathbb{Z}[1/k]$.

Proof. Note that

$$(z_1k^{-y_1}, r_1) \cdot (z_2k^{-y_2}, r_2) \cdots (z_nk^{-y_n}, r_n) =$$

$$(z_1k^{-y_1} + z_2k^{-(y_2+r_1)} + ... + z_nk^{-(y_n+r_1+...+r_{n-1})}, r_1 + ... + r_n)$$

The system of equations in the first and second component corresponds to systems of equations of the form (3.1) and (3.2), respectively.

□

3.1.1 Reducing to a system of linear equations

To solve a system of equations in $BS(1, k)$, we begin by solving system (3.2). This system is just a linear system of equations with integer coefficients, and it can be regarded as the equation $AX = B$, where $X = (r_1, \dots, r_n)^T$ and A is the matrix of the system. Using integral elementary column operations on A and row operations on $(A|B)$, we can obtain an equivalent system $\bar{A}\bar{X} = \bar{B}$ such that $\bar{A}$ has a diagonal form. This is Smith normal form. Column operations on A correspond to change of variables. Row operations on $(A|B)$ correspond to transformations of the system of equations into an equivalent system. If the system $\bar{A}\bar{X} = \bar{B}$ does not have a solution, then the corresponding system of equations in the group does not have a solution. If the system $\bar{A}\bar{X} = \bar{B}$ has a solution, then we replace this general solution into system (3.1).

Denote the set of remaining r_i's appearing in (3.1) after substitution by $\hat{X} = \{r_{i_1} \dots r_{i_m}\}$. Note that it is possible that system (3.2) has one solution and that $\hat{X} = \emptyset$.

To solve system (3.1), we will regard the system as a linear system with variables $z_i k^{-y_i}$, and linear combinations of exponential functions as coefficients (which may contain variables in $\hat{X}$). It can be transformed using row operations to an equivalent disjunction of triangular systems (with respect to variables $z_s k^{-y_s}$, $s = 1, \dots, q$) of the following form:

$$z_s k^{-y_s} (\sum_j \pm k^{\tau_{sj}(\bar{r})}) = \sum_{i>q} z_i k^{-y_i} (\sum_j \pm k^{\sigma_{ij}(\bar{r})}) + \sum_t \gamma_t k^{\tau_t(\bar{r})},\ s = 1, \dots, q, \tag{3.3}$$

and each system (possibly) with an additional set of equations of the form:

$$\sum_j a_j k^{\phi_j(\bar{r})} = 0. \tag{3.4}$$

Here, $\tau_{sj}, \sigma_{ij}, \tau_t, \phi_j$ are linear combinations of elements in $\hat{X}$ and constants, and $a_j, \gamma_t \in \mathbb{Z}$. We will get a disjunction of systems because when multiplying equations by some coefficient, we have to consider separately the case when this coefficient is zero.

Example 1. *Consider the following example of a system in two variables:*

$$z_1k^{-y_1} + z_2k^{-y_2}(k^{-r_1}) = k^{2-r_1-r_2}$$

$$z_1k^{-y_1}(k^2) + z_2k^{-y_2}(k^{2-r_1}) = -2k^{-1}$$

Note that on the left side of each equation we have terms with $z_ik^{-y_i}$, which we will regard as variables, and on the right we have the terms which we will regard as constants. We begin by multiplying the first equation by $-k^2$, adding the two equations and replacing the second equation by this sum. When we add the two equations, the terms on the left side cancel out. We obtain the system:

$$z_1k^{-y_1} + z_2k^{-y_2}(k^{-r_1}) = k^{2-r_1-r_2}$$

$$0 = -k^{4-r_1-r_2} - 2k^{-1}$$

Note that the equations are of the form (3.3) and (3.4), respectively. In this example, the coefficient $-k^2 \neq 0$ and thus we do not obtain a disjunction of systems.

Example 2. *Now consider the following system in two variables:*

$$z_1k^{-y_1} + z_2k^{-y_2}(k^{-2-r_1}) = 3k^{-1-r_1}$$

$$z_1k^{-y_1}(1-k^{-r_2-r_1})+z_2k^{-y_2}(k^{-r_1-1})=k^{2-r_1}$$

We multiply the first equation by $(k^{-r_2-r_1}-1)$*, add the two equations and replace the second equation by this sum. We must consider separately the case when* $1-k^{-r_2-r_1}=0$*. Thus we get two new systems, the first is:*

$$z_1k^{-y_1}+z_2k^{-y_2}(k^{-2-r_1})=3k^{-1-r_1}$$

$$z_2k^{-y_2}(k^{-2-2r_1-r_2}-k^{-2-r_1}+k^{-r_1-1})=3k^{-1-2r_1-r_2}-3k^{-1-r_1}+k^{2-r_1}$$

The second system is:

$$z_1k^{-y_1}+z_2k^{-y_2}(k^{-2-r_1})=3k^{-1-r_1}$$

$$z_2k^{-y_2}(k^{-r_1-1})=k^{2-r_1}$$

$$1-k^{-r_2-r_1}=0$$

.

The first system is of the form (3.3), whereas in the second, we have equations of the form (3.3) and (3.4), respectively.

We will first show how to solve a system with equations of the form (3.4). In the case where $\hat{X}=\emptyset$, equations of the from (3.4) have no variables and therefore are easily decidable. We show how to solve the system in the case when $\hat{X}\neq\emptyset$.

Semenov's ideas in [Sem84] (where he proved that the theory of $\langle \mathbb{Z}, +, k^x \rangle$ is decidable) can be used to prove the following lemma:

Lemma 11. *Any system of equations over $\mathbb{Z}$ of the form*

$$F(\bar{y}) = \sum_j \beta_j k^{y_j} + C = 0, \tag{3.5}$$

where $\beta_j \in \mathbb{Z}$, $k \in \mathbb{N}, k > 1$, with variables $\bar{y} = (y_1, ..., y_n)$, is equivalent to a disjunction of linear systems of equations over $\mathbb{Z}$.

Proof. Let $\bar{y} = (y_1, \ldots, y_n)$ and let $\lambda : \{y_1, \ldots, y_n\} \to \{+, -\}$ be a map that assigns to each variable a positive or negative sign (we will consider $y_i = 0$ a positive assignment). System (3.5) over $\mathbb{Z}$ is equivalent to a disjunction of 2^n systems, each with an assignment λ. Now we fix one of these systems and we show how to describe all solutions.

We begin by rewriting each equation so that all variables are positive. We may do this by substituting in each equation $-y_i$ for y_i for each y_i that has a negative assignment. Then we multiply each equation by $k^{y_{i_1}+\ldots+y_{i_s}}$, where $y_{i_1}, \ldots, y_{i_s}$ are all the variables whose signs were changed.

For example, suppose we have an equation $k^{y_1} - k^{y_2} + k^{y_3} + c = 0$ with assignment $y_1 < 0, y_2 \geq 0, y_3 \geq 0$. Then we rewrite it as $k^{-y_1} - k^{y_2} + k^{y_3} + c = 0$ with assignment $y_1 \geq 0, y_2 \geq 0, y_3 \geq 0$ and multiply the equation by k^{y_1}. We then obtain the equation

$$1 - k^{y_1+y_2} + k^{y_1+y_3} + ck^{y_1} = 0$$

with assignment $y_1 \geq 0, y_2 \geq 0, y_3 \geq 0$. We now obtain a system over $\mathbb{N}$ of the form

$$\sum_i \beta_i k^{\sum_j y_{ij}} + C = 0$$

where $\beta_i, C \in \mathbb{Z}$.

Next, we substitute all sums in exponents of k by new variables to obtain a system of equations over $\mathbb{N}$ of the form

$$F'(\bar{y}) = \sum_i \beta_i k^{\hat{y}_i} + C = 0 \tag{3.6}$$

Claim: A finite system of equations in the form (3.6) is equivalent to a disjunction of systems of linear equations of the form $\{\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \ldots, \hat{y}_{s-1} = \hat{y}_s + c_s\}$.

Proof. Denote the new variables as $\bar{y}' = \{\hat{y}_1, \ldots \hat{y}_m\}$. We begin by showing that for each i, there is a $\Delta_i \in \mathbb{N}$ such that system (3.6) does not have a solution if $\hat{y}_i > \hat{y}_j + \Delta_i$ for all $j \neq i$.

Fix i. We can rewrite each equation in the system in the form $k^{\hat{y}} + \sum_i \gamma_i k^{\hat{x}_i} = \sum_j \delta_j k^{\hat{z}_j} + C$, where all γ_i, δ_j are positive integers, $\hat{y} = \hat{y}_i$ and $\hat{x}_i, \hat{z}_j$ are all variables in $\bar{y}' - \hat{y}_i$. For each equation, let $\Delta > \log_k(\sum_j \delta_j + C)$ if $C \geq 0$ and $\Delta > \log_k(\sum_j \delta_j)$ if $C < 0$, and suppose $\hat{y} > \hat{x}_i + \Delta$ and $\hat{y} > \hat{z}_j + \Delta$ for all i, j. Then $k^{\hat{y}} > k^{\Delta} k^{\hat{z}_j} > (\sum_j \delta_j + C) k^{\hat{z}_j}$ for all j. Thus, the right side of the equation will always be smaller than the left side, and the equation has no solution. Thus, we can take Δ_i to be the smallest such Δ.

So we have shown that for all variables $\hat{y}_i$, if F' (or a finite system of equations where each equation has form F') has a solution then there is a $j \neq i$ such that $\hat{y}_i \leq \hat{y}_j + \Delta_i$. Now consider a finite graph $\mathcal{G}$ with n vertices labeled $\hat{y}_1, \ldots, \hat{y}_m$ and directed edges from $\hat{y}_i$ to $\hat{y}_j$ whenever $\hat{y}_i \leq \hat{y}_j + \Delta_i$. Note that each vertex must be the initial vertex of some edge and thus the graph must contain a cycle in every connected component. Suppose there is a cycle $\hat{y}_{i_1}, \ldots, \hat{y}_{i_s} = \hat{y}_{i_1}$, $s \leq m + 1$. Then

$$\hat{y}_{i_1} \leq \hat{y}_{i_2} + \Delta_{i_1} \leq \hat{y}_{i_3} + \Delta_{i_2} + \Delta_{i_1} \leq \ldots \leq \hat{y}_{i_s} + \Delta_{i_{(s-1)}} + \ldots + \Delta_{i_1}$$

$$= \hat{y}_{i_1} + \Delta_{i_{(s-1)}} + \ldots + \Delta_{i_1}$$

Therefore for any $2 \leq j \leq s - 1$, we have that

$$\hat{y}_{i_1} - \sum_{t=1}^{j-1} \Delta_{i_t} \leq \hat{y}_{i_j} \leq \hat{y}_{i_1} + \sum_{t=j}^{s-1} \Delta_{i_t}$$

Therefore, the value of any $\hat{y}_{i_j}$ with $2 \leq j \leq s-1$ is bounded by the value of $\hat{y}_{i_1}$.

Fix a y_{i_j} and let $\Delta_{j_1} = \sum_{t=1}^{j-1} \Delta_{i_t}$ and $\Delta_{j_2} = \sum_{t=j}^{m-1} \Delta_{i_t}$. Then we may replace the equation $F'(\bar{y})$ by a disjunction of equations $G(\bar{y} \backslash \hat{y}_{i_j})$ where G is the same as the formula F', but $\hat{y}_{i_j}$ is replaced by $\hat{y}_{i_1} - \Delta_{j_1}$ in one equation, $y_{i_1} - \Delta_{j_1} + 1$ in the next, and so on until $y_{i_1} + \Delta_{j_2}$.

Now we may eliminate variables from each equation in m variables inductively, obtaining at each step a new disjunction consisting of a system of equations in less variables and a set of linear equations of the form $\hat{y}_i = \hat{y}_j + c_i$ which we use to eliminate one variable. At the last level of each branch of this procedure, we will have one of three possible outcomes:

1. All exponential terms have canceled out and we have a false equation with constant terms. In this case there is no solution to (3.6) or (3.5) in this branch.

2. There is an equation $0 = 0$ (i.e. all terms cancel out after a substitution). In this case all variables (after renumbering) $\hat{y}_{i+1}, \ldots, \hat{y}_m$ that remained in the previous step of the branch are taken as free variables, and we obtain a general solution $\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \ldots, \hat{y}_i = \hat{y}_{i+1} + c_i$ to system (3.6) along this branch.

3. There is one equation left of the form $\beta_s k^{y_s} + C = 0$. In this case, this equation has a unique solution $y_s = b$ or no solution.

In the second case, any solution in $\mathbb{Z}$ of the linear system $\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \ldots, \hat{y}_i = \hat{y}_{i+1} + c_i$ will be a solution to system (3.6) since when we substitute the variables into this equation, the same cancellations will occur and we will remain with the equation $0 = 0$. This proves the claim. □

System (3.5) can also be reduced to a disjunction of linear systems by substituting each $\hat{y}_i$ back to the corresponding linear combination of $y_1, \ldots, y_n$. This completes the proof of the lemma. □

System (3.4) is also equivalent to a disjunction of linear systems –we first replace sums appearing in the exponent of k by new variables and then apply Lemma 11. We now solve this disjunction of linear systems –if it is solvable, the general solution will correspond to the disjunction of systems of linear equations on $\hat{X}$. We fix one of these systems and substitute those r_i's that are fixed numbers into system (3.3) that has triangular form. Denote the new tuple of r_i's by $\tilde{X}$.

3.1.2 Algorithm to solve remaining systems

We now describe two procedures: the first will stop if it finds a solution to (3.3), the second will stop if there is no solution.

Procedure 1. If an integer solution to the system (3.3) exists, we can find it by enumerating all integer values of $\tilde{X}, Y, Z$.

Now we will justify the second procedure. We can assume all $y \in Y$ are non-negative. Splitting into several cases as before, we can also assume that all $r \in \tilde{X}$ are non-negative. Then system (3.3) is equivalent to a disjunction of systems

$$z_s k^{-y_s}(\sum_j \delta_{sj} k^{\tau_{sj}(\bar{r})}) = \sum_{i>q} z_i k^{-y_i}(\sum_j \delta_{ij} k^{\sigma_{ij}(\bar{r})}) + \sum_t \gamma_t k^{\tau_t(\bar{r})}, \tag{3.7}$$

where $s = 1, \ldots, q$; $y_j, r_j \in \mathbb{N}$, τ_{sj}, σ_{ij} are linear combinations of elements in $\tilde{X}$ and constants and $\delta_{is}, \delta_{ij}, \gamma_t \in \mathbb{Z}$.

Lemma 12. *Equation $zk^{-y}A = B$, where $A, B \in \mathbb{Z}$ has a solution in $\mathbb{Z}$ if and only if for any prime power p^m with p not dividing k, $m \in \mathbb{N}$, equation $zA = k^y B$ has a solution modulo p^m.*

Proof. If equation $zA = k^y B$ has a solution in $\mathbb{Z}$, then it has a solution modulo p^m for any p not dividing k.

Suppose that equation $zA = k^y B$ has a solution modulo p^m for any p not dividing k. Then every prime power p^m, not dividing k, that divides A also divides B. We can represent $A = A_1 A_2$, where A_1 is the maximal factor relatively prime with k, and let A_3 is such that $A_2 A_3 = k^a$ for some $a \in \mathbb{N}$. Then $zk^{-y} = B/(A_1 A_2) = k^{-a} B A_3 / A_1$ and A_1 divides B. Therefore the equation has a solution in $\mathbb{Z}$. □

Notice that we can multiply each equation of (3.7) by $k^{y_s+\sum_{i>q} y_i}$ and not have negative powers of k on the right side of the equation. Denote this equivalent system by (3.7′).

Lemma 13. *There is an integer solution to system (3.7) if and only if there are values for the variables $\tilde{X} \cup \{z_i, y_i | i > q\}$, for which the system obtained from system (3.7 ′) after substituting these values for variables in $\tilde{X} \cup \{z_i, y_i | i > q\}$ has a solution modulo any prime power p^m for any prime number p not dividing k, and any natural m.*

Proof. If there is an integer solution to system (3.7) then there is a solution modulo p^m for any prime number p not dividing k and any natural m.

Suppose there are values for the variables $\tilde{X} \cup \{z_i, y_i | i > q\}$, for which the system obtained from (3.7) after substituting these values for variables in $\tilde{X} \cup \{z_i, y_i | i > q\}$ has a solution modulo any prime power p^m for any prime number p not dividing k. After we substitute these values, each equation of the system will have the form as in Lemma 12. And by Lemma 12 system (3.7) has an integer solution. □

Lemma 14. *If a prime p does not divide a positive natural number k, then the function k^y, $y \in \mathbb{N}$, is periodic modulo p^m with some period P, namely*

$k^P \equiv 1 (mod\ p^m)$.

Proof. One can compute all possible values of k^y modulo p^m. Suppose these are $V = \{1, \ldots, q\}$. Therefore there are different numbers $P_1 < P_2$ such that $k^{P_1} \equiv k^{P_2} (mod\ p^m)$. Therefore $k^{P_1}(k^{P_2-P_1} - 1) \equiv 0\ (mod\ p^m)$. Since p does not divide k, $k^{P_2-P_1} \equiv 1\ (mod\ p^m)$. This implies that the function k^y, $y \in \mathbb{N}$, is periodic modulo p^m with some period P. □

We can now describe the second procedure.

Procedure 2. Note that one can enumerate all prime powers p^m not dividing k.

We begin by enumerating the first prime power p^m. Let all values of k^y modulo p^m be $V = \{1, \ldots, q\}$. We go through each equation in system (3.7′), substituting each term k^y, k^r by a value in V and each variable z_i by a value in $\{0, \ldots, p^m - 1\}$. Note that this is a finite process since there are finitely many possible solutions and a finite number of systems. If none of the systems has a solution, then system (3.7) does not have a solution. If some of the assignments for $\tilde{X}, Y, Z$ give a solution modulo p^m, then for each such assignment we rewrite the variables in $\tilde{X}$ in the form $r_i = t_i + P\bar{r}_i$, where $t_i \in V$, variables $y_i, i > q$, in the form $y_i = a_i + P\bar{y}_i$, $a_i \in V$, and $z_i, i > q$, in the form $z_i = b_i + p^m\bar{z}_i, 0 \leq b_i < p^m$. Here, $\bar{r}_i, \bar{y}_i$, and $\bar{z}_i$ are new variables. This restricts their domains when considering prime powers on the following steps of the procedure. When we make substitutions for the variables $\tilde{X} = \{r_i\}$ in the terms $\tau_{sj}, \sigma_{ij}, \tau_t$, these terms will then be linear combinations in variables $\{\bar{r}_i\}$. When we make substitutions for the variables in $\{z_i, y_i | i > q\}$, the terms k^{y_i} will then be $k^{a_i + P\bar{y}_i}$. The form of the equation will therefore change slightly, but we may still apply the next step of Procedure 2.

The restrictions on the domains of $\tilde{X} \cup \{z_i, y_i | i > q\}$ guarantee that when considering the prime powers on the subsequent steps of the procedure, we only consider those values of $\tilde{X} \cup \{z_i, y_i | i > q\}$ for which system (3.7′) has solution modulo p^m for all previously considered prime powers p^m.

On each step of the second procedure we obtain a disjunction of possible domains for variables $\tilde{X} \cup \{z_i, y_i | i > q\}$, therefore we have a branching process. If system (3.7) does not have a solution, the second procedure will stop along all the branches.

3.2 Diophantine Problem in restricted wreath products with $\mathbb{Z}$

The restricted wreath product $G \wr \mathbb{Z}$ is isomorphic to the semidirect product $\oplus_{i\in\mathbb{Z}} G \rtimes \mathbb{Z}$, where the action of $\mathbb{Z}$ on $\oplus_{i\in\mathbb{Z}} G$ is by translation of indices, that is, $k \cdot \{g_n\}_{n\in\mathbb{Z}} = \{g_{n+k}\}_{n\in\mathbb{Z}}$. The product of two elements $(\{g_n\}_{n\in\mathbb{Z}}, k) \cdot (\{h_n\}_{n\in\mathbb{Z}}, l)$ is $(\{g_n + h_{n+k}\}_{n\in\mathbb{Z}}, k+l)$. When $G = \mathbb{Z}_2$, the group is called the lamplighter group.

If A is a finitely generated abelian group, then $A = \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$ as an additive group. Denote by R the ring $\mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$. In this case $A \wr \mathbb{Z}$ is isomorphic to the group of matrices of the form

$$M = \begin{pmatrix} t^x & P \\ 0 & 1 \end{pmatrix}$$

where P is a Laurent polynomial in $R[t, t^{-1}]$. Note that $P = f(t)t^{-k}$ where $f(t) \in R[t]$ and $k \in \mathbb{N}$.

We will first show that equations in $A \wr \mathbb{Z}$ are decidable for $A = \mathbb{Z}_n$ and $A = \mathbb{Z}$. We will denote $\mathbb{Z}_n \wr \mathbb{Z}$ by L_n and $\mathbb{Z} \wr \mathbb{Z}$ by L.

Theorem 9. *Equations in L_n are decidable.*

Proof. The product of n elements in L_n is

$$\begin{pmatrix} t^{x_1} & P_1 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} t^{x_n} & P_n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} t^{x_1+\cdots+x_n} & Q \\ 0 & 1 \end{pmatrix}$$

where $P_j = f_j(t)t^{-y_j}$ and

$$Q = f_n(t)t^{-y_n}t^{x_1+\cdots+x_{n-1}} + f_{n-1}(t)t^{-y_{n-1}}t^{x_1+\cdots+x_{n-2}} + \cdots + f_1(t)t^{-y_1}$$

In a system of equations in L_n, some of the $x_i, f_j(t)$ and y_j may be constants and some may be variables.

Moreover,

$$\begin{pmatrix} t^x & f(t)t^{-y} \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} t^{-x} & -f(t)t^{-y-x} \\ 0 & 1 \end{pmatrix}.$$

Thus, any system of equations in L_n is equivalent to a system of equations of the form:

$$F_1(\bar{x}, t, t^{-1})f_1(t)t^{-y_1} + \ldots + F_m(\bar{x}, t, t^{-1})f_m(t)t^{-y_m} = P(\bar{x}, t, t^{-1}) \qquad (3.8)$$

and

$$\sum_i c_i x_i + C = 0 \qquad (3.9)$$

where $F_j(\bar{x}, t, t^{-1}) = \sum_i \alpha_i t^{\sigma_i(\bar{x})}$ where $\alpha_i = \pm 1$, and $\sigma_i(\bar{x})$ is a linear combination of elements in x and a constant, $f_j(t)$ is a variable that runs over $\mathbb{Z}_n[t]$, y_j is a variable that runs over $\mathbb{N}$, and $P(\bar{x}, t, t^{-1})$ is a polynomial in $\mathbb{Z}_n[t, t^{-1}]$ with linear combinations of $\bar{x}$ in the exponents of t and $c_i, C \in \mathbb{Z}$.

3.2.1 Reducing to a system of linear equations

We begin by solving the linear system (3.9) as in Section 3.1. If the system does not have a solution, then then the system of equations in the group will not have a solution either. If the system has a solution, then we substitute the general solution into system (3.8). Denote the set of remaining variables (free variables) by $\tilde{X} = \{x_{i_1}, \ldots, x_{i_n}\}$. Note that if system (3.9) has exactly one solution, then $\tilde{X} = \emptyset$ and after substituting, there will be no occurrences of variables x_i in system (3.8).

Now we solve system (3.8). This system can be put in Smith normal form by regarding the terms $f_j(t)t^{-y_j}$ as variables, the terms $F_j(\bar{x}, t, t^{-1})$ as coefficients, and $P(\bar{x}, t, t^{-1})$ as a constant.

Thus, the system is equivalent to a disjunction of systems of the form:

$$F'_s(\bar{x}, t, t^{-1}) f_s(t) t^{-y_s} = \sum_{i>q} F'_{s_i}(\bar{x}, t, t^{-1}) f_i(t) t^{-y_i} + P'_s(\bar{x}, t, t^{-1}) \tag{3.10}$$

for $s = 1, \ldots, q$, and

$$\sum_i a_i t^{\sigma_i(\bar{x}, d_i)} = 0 \tag{3.11}$$

where $a_i, \in \mathbb{Z}_n$ and $\sigma_i(\bar{x}, d_i)$ is a linear combination of elements in $\bar{x}$ with constants.

Example 1: Consider the following system in L_5 with two variables:

$$f_1(t)t^{-y_1} + (t^{x_1}) f_2(t) t^{-y_2} = 1 - 2t$$

$$(t^{-2}) f_1(t) t^{-y_1} + (t^{x_1 - 2}) f_2(t) t^{-y_2} = 3t^{-3+x_1+x_2} - 2t^{-1} + t^2$$

To put the system in Smith normal form, we multiply the first equation by $-t^{-2}$, add the two equations and replace the second equation by this sum. We get the following system:

$$f_1(t)t^{-y_1} + (t^{x_1})f_2(t)t^{-y_2} = 1 - 2t$$

$$0 = -t^{-2} + 2t^{-1}3t^{-3+x_1+x_2} - 2t^{-1} + t^2$$

The equations are of the form (3.10) and (3.11), respectively. We first show how to solve system (3.11). We begin by grouping terms in each equation such that the sum of the coefficients of each group is zero modulo n. If there is no way to group each equation in the system in this way, then this system does not have a solution. For, suppose there is a solution to system (3.11), then after substituting the solution in each equation and simplifying, the coefficients of each t^i should be zero in each equation, thus the sum of the coefficients of t^i before simplifying must be zero modulo n.

There may be more than one way to group the terms of each equation, in which case we will obtain a disjunction of systems. We fix one system after grouping and for each equation, we set the powers of t in the terms that were grouped together equal to each other, consequently obtaining a system of linear equations.

Example 3. *Consider the equation in L_5:*

$$3t^{3-x_1+x_2} + 4t^{-2+x_1} + 2t^{x_3-2} + 1 = 0$$

can be grouped in the following two ways:

$$(3t^{3-x_1+x_2} + 2t^{x_3-2}) + (4t^{-2+x_1} + 1) = 0$$

$$(3t^{3-x_1+x_2} + 2t^{x_3-2} + 4t^{-2+x_1} + 1) = 0$$

We then obtain two linear systems:

$$3 - x_1 + x_2 = x_3 - 2$$

$$-2 + x_1 = 0$$

and

$$3 - x_1 + x_2 = x_3 - 2 = -2 + x_1 = 0$$

.

We now fix one system of linear equations and solve. If there is no solution, system (3.10) has no solution in this branch. If there is a solution, then we substitute the general solution back into (3.10).

3.2.2 Algorithm to solve remaining systems

To solve system (3.10), we will describe two procedures. The first will halt when a solution to the system is found, the second will halt if there is no solution to the system.

We can rewrite system (3.10) so that all the variables x_i have solutions in $\mathbb{N}$ and so that it is a system of equations over $\mathbb{Z}_n[t]$. We do this by rewriting the system as a disjunction of systems together with a sign assignment on the x_i (as in Section 3.1 in the proof of Lemma 11). We then fix one system and multiply on both sides of each equation of the system by $t^{\sum x_i + \sum y_i + c}$, where the first sum is over all x_i with a negative assignment and c is the sum of all negative constant exponents. We then obtain a system with equations of the form:

$$F'_s(\bar{x},t) f_s(t) t^{\sum_{i>q} y_i} = \sum_{i>q} F'_{i_s}(\bar{x},t) f_i(t) t^{y_s + \sum_{i \neq j, i>q} y_i} + P'_s(\bar{x},t) t^{y_s + \sum_{i>q} y_i} \tag{3.12}$$

for $s = 1, \ldots, q$.

Procedure 1. If a solution to the system exists, we can find it by enumerating and testing all possible solutions. We assign values in $\mathbb{N}$ to the x_i and the y_i, and values in $\mathbb{Z}_n[t]$ to the $f_i(t)$. In L, we follow the same procedure, but instead assign values in $\mathbb{Z}[t]$ to the $f_i(t)$.

Now we justify the second procedure for L_n.

Lemma 15. *Any element $g \in \mathbb{Z}_{p^n}[t]$, where p is a prime number, can be written as $g(t) = p^k \cdot u \cdot m(t)$, where u is a unit, $m(t)$ is a monic polynomial and $k \in \mathbb{N}$.*

Proof. Note first that $g(t)$ can be written as $p^m f(t)$, where $f(t)$ is a regular polynomial (that is, it's not a zero divisor). This can be done by factoring out the maximum power of p so that at least one coefficient is not divisible by p.

Now we show that any regular polynomial $f(t)$ can be written as $f(t) = u \cdot m(t)$, where $m(t)$ is a monic polynomial and u a unit. We will use the same proof as in [Gre10] to show that for any regular polynomial $f(t)$, there is a sequence $\{f_i\}$ of monic polynomials such that

$$f_j = f_{j+1} \mod (p^j)$$

and there is a $g_j \in (p)$ and a unit $b \in \mathbb{Z}_{p^n}$ such that

$$bf = f_j + g_j f_j \mod (p^j)$$

We will define this sequence inductively.

Let $f(t) = \sum_{i=0}^{n} d_i t^i$ be a regular polynomial and let d_u be the coefficient with the highest degree that is a unit. Define $f_1(t) = d_u^{-1}(d_u t^u + \cdots + d_0)$, $g_1 = 0$ and $b = d_u^{-1}$. Now suppose $\{f_i\}_{i=1}^{j}$ satisfies the conditions so that $bf = f_j + g_j f_j + h$ where $h \in (p^j)$. Since f_j is monic, we can find a $q, r \in \mathbb{Z}_{p^n}[t]$ such that $h = f_j q + r$, where the $deg(r) < deg(f_j)$ or $r = 0$. Now we set $f_{j+1} = f_j + r$ and $g_{j+1} = g_j + q$ and we check that the conditions above are satisfied.

If $r = 0$, then we have the result. Suppose $r \neq 0$. Let $f_j = t^u + a_{u-1}t^{u-1} + \cdots + a_0$ and $q = c_s t^s + \cdots + c_1 t + c_0$. The coefficient of x^{s+u} in $f_j q$ is c_s, the coefficient of x^{s+u-1} is $c_{s-1} + a_{u-1}c_s$, and so on. Since $h = 0 \mod (p^j)$ and the $deg(r) < deg(f_j)$, we have that the coefficients $c_s \in (p^j)$ and $c_{s-1} \in (p^j)$ and so on, so $q \in (p^j)$. Then $g_{i+1} = g_i + q$ is in (p) and $r = h - qf_j \in (p^j)$. Therefore, we have that

$$bf = f_j + g_j f_j + h$$

$$= (f_j + r) + (g_j + q)(f_j + r) - rg_j - rq$$

$$= f_{j+1} + g_{j+1} f_{j+1} - r(g_j + q)$$

$$= f_{j+1} + g_{j+1} f_{j+1} \mod (p^{j+1})$$

Finally, note that $f = b^{-1}(1+g_n)f_n$ where f_n is monic, b^{-1} is a unit, and $g_n \in (p)$. Note that $(1+g_n)$ is a unit since its constant term is not a zero divisor.

□

Lemma 16. *Any element $f \in \mathbb{Z}_n[t]$ can be written as $f(t) = \gamma \cdot z \cdot g$ where γ is a zero divisor, z is a unit, and g is a monic polynomial.*

Proof. Note that there is an isomorphism $\sigma : \mathbb{Z}_n[t] \to \mathbb{Z}_{p_1^{k_1}}[t] \times \cdots \times \mathbb{Z}_{p_m^{k_m}}[t]$, where $p_1, \cdots, p_m$ are distinct prime numbers and such that $n = p_1^{k_1} \cdots p_m^{k_m}$, and $k_1, \cdots, k_m \in \mathbb{N}$. Let $f \in \mathbb{Z}_n[t]$ and let $(f_1, \ldots, f_m)$ be its image under σ. Denote $\mathbb{Z}_{p_i^{k_i}}$ by S_i. By Lemma 15, for $i = 1, \ldots, m$ we have that $f_i = p_i^{s_i} \cdot u_i \cdot \bar{f}_i$ where u_i is a unit and $\bar{f}_i$ is a monic polynomial. Set $\gamma_i = (1_{S_1}, \ldots, p_i^{s_i}, \ldots, 1_{S_m})$, $z_i = (1_{S_1}, \ldots, u_i, \ldots 1_{S_m})$, and $g_i = (1_{S_1}, \ldots, \bar{f}_i, \ldots, 1_{S_m})$. Thus we have that $(f_1, \ldots, f_m) = \prod_{i=1}^{m} \gamma_i \cdot z_i \cdot \bar{f}_i$.

Note that the preimages of z and γ will be a unit and a zero divisor, respectively, since σ is an isomorphism. We need only check that the preimages of the g_i are monic polynomials. But this is easy to see, since σ maps a coefficient $1 \mapsto 1 \mod p_i^{k_i}$ which is 1.

□

Lemma 17. *There is an integer solution to system (3.12) if and only if there is a value of $\bar{x}$, $f_i(t)$ and y_i for $i > q$ that is a solution to this system modulo $h(t)$ for any monic polynomial $h(t)$ and in any $\mathbb{Z}_k[t]$, where $k|n$.*

Proof. An integer solution to system (3.12) may fail to exist only if there is a polynomial $h(t)$ in $\mathbb{Z}_n[t]$ that divides some $F'_s(\bar{x}, t)$ in the left side of some of the equations and does not divide the right side. For n prime, $\mathbb{Z}_n$ is a field and it is enough to consider monic polynomials. For n composite, by [Gre10], Lemma 4.6, every polynomial is a product of monic polynomials, a unit and a zero divisor in $\mathbb{Z}_n$. Therefore it is enough to consider monic polynomials and zero divisors in $\mathbb{Z}_n$. Factoring by m that divides n is equivalent to considering (3.12) in $\mathbb{Z}_k[t]$, where $k = m/n$.

□

Procedure 2 for L_n: By Lemma 17, system (3.12) does not have a solution if one of the following happens:

- **Case 1:** For any valuation of $\bar{x}, \bar{y}$ and $f_i(t)$, there is a monic polynomial $h(t) \in \mathbb{Z}_n[t]$ and an $s = 1, \ldots, q$ such that $h(t)$ divides $F'_s(\bar{x}, t)$ but $h(t)$ does not divide the right side of this equation.

- **Case 2:** For any values of $x_i, y_i, f_i(t)$, there is a $k|n$ and an $s = 1, \ldots, q$ such that $F'_s(\bar{x}, t)$ is zero in $\mathbb{Z}_k[t]$ but the right side of this equation is non-zero in $\mathbb{Z}_k[t]$.

We will describe two procedures that will alternate.

Case 1. We fix a monic polynomial $h(t)$ in $\mathbb{Z}_n[t]$. Note that each term $f_i(t)$, $i > q$ in system (3.12) can take finitely many values modulo $h(t)$, namely all polynomials in $\mathbb{Z}_k[t]$ with degree less than $h(t)$. Similarly, because the function t^n is periodic modulo any $h(t)$, then for any term t^{x_i} and t^{y_i} we only have to consider values $\{0, \dots, P-1\}$ for the x_i and y_i, where P is the period of t^n modulo $h(t)$. We then test each possible solution set to see if there is a solution of the system modulo $h(t)$. If some of the possibilities for the $f_i(t), t^{x_i}, t^{y_i}$ work, then we rewrite our variables as follows: the terms $f_i(t)$ can be rewritten as $f_i(t) = r(t) + h(t)\bar{f}_i(t)$, where $r(t)$ is a polynomial in $\mathbb{Z}_k[t]$ with degree less than $h(t)$, and the terms x_i, y_i can be rewritten as $x_i = P\bar{x}_i + c_i$ and $y_i = P\bar{y}_i + d_i$, where P is the period of t^n modulo $h(t)$ and $c_i, d_i < P$. We may get more than one possible solution modulo $h(t)$ so that we have a new disjunction of systems. We continue this process for each monic polynomial in $\mathbb{Z}_n[t]$. If there is no solution, we will find an $h(t)$ for which (3.12) has no solution and the procedure will halt.

Case 2. Every time the coefficient $F'_s(\bar{x}, t)$ in the left side of some equation of system (3.12) is zero modulo k, where $k|n$, we have to exclude the corresponding $\bar{x}$ in the system corresponding to the right side

$$\sum_{i>q} F'_{i_s}(\bar{x}, t) f_i(t) t^{y_s + \sum_{i \neq j, i>q} y_i} + P'_s(\bar{x}, t) t^{y_s + \sum_{i>q} y_i} = 0$$

does not have a solution in $\mathbb{Z}_k[t]$. It has the same form as system (3.10), (3.11). We will run Procedure 2 for this system in $\mathbb{Z}_k[t]$. This will include sub-procedures for $\mathbb{Z}_s[t]$ for divisors s of k and eventually for $\mathbb{Z}_p[t]$ for prime divisors of n. For $\mathbb{Z}_p[t]$ we will only have Case 1. □

Theorem 10. *Equations in L are decidable.*

A system of equations in L reduces to equations of the form (3.8) and (3.9), but the $f_j(t)$ are variables in $\mathbb{Z}[t]$ and $P(\bar{x}, t, t^{-1})$ is a polynomial with coefficients in $\mathbb{Z}$. To solve system (3.11) we group terms whose coefficients add up to 0. Then we reduce this system to system (3.12).

Lemma 18. *There is an integer solution to system (3.12) in $\mathbb{Z}[t]$ if and only if there is a value of $\bar{x}$, $f_i(t)$ and y_i for $i > q$, for which there is a solution to this system in any $\mathbb{Z}_n[t]$, where n is prime.*

Proof. In one direction the statement is obvious. Suppose now that there is no integer solution to system (3.12) in $\mathbb{Z}[t]$. Then for any value of $\bar{x}$, $f_i(t) \in \mathbb{Z}[t]$ and y_i for $i > q$, there is a polynomial $h(t)$ in $\mathbb{Z}[t]$ that divides the left side of one of the equations in system (3.12) and does not divide the right side of this equation. Then the right side of the equation has the form $h(t)g(y) + r(t)$ and there is n such that the images of $h(t)$ and $r(t)$ are not zeros in $\mathbb{Z}_n[t]$. □

The first procedure will be looking for a solution. The second procedure will be looking for a number n and a monic polynomial $h(t) \in \mathbb{Z}_n[t]$ such that for any value of $\bar{x}$, $f_i(t) \in \mathbb{Z}[t]$ and y_i for $i > q$ there is no solution to the system in $\mathbb{Z}_n[t]$ modulo $h(t)$.

Theorem 10 implies the following corollary.

Corollary 9. *The Diophantine problem is decidable in $\mathbb{Z}^n \wr \mathbb{Z}$.*

Proof. Equations in $\mathbb{Z}^n \wr \mathbb{Z}$ have the same form as equations (3.8) and (3.9) in the proof of Theorem 10, with the exception that the terms $f_i(t)$ are in the ring $\mathbb{Z}^n[t]$. Each equation of the form (3.8) is equivalent to n equations, each corresponding to a component of $\mathbb{Z}^n$. Thus, any system of equations in $\mathbb{Z}^n \wr \mathbb{Z}$ is equivalent to a system in $\mathbb{Z} \wr \mathbb{Z}$, so the decidability follows from the decidability of $\mathbb{Z} \wr \mathbb{Z}$. □

Combining Theorems 9 and 10 we obtain the second main result.

Theorem 11. *The Diophantine problem is decidable in $A \wr \mathbb{Z}$, where A is a finitely generated abelian group.*

Proof. Let $A = \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$. Equations in $A \wr \mathbb{Z}$ have the same form as equations (3.8) and (3.9) in the proof of Theorems 9, 10 with the exception that the terms $f_i(t)$ are in the ring $R[t]$. Each system of the form (3.8) is equivalent to several systems, some of them over $\mathbb{Z}$ and some over $\mathbb{Z}_{n_i}$, each corresponding to a component of $\mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$. Solving these systems simultaneously we will solve the original system. $\square$

Bibliography

[BS62] Gilbert Baumslag and Donald Solitar. “Some two-generator one-relator non-Hopfian groups”. In: *Bulletin of the American Mathematical Society* 68.3 (1962), pp. 199–201.

[Chi76] Ian M Chiswell. “Abstract length functions in groups”. In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 80. 3. Cambridge University Press. 1976, pp. 451–463.

[CK12] Montserrat Casals-Ruiz and Ilya Vladimirovich Kazachkov. “Two remarks on the first-order theories of Baumslag-Solitar groups”. In: *Siberian mathematical journal* 53.5 (2012), pp. 805–809.

[Coo17] S Barry Cooper. *Computability theory*. Chapman and Hall/CRC, 2017.

[CR00] Ian M Chiswell and VN Remeslennikov. “Equations in free groups with one variable. I”. In: *Journal of Group Theory* 3.4 (2000), pp. 445–466.

[Dav96] Martin Davis. “The decision problem for exponential diophantine equations”. In: *The Collected Works of Julia Robinson* 6 (1996), p. 77.

[DLS15] Moon Duchin, Hao Liang, and Michael Shapiro. “Equations in nilpotent groups”. In: *Proceedings of the American Mathematical Society* 143.11 (2015), pp. 4723–4731.

[Dur73] Valery Georgievich Durnev. “Positive theory of a free semigroup”. In: *Doklady Akademii Nauk*. Vol. 211. 4. Russian Academy of Sciences. 1973, pp. 772–774.

[Dur95] Valery G Durnev. “Undecidability of the positive $\forall\exists^3$ -theory of a free semigroup”. In: *Siberian Mathematical Journal* 36.5 (1995), pp. 917–929.

[Ers+65] Yu L Ershov, Igor A Lavrov, Asan D Taimanov, and Michael A Taitslin. “Elementary theories”. In: *Russian mathematical surveys* 20.4 (1965), p. 35.

[GG19] Albert Garreta and Robert D Gray. “Equations and first-order theory of one-relator and word-hyperbolic monoids”. In: *arXiv preprint arXiv:1908.00098* (2019).

[GMO16] Albert Garreta, Alexei Myasnikov, and Denis Ovchinnikov. “Properties of random nilpotent groups”. In: *arXiv preprint arXiv:1612.01242* (2016).

[GMO18] Albert Garreta, Alexei Myasnikov, and Denis Ovchinnikov. “Diophantine problems in solvable groups”. In: *arXiv e-prints*, arXiv:1805.04085 (May 2018), arXiv:1805.04085. arXiv: `1805.04085 [math.GR]`.

[Gre10] Ornella Greco. “Unique non-unique factorization”. MA thesis. Royal Institute of Technology (KTB), 2010.

[GS93] Anthony M Gaglione and Dennis Spellman. “Even more model theory of free groups”. In: *Infinite Groups and Group Rings.* World Scientific, 1993, pp. 37–40.

[GT09] Ch K Gupta and Evgenii Iosifovich Timoshenko. “Partially commutative metabelian groups: Centralizers and elementary equivalence”. In: *Algebra and logic* 48.3 (2009), pp. 173–192.

[Hme71] Ju I Hmelevskiĭ. “Systems of equations in a free group. I”. In: *Mathematics of the USSR-Izvestiya* 5.6 (1971), p. 1245.

[Hod93] Wilfrid Hodges. *Model theory.* Cambridge University Press, 1993.

[Kha+10] Olga Kharlampovich, IG Lysënok, Alexei G Myasnikov, and N WM Touikan. “The solvability problem for quadratic equations over free groups is NP-complete”. In: *Theory of Computing Systems* 47.1 (2010), pp. 250–258.

[Khe07] Anatole Khelif. “Bi-interprétabilité et structures QFA: étude de groupes résolubles et des anneaux commutatifs”. In: *Comptes Rendus Mathematique* 345.2 (2007), pp. 59–61.

[KL19] Olga Kharlampovich and Laura López. “Bi-interpretability of some monoids with the arithmetic and applications”. In: *Semigroup Forum.* Springer. 2019, pp. 1–14.

[KLM19] Olga Kharlampovich, Laura López, and Alexei Myasnikov. “Equations in Metabelian Baumslag-Solitar Groups”. In: *arXiv preprint arXiv:1903.10068* (2019).

[KM06] Olga Kharlampovich and Alexei Myasnikov. “Elementary theory of free non-abelian groups”. In: *Journal of Algebra* 302.2 (2006), pp. 451–552.

[KM13] Olga Kharlampovich and Alexei Myasnikov. “Definable sets in a hyperbolic group”. In: *International Journal of Algebra and Computation* 23.01 (2013), pp. 91–110.

[KM19] Olga Kharlampovich and Alexei Myasnikov. “Model Theory in One Relator Groups”. In: *preprint* (2019).

[KM96] O Kharlampovich and A Myasnikov. “Irreducible affine varieties over a free group. 1”. In: *Irreducibility of quadratic equations and Nullstellensatz* (1996).

[KM98] Olga Kharlampovich and Alexei Myasnikov. “Irreducible affine varieties over a free group: II. Systems in triangular quasi-quadratic form and description of residually free groups”. In: *Journal of Algebra* 200.2 (1998), pp. 517–570.

[Lor68] Aivars A Lorencs. “Representations of sets of solutions of systems of equations with one unknown in a free group”. In: *Doklady Akademii Nauk*. Vol. 178. 2. Russian Academy of Sciences. 1968, pp. 290–292.

[Lyn60a] Roger C Lyndon. “Equations in free groups”. In: *Transactions of the American Mathematical Society* 96.3 (1960), pp. 445–457.

[Lyn60b] Roger C Lyndon. “Groups with parametric exponents”. In: *Trans. Amer. Math. Soc* 96 (1960), pp. 518–533.

[Mag30] Wilhelm Magnus. “Über diskontinuierliche Gruppen mit einer definierenden Relation.(Der Freiheitssatz).” In: *Journal für die reine und angewandte Mathematik* 163 (1930), pp. 141–165.

[Mag32] Wilhelm Magnus. “Das Identitätsproblem für Gruppen mit einer definierenden Relation”. In: *Mathematische Annalen* 106.1 (1932), pp. 295–307.

[Mak77] Gennadiy Semyonovich Makanin. “The problem of solvability of equations in a free semigroup”. In: *Matematicheskii Sbornik* 145.2 (1977), pp. 147–236.

[Mak83] Gennadiy Semyonovich Makanin. “Equations in a free group”. In: *Mathematics of the USSR-Izvestiya* 21.3 (1983), p. 483.

[Mal60] AI Malcev. “On a correspondence between rings and groups (Russian)”. In: *Math. Sb* 50.92 (1960), pp. 257–266.

[Mal62] Anatolij I Mal’cev. “On the equation $zxyx^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ in a free group”. In: *Algebra i Logika Sem* 1.5 (1962), pp. 45–50.

[Mar06] David Marker. *Model theory: an introduction.* Vol. 217. Springer Science & Business Media, 2006.

[Mar82] SS Marchenkov. “Unsolvability of positive ∃-theory of free semigroup”. In: *Sibirsky Matematicheskie Jurnal* 23.1 (1982), pp. 196–198.

[Mat71a] Yuri Vladimirovich Matiyasevich. “Diophantine representation of enumerable predicates”. In: *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 35.1 (1971), pp. 3–30.

[Mat71b] Yuri Vladimirovich Matiyasevich. “Diophantine representation of recursively enumerable predicates”. In: *Studies in Logic and the Foundations of Mathematics.* Vol. 63. Elsevier, 1971, pp. 171–177.

[Mer66] Yuri I Merzlyakov. “Positive formulae on free groups”. In: *Algebra i Logika* 5.4 (1966), pp. 25–42.

[Mol91] DI Moldavanskii. “Isomorphism of the Baumslag-Solitar groups”. In: *Ukrainian Mathematical Journal* 43.12 (1991), pp. 1569–1571.

[Nie07] André Nies. “Describing groups”. In: *Bulletin of Symbolic Logic* 13.3 (2007), pp. 305–339.

[Nos84] Gennady A Noskov. “On the elementary theory of a finitely generated almost solvable group”. In: *Mathematics of the USSR-Izvestiya* 22.3 (1984), p. 465.

[Oge91] Francis Oger. “Cancellation and elementary equivalence of finitely generated finite-by-nilpotent groups”. In: *Journal of the London Mathematical Society* 2.1 (1991), pp. 173–183.

[Ozh83] Yuri Igorevich Ozhigov. "Equations with two unknowns in a free group". In: *Doklady Akademii Nauk*. Vol. 268. 4. Russian Academy of Sciences. 1983, pp. 809–813.

[Qui46] Willard V Quine. "Concatenation as a basis for arithmetic". In: *The Journal of Symbolic Logic* 11.4 (1946), pp. 105–114.

[Rem89] VN Remeslennikov. "*exists*-free groups". In: *Siberian Mathematical Journal* 30.6 (1989), pp. 998–1001.

[Rom77] VA Romankov. "Unsolvability of the endomorphic reducibility problem in free nilpotent groups and in free rings". In: *Algebra and Logic* 16.4 (1977), pp. 310–320.

[Rom79] VA Roman'kov. "Equations in free metabelian groups". In: *Siberian Mathematical Journal* 20.3 (1979), pp. 469–471.

[RR67] Hartley Rogers and H Rogers. *Theory of recursive functions and effective computability*. Vol. 5. McGraw-Hill New York, 1967.

[RSS86] Pat Rogers, Howard Smith, and Donald Solitar. "Tarski's problem for solvable groups". In: *Proceedings of the American Mathematical Society* 96.4 (1986), pp. 668–672.

[Sel01] Zlil Sela. "Diophantine geometry over groups I: Makanin-Razborov diagrams". In: *Publications Mathematiques de l'IHES* 93 (2001), pp. 31–105.

[Sel09] Zlil Sela. "Diophantine geometry over groups VII: The elementary theory of a hyperbolic group". In: *Proceedings of the London Mathematical Society* 99.1 (2009), pp. 217–273.

[Sel13] Zlil Sela. "Diophantine geometry over groups VIII: Stability". In: *Annals of Mathematics* (2013), pp. 787–868.

[Sem84] Aleksei Lvovich Semenov. "Logical theories of one-place functions on the set of natural numbers". In: *Mathematics of the USSR-Izvestiya* 22.3 (1984), p. 587.

[Szm55] Wanda Szmielew. "Elementary properties of Abelian groups". eng. In: *Fundamenta Mathematicae* 41.2 (1955), pp. 203–271.