THE BULLETIN OF SYMBOLIC LOGIC
Volume 13, Number 3, Sept. 2007

DESCRIBING GROUPS

ANDRÉ NIES

Abstract. Two ways of describing a group are considered. 1. A group is *finite-automaton presentable* if its elements can be represented by strings over a finite alphabet, in such a way that the set of representing strings and the group operation can be recognized by finite automata. 2. An infinite f.g. group is *quasi-finitely axiomatizable* if there is a description consisting of a single first-order sentence, together with the information that the group is finitely generated. In the first part of the paper we survey examples of FA-presentable groups, but also discuss theorems restricting this class. In the second part, we give examples of quasi-finitely axiomatizable groups, consider the algebraic content of the notion, and compare it to the notion of a group which is a prime model. We also show that if a structure is bi-interpretable in parameters with the ring of integers, then it is prime and quasi-finitely axiomatizable.

CONTENTS

1. Introduction 306
1.1. First-order logic 307
2. FA-presentability 308
2.1. Definition and an example 309
2.2. Interpretations and decidability 310
2.3. Classes of FA-presentable structures 311
2.4. A simple class, and some complex classes 311
2.5. The first-order theory 313
3. FA-presentable abelian groups 313
3.1. Examples 313
3.2. More examples 314
3.3. Some restrictions, via non-embeddability of $(\mathbb{N}, +)^r$ 316
4. Nonabelian FA-presentable groups 320
4.1. Examples 320
4.2. Restrictions on FA-presentable groups 321
4.3. FA-presentable rings 323

Received November 14, 2005.
Partially supported by the Marsden Fund of New Zealand, grant no. UOA-319.

1079-8986/07/1303-0001/$4.50

5. Structures presentable by Büchi automata 324
5.1. Büchi automata 324
5.2. Büchi-presentable structures 324
5.3. Multiple representations of elements 325
6. Quasi-axiomatizable groups 325
7. Quasi-finitely axiomatizable groups 327
7.1. Abelian groups 327
7.2. Nilpotent groups 328
7.3. Metabelian groups 329
7.4. QFA groups with complex word problem 330
7.5. Prime groups 331
7.6. QFA rings 332
7.7. Bi-interpretability with the integers 333

§1. Introduction. How can one describe a countable infinite group using a finite amount of information? The first way one thinks of is to give a finite presentation. But what if the group is not finitely generated? Or if it is finitely generated, but not finitely presented?

Group theory is a discipline blessed with many concrete examples. Whenever one specifies a group, one gives a finite description. For instance, let p be a prime, then the expression "$\mathbb{Z}/_{p\mathbb{Z}} \wr \mathbb{Z}$" describes a group. The ability to understand this description depends on knowing the language used. The notation "$\mathbb{Z}/_{p\mathbb{Z}} \wr \mathbb{Z}$" is short for the natural language description "the restricted wreath product of the cyclic group of order p by $\mathbb{Z}$", and someone who knows those terms is able to recover the group from the description. A considerable part of standard textbooks in group theory, such as [10, 29], is devoted to building up that language, mostly by introducing lots of constructions of new groups from given ones. We will consider two newer approaches to describing groups. They are more restricted, in the sense that the language used is clearly specified.

In the first approach, one describes a group G by representing it in an extremely efficient way, from the computational point of view. A group G is *finite-automaton presentable* if the elements of G can be represented by strings over a finite alphabet, in such a way that the set of representing strings and the group operation can be recognized by finite automata (FA). $(\mathbb{Z}, +)$, with the binary representation of integers and an FA implementing the usual carry bit algorithm is the easiest example of an infinite FA-presentable group. However, most of the interesting examples are not finitely generated. There are several types of abelian examples, but few non-abelian examples at present.

The second approach only applies to finitely generated (f.g.) groups. An infinite f.g. group is *quasi-finitely axiomatizable* (QFA) if there is a description consisting of a single first-order sentence, together with the information that the group is finitely generated. $\mathbb{Z}/_{p\mathbb{Z}} \wr \mathbb{Z}$ is an example of a QFA group that is not finitely presented [19, Thm. 2.3 and Prop. 2.1]. Not every finitely presented group is QFA; any infinite f.g. abelian group is a counterexample.

The properties of being FA-presentable and being QFA are incompatible, and in fact opposite to each other. For instance, the Heisenberg group $\mathrm{UT}_3(\mathbb{Z})$ is QFA but does not even embed into any FA-presentable group. No group can have both properties, since we only consider being QFA for infinite groups. Without that restriction, only the finite groups would be both FA-presentable and QFA. Essentially, both the transition function of the automaton for the group operation and the first-order axiom represent the group table. Note that the length of such a description is at least the cardinality of the group, in fact some polynomial in it, so one could still try to find a shorter description of either type for a finite group. For instance, the cyclic group of order 2^k has an FA-representation with only $O(k)$ states.

The two ways of describing also make sense for other types of structures, for instance rings. Therefore we will be more general and also consider rings and other structures to some extent. No non-trivial examples of FA-presentable rings are known. All finitely generated commutative rings with identity are finitely presented, and Khelif [12] has shown that all entire rings and many others are quasi-finitely axiomatizable. The proof uses the result of Scanlon [31] that each infinite commutative f.g. field is bi-interpretable with the semiring $\mathbb{N}$ and therefore with the ring $\mathbb{Z}$. Such a structure is QFA and prime; see Subsection 7.7.

The paper has two parts that can be read independently, corresponding to the two ways of describing groups.

Part 1: Section 2 introduces FA-presentable structures, Section 3 treats examples and restrictions for abelian FA-presentable groups, and Section 4 does the same for non-abelian groups and for rings. In Section 5 we briefly consider structures of size $2^{\aleph_0}$ which can be represented by Büchi automata.

Part 2: Section 6 gives some background leading to the notion of a QFA group, which is studied in the final Section 7.

Work on this paper started with my talk "Algebras with finite descriptions" given at the 2005 ASL summer meeting in Athens. The support of the organizers of this memorable meeting, especially of Costas Dimitracopoulos, is gratefully acknowledged.

1.1. First-order logic. First-order logic obviously plays an important role in studying QFA structures, but it also is essential for FA-presentable structures, as explained in Subsection 2.2. In the following, a brief introduction to first-order logic is given, mainly aimed at group theorists. The first–order language of groups consists of *formulas* built up in the expected way from equations $t = s$, using brackets, the connectives $\neg, \wedge, \vee, \rightarrow$, and the quantifiers $\exists x, \forall x$. A *sentence* is a formula where every variable is in the range of some quantifier. For a group G, $\mathrm{Th}(G)$ is the set of sentences which hold in G.

Here are some examples of what first-order logic can express in groups. The *commutator* $[x, y]$ is the term $x^{-1}y^{-1}xy$.

The sentence $\forall x \forall y\ [x, y] = 1$ expresses that the group is abelian.
The sentence $\forall u, v \exists r, s, t\ [u, v] = r^2 s^2 t^2$ holds for all groups (via the substitutions $r = u^{-1}v^{-1}$, $s = vuv^{-1}$, $t = v$.)

More generally, a first-order language and analogs of the notions above can be defined for any set of symbols denoting constant, functions, or relations. Such a set of symbols is called a *signature*. For instance, the signature of groups is $\{1, \circ, ^{-1}\}$, and the signature of Boolean algebras is $\{0, 1, ', \vee, \wedge, \leq\}$. We call *atomic formulas* the formulas which do not involve quantifiers or connectives. For instance, "$u \circ v = v \circ u$" is an atomic formula in the first-order language of groups (in the examples above, we have omitted $\circ$ in the usual way). "$1 \leq x' \vee y$" is an atomic formula in the language of Boolean algebras.

If G is a group, if $\psi(x_1, \dots, x_n)$ is a first-order formula with the free variables displayed and $g_1, \dots, g_n \in G$, then $G \models \psi(g_1, \dots, g_n)$ denotes that ψ is satisfied by $g_1, \dots, g_n$ in G. A relation $R \subseteq G^n$ is *first-order definable* if there is a formula $\psi(x_1, \dots, x_n)$ such that

$$R = \{(g_1, \dots, g_n) \colon G \models \psi(g_1, \dots, g_n)\}.$$

For instance, if $\psi(x)$ is the first-order formula $\forall u\,[x, u] = 1$, then $\psi(x)$ defines the center in a group. The commutator subgroup G' is usually not first-order definable (arbitrarily long finite products are not allowed in our language). Sometimes we allow fixed elements from G in ψ, and in that case R is called *first-order definable with parameters.* An example here is the centralizer of an element d of the group, that is, $C(d) = \{x \colon [x, d] = 1\}$.

§2. FA-presentability. This section contains a brief general introduction to FA-presentability, to the extent needed here. For more details, see [13, 30].

A (nondeterministic) finite automaton $\mathcal{A}$ is given by

- a finite nonempty alphabet Σ,
- a finite set of states S,
- a nonempty subset $F \subseteq S$, the set accepting states,
- a start state $s_0 \in S$,
- a transition relation $\delta \subseteq S \times \Sigma \times S$.

A computation of $\mathcal{A}$ on input w begins in state s_0. At each step, it reads another input symbol and attempts to choose a next state permitted by the transition relation. The recognized language is $\{w \in \Sigma^*$: some computation of $\mathcal{A}$ on input w reaches an accepting state$\}$. For an introduction to finite automata see, for instance, [33].

The concept of FA-presentability was introduced by Hodgson [8, 9], who among other things used it to give a new proof of the decidability of Pressburger arithmetic, that is, the theory of $(\mathbb{N}, +)$. The study of FA-presentable structures was carried on in Khoussainov and Nerode [13]. They used the term "automatic structures", but I prefer to avoid this term here, because it can be confused with the term "automatic group" in the sense of Thurston. FA-presentable groups have next to nothing to do with automatic groups, a concept that only applies to finitely generated groups. The only FA-presentable f.g. groups are the abelian-by-finite ones ([28]; see Subsection 4.2 below), while for instance all word hyperbolic groups are automatic. Automatic groups have received considerable attention in the literature; see for instance [3].

2.1. Definition and an example. A structure in a finite signature is **FA-presentable** if for some alphabet Σ, the elements of the domain can be represented by the strings in a regular language $D \subseteq \Sigma^*$, in such a way that finite automata can also check whether the atomic relations given by the first-order language for this signature hold for a tuple of elements $u_1, \dots, u_k$ (an atomic relation is a relation defined by an atomic formula, such as $f(x) = g(y)$ or $Rxf(x)$). For checking the atomic relations, the strings representing the entries u_i of the tuple are written below each other, using stack symbols like

$$\begin{matrix} a \\ b, \\ a \end{matrix} \quad \text{or} \quad \begin{matrix} c \\ b \\ \diamond \end{matrix}$$

with entries in $\Sigma \cup \{\diamond\}$. One pads out the representing strings with a special symbol $\diamond$ at the end to get the same lengths. The formal definition can be found in [13, 30]. Let us see why $(\mathbb{N}, +)$ is FA-presentable. We write numbers in binary, the *least* significant digit first; 0 is represented by the empty string. Thus the alphabet Σ is $\{0, 1\}$, and the domain consists of the strings over $\{0, 1\}$ ending in 1, and the empty string. A finite automaton can check the correctness of the sum, via the usual carry bit procedure, where the carry goes to the right. $\diamond$ is treated like 0. For instance, the automata verifies 5+22=27 by accepting this string:

$$\begin{matrix} 1 & 0 & 1 & \diamond & \diamond & \diamond \\ 0 & 1 & 1 & 0 & 1 & \diamond \\ 1 & 1 & 0 & 1 & 1 & \diamond \end{matrix}$$

The automaton has three states: N (no carry), C (carry) and A (accept). N is the initial state.

Transitions include: $\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}$ from N to N, $\begin{smallmatrix} 1 \\ 1 \\ 0 \end{smallmatrix}$ from N to C, and $\begin{smallmatrix} \diamond \\ \diamond \\ \diamond \end{smallmatrix}$ from N to A (which is the only way to get to the accept state).

PROPOSITION 2.1. (i) *Each finite structure F is FA-presentable.*
(ii) *A finite product of FA-presentable structures is FA-presentable.*

PROOF. (i). Simply let $\Sigma = F$. The domain consists of all words over Σ of length 1. Each atomic relation R is recognized by a three-state automaton, whose transition function leads from the initial state to the accepting state, for all stack symbols corresponding to tuples that are in R, and to the rejecting state, for all other stack symbols.

(ii). It is sufficient to consider two structures and then argue by induction. To represent elements of the product, one uses two tracks, one for the first component and one for the second. The details are in [13, 30]. $\dashv$

Note that one may represent the same element of the given structure by several strings, though the equivalence relation E to represent the same element has to be regular. See Subsection 5.3 for more on this.

2.2. Interpretations and decidability. Interpretations via first-order formulas are introduced in [7, Ch.5]. Roughly speaking, **B** is interpretable in **A** if the elements of **B** can be represented by tuples in a definable relation D on **A**, in such a way that equality of **B** becomes an **A**-definable equivalence relation E on D, and the other atomic relations on **B** are also definable. A simple example is the difference group construction: for instance, $(\mathbb{Z}, +)$ can be interpreted in $(\mathbb{N}, +)$, where the relation D is $\mathbb{N} \times \mathbb{N}$, addition is componentwise and E is the relation given by $(n, m)E(n', m') \Leftrightarrow n + m' = n' + m$. Further examples include the quotient fields, which can be interpreted in the given integral domain, and the group $GL_n(R)$ for fixed $n \geq 1$, which can be first-order interpreted in the ring R. Here, a matrix B is represented by a tuple of length n^2, D is given by the first-order condition that $\det(B)$ be a unit of R, and E simply is equality of tuples. Multiplication of matrices can be expressed in a first-order way from the ring operations.

FA-presentable structures are quite attractive because of the *query evaluation property*: Given an FA-presentation of a structure **A** and a first-order formula φ, possibly with parameters, one can effectively determine an FA recognizing the relation on **A** defined by φ. The proof is by induction over the formula φ. In order to treat the case that $\varphi = \exists x \psi$, one uses that each non-deterministic finite automaton (guessing at the existential witness x) is equivalent to a deterministic finite automaton.

The query evaluation property implies that a structure **B** interpretable in an FA-presentable structure **A** is also FA-presentable. We obtain FA presenting **B** from the presentation of **A** and the collection of formulas used for the interpretation. Also, *model checking* is decidable, namely, one can decide whether $\mathbf{A} \models \varphi(a_1, \dots, a_n)$, given **A**, a formula φ with n free variables and $a_1, \dots, a_n \in \mathbf{A}$. It follows that the first-order theory of an FA-presentable structure is uniformly decidable: given an FA-presentation of a structure **A** and a sentence φ, "$\mathbf{A} \models \varphi$" is decidable. For details see [2].

One may even extend the first-order language by allowing the quantifier $\exists^\infty x$ in the formulas, because any FA-presentation implicitly contains the FA-recognizable relation "x is longer than y", though it is not part of the signature. Then "$\exists^\infty x(...)$" can be replaced by "for all y, there is an x that is longer than y such that (...)".

2.3. Classes of FA-presentable structures. To be FA-presentable seems to be a rather strong restriction on a countable structure. So one would think that if one fixes a sort of structures, like graphs or linear orders, that the class of FA-presentable structures of that sort is very small. But this is not always the case: surprisingly, some classes of FA-presentable structures turn out to be very complex, in the sense of the isomorphism relation; see Theorem 2.3 below. In particular, some classes have many non-isomorphic countable members. We will consider the following sorts of structures, all given by a finite axiom system:

Boolean algebras, graphs, (abelian) groups and rings.

Usually one proves that a class is not too complex by describing all the structures in it. This has been done, for instance, in the case of FA-presentable Boolean algebras. For the classes we are mainly concerned with, namely FA-presentable (abelian) groups and to some extent rings, we cannot determine yet if one of the extremes applies, or if the truth even lies in between. This is so because, first of all, we have to know what is in the class. Obviously, we approach the problem from both sides:

- find examples of FA-presentable structures of the given sort
- prove restrictions on FA-presentable structures of the given sort.

For groups, there have been some recent advances in both directions, as we will see later. But first, we briefly discuss the classification of FA-presentable Boolean Algebras (for details see [14, 30]) and also give some examples of complex classes, namely graphs and semigroups. The rest of this section can be skipped by group theorists.

2.4. A simple class, and some complex classes. Given a finite structure F, the following structure is FA-presentable:

$$F^{(\omega)} = \{g : \mathbb{N} \mapsto F \mid g \textit{ is almost constant}\},$$

with the operations and relations defined componentwise. Just as for the FA-presentation of the structure F itself in Proposition 2.1, the alphabet is F. The domain now consists of all non-empty strings $w_0 \dots w_n$ over F such that $w_{n-1} \neq w_n$ in case that $n > 0$. The string $w_0 \dots w_n$ represents the sequence $w_0 \dots w_n w_n w_n \dots$ in $F^{(\omega)}$, where the last entry is repeated from the position n on. To recognize an atomic relation R by an FA, one programs the transition relation in a way that it checks whether R holds at each component.

Classifying Boolean Algebras. Let F be the 2-element Boolean algebra, then the above shows that $B_{\textit{fin-cof}} = F^{(\omega)}$ is FA-presentable. $B_{\textit{fin-cof}}$ is isomorphic to the Boolean algebra of finite or cofinite subsets of $\mathbb{N}$, Theorem 2.2 (Khoussainov, Nies, Rubin, Stephan [14]). *An infinite Boolean algebra B is FA-presentable iff it is isomorphic to $(B_{\text{fin-cof}})^n$ for some n.*

Note that $\mathrm{Th}(B)$ is decidable, since it is equal to the theory of infinite atomic Boolean Algebras.

The isomorphism problem for FA-presentable Boolean Algebras. Recall from Subsection 2.2 there is a decision procedure for properties of FA-presentable structures that can be formalized using the extra quantifier $\exists^\infty x$.

A finite Boolean algebra is determined by its cardinality. An infinite FA-presentable Boolean algebra $\mathbf{A}$ is determined by the number n such that $\mathbf{A} \cong (B_{\text{fin-cof}})^n$, and n can be obtained effectively: n is the largest number k such that

$\mathbf{A} \models$ "there are k disjoint elements with infinitely many atoms below."

Given an FA-presentation of a structure $\mathbf{A}$ in the signature of Boolean algebras, one can decide if $\mathbf{A}$ is an infinite Boolean algebra, and if so which one. Thus the problem whether two presentations describe the same structure is decidable.

Complex classes. Fix a finite signature, and consider FA-presentations $\mathbf{A}, \mathbf{B}$ of structures which are given by tuples of FA's. The isomorphism problem

$$\{\langle \mathbf{A}, \mathbf{B}\rangle \mid \exists f : \mathbf{A} \cong \mathbf{B}\}$$

is Σ^1_1. We have seen that it is decidable for Boolean algebras. In contrast, it is as hard as possible for graphs.

Theorem 2.3. [14] *The isomorphism problem for FA-presentable graphs is Σ^1_1-complete.*

In fact, the graphs can be chosen connected and without cycles (such graphs are called successor trees).

Proof. We encode the isomorphism problem for computable subtrees X of $(\mathbb{N}^*, \preceq)$ (here $\preceq$ is the prefix ordering), which is Σ^1_1-complete. For each X, we effectively determine an FA presentation of a successor tree A_X, in a way that $X \cong Y \Leftrightarrow A_X \cong A_Y$. Actually, for technical reasons, the trees have to be chosen as subtrees of $(2\mathbb{N})^*$.

We use that $(\mathbb{N}^*, \prec)$ has a nice FA presentation over $\{0, 1\}$: the domain D consists of the empty word λ and words that end in 1. The tuple $n_1 \dots n_k$ is represented by $0^{n_1}1 \dots 0^{n_k}1$. The relation is the prefix ordering of $\{0, 1\}^*$, restricted to D. The recursive tree R is given by a reversible Turing machine T. T halts on $w \in D$ iff w is not in R. The configuration graph of T, where the edges are transitions, is FA-presentable. A_R is obtained form D by attaching computations of T at each element $w \in D$. Also attach finite chains of each length, and add infinitely many isolated chains of each length. Then $w \in R$ iff some infinite chain starts at w. So $R \cong S \Leftrightarrow A_R \cong A_S$. $\dashv$

The proof can be modified to obtain undirected graphs instead of successor trees. These can be coded into the following: commutative associative semigroups, partial orders, and lattices of height 4. The coding preserves FA-presentability, and isomorphism in both directions. For instance, to code an undirected graph into a commutative associative semigroup, the domain is simply the vertex set extended by elements c, d, and for vertices x, y, we let $x \circ y = c$ if there is an edge, and $x \circ y = d$ otherwise.

So the isomorphism problem for FA-presentable structures in any of these classes is Σ^1_1-complete.

2.5. The first-order theory. Besides considering the isomorphism problem, the complexity of a class can to some extent be measured by the computational complexity of its theory. Recall from Subsection 2.2 that, given an FA-presentation A and a sentence ψ, "$A \models \psi$" is decidable. So, if $\mathcal{C}$ is a finitely axiomatizable class, then

$$\mathrm{Th}(\mathcal{C} \cap \text{ FA-presentable}) \text{ is } \Pi^0_1,$$

(that is, its complement is recursively enumerable). How about a lower bound on the complexity? For many interesting classes, like graphs, groups and rings, $\mathrm{Th}(\mathcal{C} \cap \text{finite})$ is Π^0_1-complete, and, in fact, the valid and the finitely refutable sentences are effectively inseparable. In this case, $\mathrm{Th}(\mathcal{C} \cap$ FA-presentable) is Π^0_1-complete as well.

§3. FA-presentable abelian groups.

The theory of finite abelian groups is decidable, so the argument in Subsection 2.5 used for showing that the theory of the FA-presentable structures in the class is complex does not work here. In fact, it is unknown whether the theory of FA-presentable abelian groups is decidable. We approach this class by the examples/restrictions method.

3.1. Examples. We have seen in Subsection 2.1 that $(\mathbb{N}, +)$ is FA-presentable. Then so is $(\mathbb{Z}, +)$, because it can be interpreted in $(\mathbb{N}, +)$; see Subsection 2.2. We give further examples. Let

$$\mathbb{Z}(m) = \mathbb{Z}/_{m\mathbb{Z}},$$

and for $k \in \mathbb{N}, k \geq 2$, let

$$R_k = \mathbb{Z}[1/k] = \{zk^{-i} : z \in \mathbb{Z}, i \in \mathbb{N}\}.$$

PROPOSITION 3.1. *The following abelian groups are FA-presentable*:

(i) $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}(m)$, *the direct sum of countably many copies of* $\mathbb{Z}(m)$,

(ii) *the Prüfer groups* $\mathbb{Z}(k^\infty) = R_k/_{\mathbb{Z}}$, *for any* k,

(iii) R_k, *for any* k.

PROOF. (i) is proved by modifying the argument at the beginning of Subsection 2.4 that $F^{(\omega)}$ is FA-presentable for any finite structure F.

For (ii), first let $k = 2$. Just as for $(\mathbb{N}, +)$, the alphabet is $\{0, 1, \diamond\}$, and elements are represented in binary by strings over $\{0, 1\}$ ending in 1. But this time the *most* significant digit comes first. For instance, the string 001 represents [1/8]. As before, the empty string represents 0. A finite automaton checks the correctness of a sum, via the carry bit procedure, where the carry goes to the left this time. The leftmost carry is ignored.

For instance, the automaton verifies [5/8]+[1/2]=[1/8] by accepting the string

$$\boxed{\begin{array}{ccc} 1 & 0 & 1 \\ 1 & \diamond & \diamond \\ 0 & 0 & 1 \end{array}}.$$

For $\mathbb{Z}(k^\infty)$, one generalizes this to the alphabet $\{0, \dots, k-1, \diamond\}$.

(iii) The following is from [21]. For $R_k^{+,0} = \{x \in R_k : x \geq 0\}$, one puts the FA-presentations for $(\mathbb{N}, +)$ and for $\mathbb{Z}(k^\infty)$ together, but with a non-trivial interaction via the leftmost carry bit. One uses two tracks. The top track is for the integers *in binary* (this will be important at the end of the next subsection), and the bottom track is for the fractional part. For example, if $k = 3$, then the element $14 + \frac{17}{27} \in R_3^{+,0}$ is represented by $\boxed{\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 1 & 2 & 2 & \diamond \end{array}}$. When adding, the carry goes left for the addition of the bottom tracks, and right for the addition of the top tracks. The leftmost carry bit for the addition of the bottom tracks becomes the leftmost one for the top tracks. For instance, the automata verifies $14\frac{17}{27} + 1\frac{2}{3} = 16\frac{8}{27}$ by accepting the string

$$\boxed{\begin{array}{ccccc} 0 & 1 & 1 & 1 & \diamond \\ 1 & 2 & 2 & \diamond & \diamond \\ \hline 1 & \diamond & \diamond & \diamond & \diamond \\ 2 & \diamond & \diamond & \diamond & \diamond \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 2 & \diamond & \diamond \end{array}}.$$

Finally one obtains an FA-presentation of R_k via the difference group construction already used in Subsection 2.2. $\dashv$

Further FA-presentable abelian groups are obtained by taking finite products of any of the examples above. Next, we will discuss substantially different examples.

3.2. More examples. Most of the material in this subsection is from [21]. We give examples of abelian groups that are torsion-free, indecomposable (or even rigid) and of rank 2 or higher. Recall that the (torsion-free) *rank* of an abelian group A is the maximum size of a linearly independent set, and that A is *indecomposable* if A is not of the form $B \oplus C$ for nontrivial groups B, C. We discuss two methods to obtain new FA-presentable abelian groups from given ones.

PROPOSITION 3.2. *Let B be an FA-presentable abelian group, and let A be a abelian group that is a finite index extension of B. Then A is FA-presentable.*

PROOF. A will be written multiplicatively. Fix a set $r_0, r_1, \dots, r_k$ of coset representatives of B in A. There are a function $g: \{0, \dots, k\}^2 \to \{0, \dots, k\}$ and elements $b_{i,j} \in B$ such that $r_i r_j = r_{g(i,j)} b_{i,j}$ for every i and j. We may suppose the FA-presentation of B uses an alphabet Σ such that $0, \dots, k \notin \Sigma$. Let $D \subseteq \Sigma^*$ be the domain of the presentation of B. The FA-presentation of A is via the alphabet $\Sigma \cup \{0, \dots, k\}$. An element of A has the unique form $r_i b$ for some $b \in B$, and is represented by the string iv, where $v \in D$ represents b. Since A is abelian,

$$(r_i b)(r_j c) = r_{g(i,j)} b_{i,j} bc.$$

Hence an FA can check the correctness. ⊣

The hypothesis that A be abelian is necessary. For, recall from Proposition 3.1 that $B = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}(2)$ is FA-presentable. B has uncountably many non-isomorphic extensions A of index 2, so not all are FA-presentable (Nies and Thomas, unpublished). On the other hand, if B, or equivalently A, is f.g., then the hypothesis can be removed. See Theorem 4.1 below.

EXAMPLE 3.3. The following group G, from [4, Ch. XIII, Example 88.2], is FA-presentable. Let $\mathbf{e}_0, \mathbf{e}_1$ be the standard base of $\mathbb{Q}^2$. For $\mathbf{a} \in \mathbb{Q}^2$ and $p \in \mathbb{N}$, let

$$p^{-\infty} a$$

denote the infinite set $\{a, p^{-1}a, p^{-2}a, \dots\}$. Thus $\langle p^{-\infty}\mathbf{a}\rangle_{gp} \cong R_p$ for $\mathbf{a} \neq 0$. Fix distinct primes p_0, p_1, q, and let G be the group generated by $p_0^{-\infty}\mathbf{e}_0$, $p_1^{-\infty}\mathbf{e}_1$ and $q^{-1}(\mathbf{e}_0 + \mathbf{e}_1)$. Then G is indecomposable [4, XIII.88]. G is FA-presentable because the FA-presentable group $\langle p_0^{-\infty}\mathbf{e}_0, p_1^{-\infty}\mathbf{e}_1\rangle_{gp} \cong R_{p_0} \times R_{p_1}$ has finite index in G.

The second method is via amalgams of abelian groups. (In [21] we actually use amalgams of commutative semigroups with the cancellation property to prove the formal details of Example 3.5, since it is easier to work with the presentation of $R_k^{+,0}$ from the proof of Proposition 3.1 than with a presentation of R_k.)

PROPOSITION 3.4. *Let A,B be FA-presented subgroups of an abelian group L. Suppose that $U = \{(x, x): x \in A \cap B\}$ is an FA-recognizable subset of the direct product $A \times B$. Then the subgroup $S = A + B$ of L is FA-presentable.*

PROOF. Clearly S is isomorphic to the amalgam $A \times B/_U$, which can be interpreted in the FA presentable structure $(A \times B, +, U)$ via first-order formulas. Hence S is FA-presentable by Subsection 2.2. ⊣

Two different FA-presentations of R_6. For a first application, let $L = \mathbb{Q}$, $A = R_2$, $B = R_3$. Then $U \cong \mathbb{Z}$ and $S \cong R_6$. The FA-representation obtained is different from the one of R_6 in base 6 outlined above, in the sense that there is no FA-recognizable isomorphism. For, in the representation in base 6, no subgroup isomorphic to R_2 is FA-recognizable.

Next we use the method of amalgams to show that an abelian group from [4, Ch. XIII, Example 88.3] (also [29, 4.4.2]), which modifies the previous example S, is FA-presentable. The group has rank 2 and is *rigid*, namely, the only endomorphisms are the trivial ones, multiplication by an integer. For such a group, each subgroup of finite index is indecomposable and of course has rank 2. So S cannot be obtained from previous examples by taking products or finite extensions.

EXAMPLE 3.5. As before, let $\mathbf{e}_0, \mathbf{e}_1$ be the standard base of $\mathbb{Q}^2$. Fix distinct primes p_0, p_1, q. Let

$$A = \langle p_0^{-\infty}\mathbf{e}_0, p_1^{-\infty}\mathbf{e}_1\rangle_{gp} \text{ and } B = \langle q^{-\infty}(\mathbf{e}_0 + \mathbf{e}_1)\rangle_{gp}.$$

Then $A \cap B = \mathbb{Z}(\mathbf{e}_0 + \mathbf{e}_1)$. It can be shown that the hypotheses of Proposition 3.4 are satisfied, making use of the fact that, in the FA-presentation for any R_k obtained in Proposition 3.1, the integer part is always written in binary. So

$$T = \langle p_0^{-\infty}\mathbf{e}_0, p_1^{-\infty}\mathbf{e}_1, q^{-\infty}(\mathbf{e}_0 + \mathbf{e}_1)\rangle_{gp}$$

is FA-presentable.

These examples can be generalized to arbitrary finite ranks.

3.3. Some restrictions, via non-embeddability of $(\mathbb{N}, +)^r$. At this stage we do not know too many general theorems restricting FA-presentable *abelian* groups. One such restriction is that if $(\mathbb{N}, +)^r$ can be embedded, then $r = O(k)$, where k is the number of states of a (nondeterministic) FA representing the group operation. Since $(\mathbb{N}, +)^r$ embeds into $(\mathbb{Q}^+, \times)$ for each r, this implies the following:

THEOREM 3.6. [14] *$(\mathbb{Q}^+, \times)$, or equivalently, the free abelian group of rank ω, is not FA-presentable.*

The best framework for the non-embeddability of $(\mathbb{N}, +)^r$ for sufficiently large r is provided by the following slightly technical definition. An associative semigroup $(S, \circ)$ is given, and we ask that its operation can be represented as the restriction to some set M of an FA-recognizable ternary relation.

DEFINITION 3.7. *An associative semigroup $(S, \circ)$ is* weakly FA-presentable, *with alphabet Σ and k states, if there is a relation $R \subseteq (\Sigma^*)^3$ that can be recognized by a k-state NFA, and a set $M \subseteq \Sigma^*$ such that $R \cap (M \times M \times \Sigma^*)$ is the graph of a binary operation f on M and*

$$(M, f) \cong (S, \circ).$$

We say that (Σ, M, R) is a weak FA-presentation *of $(S, \circ)$.*

Note that, for any $x, y \in M$, there is a unique $z \in \Sigma^*$ such that $(x, y, z) \in R$, and this element z is also in M. There is no restriction on R outside M, or what kind of subset M is. In particular, we do not ask that M

be FA-recognizable. The definition can be generalized to other structures, but the case of semigroups is what we need. The class of weakly FA-presentable abelian groups is far larger than the class of FA-presentable abelian groups. For instance, for each $k \geq 2$, $R_k \times R_k$ is FA-presentable by Proposition 3.1 (iii), so each subgroup is weakly FA-presentable. There are uncountably many nonisomorphic subgroups [4, pp. 125–126]. We will see further interesting examples of weak FA-presentability in Theorem 3.11 below.

THEOREM 3.8. [22] *Suppose that* $(\mathbb{N}, +)^r$ *is weakly FA-presentable with alphabet* Σ *and* k *states; then*

$$r \leq (k+1)\log_2 |\Sigma|.$$

To prove Theorem 3.8, we need a lemma, a weaker form of which was proved in [14]. Since f in Definition 3.7 is associative, we may handle products of finitely many elements of M in the usual way; thus we write xy for $f(x, y)$. Logarithms are taken with the base 2; in particular, $\lceil \log n \rceil$ is the least $i \in \mathbb{N}$ such that $2^i \geq n$.

LEMMA 3.9. *In the situation of Definition* 3.7, *for each* $s_1, \dots, s_m \in M$, *we have*

$$|\prod_{i=1}^{m} s_i| \leq \max\{|s_i|\colon 1 \leq i \leq m\} + k\lceil \log m \rceil.$$

PROOF. First note that, by the pumping lemma, for each $x, y \in M$,

$$|xy| \leq k + \max(|x|, |y|), \tag{1}$$

otherwise there would be infinitely many z such that $(x, y, z) \in R$.

To prove the lemma, one uses induction on $i = \lceil \log m \rceil$. The lemma clearly holds for $i = 0$ (that is, $m = 1$). If $i > 1$, one writes the product $\prod_{i=1}^{m} s_i$ as a product of two parts u, v that have at most $\lceil m/2 \rceil$ factors each. Since $2^i \geq m \Leftrightarrow 2^{i-1} \geq \lceil m/2 \rceil$, the inductive hypthesis for $i-1$ can be applied to both u and v. ⊣

We now sketch the proof of Theorem 3.8.

PROOF. One uses the "explosion method". First one picks appropriate elements of short length and then one shows that the number of other short elements they generate explodes, because of the freeness of $(\mathbb{N}, +)^r$ as a monoid. The generated elements are short by Lemma 3.9. Usually this gives a contradiction, because the number of strings of lengths $\leq m$ is bounded by $|\Sigma|^{m+1}$. In our case, we do not obtain a contradiction, but rather a bound on the rank r. Since $(M, f) \cong (\mathbb{N}, +)^r$, we may choose elements $a_0, a_1, \dots, a_{r-1}$ which generate M as a monoid. For each $n \geq \max\{|a_i|\colon 0 \leq i \leq r-1\}$ let F_n be the set of all products $\prod_{0 \leq i < r} a_i^{\beta_i}$, where $0 \leq \beta_i < 2^n$ for each i. By

Lemma 3.9, each string representing a term $a_i^{\beta_i}$ has length at most

$$n + k\lceil \log \beta_i \rceil \leq n(1+k),$$

and each string representing a product $\prod_{0 \leq i < r} a_i^{\beta_i}$ has length at most $n(1+k) + k\lceil \log r \rceil$. Since all the 2^{nr} products are distinct, we have

$$2^{nr} \leq |F_n| \leq |\Sigma|^{(1+k)n + k\lceil \log r \rceil + 1}.$$

Thus $r \leq \log|\Sigma|\,[(1+k) + (\lceil \log r \rceil k + 1)/n]$. Since n can be chosen arbitrarily large, this shows that $r \leq (k+1)\log|\Sigma|$. ⊣

It is not known whether more complex variants of the abelian groups in Proposition 3.1 are FA-presentable. How about groups like $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}(2^i)$? The most striking case where FA-presentability is unknown is the following.

Question 3.10. *Is* $(\mathbb{Q}, +)$ *FA-presentable*?

One can ask the same question for $(\mathbb{Q}/\mathbb{Z}, +)$. The explosion method cannot be used here to provide a negative answer, because of the following unpublished result of F. Stephan and independently J. Miller.

Theorem 3.11. $(\mathbb{Q}/\mathbb{Z}, +)$ *and* $(\mathbb{Q}, +)$ *are weakly FA-presentable.*

Proof. Each rational $q \in [0, 1)$ has a unique factorial expansion

$$q = \sum_{i=2}^{n} a_i / i!,$$

where a_i is natural number such that $0 \leq a_i < i$. For instance, $5/6 = 1/2! + 2/3!$. (To prove this, let $q = r/n!$ where $r < n!$. If $r \geq n$, then let $r = nr' + k$, $0 \leq k < n$, $r' < (n-1)!$. Thus $q = r'/(n-1)! + k/n!$. Now repeat for r', and so on, as long as needed.)

Addition of factorial expansions is done by a carry procedure. To compute the factorial expansion $\sum_{i=2}^{n} d_i/i!$ of the fractional part of the rational $\sum_{i=2}^{n} a_i/i! + \sum_{i=2}^{n} b_i/i! = \sum_{i=2}^{n} (a_i + b_i)/i!$, at position i, $2 \leq i \leq n$ we have a carry-in $c_{i+1} \in \{0, 1\}$ (where $c_{n+1} = 0$). If $a_i + b_i + c_{i+1} \geq i$ then

$$(a_i + b_i + c_{i+1})/i! = 1/(i-1)! + (a_i + b_i + c_{i+1} - i)/i!,$$

so we have a carry-out $c_i = 1$, and let $d_i = a_i + b_i + c_{i+1} - i$. Otherwise the carry-out c_i is 0 and $d_i = a_i + b_i + c_{i+1}$.

Consider the following set D of strings u of stack symbols. The strings have the form

$$\begin{array}{ccccccccc} \# & a_2 & \# & a_3 & \# & \dots & \# & a_n & \# \\ \# & i_2 & \# & i_3 & \# & \dots & \# & i_n & \#\text{'} \end{array}$$

where a_k, i_k are numbers in reverse binary, possibly with filler symbols $\diamond$ at the end, and $a_k < i_k$. The FA-recognizable relation R holds for strings $u_0, u_1, u_2 \in D$ if all three have the same lower track, and the top track of u_2 is obtained by adding the top tracks of u_0, u_1 according to the carry procedure.

The FA uses the lower track to see if there is a carry-out. The leftmost carry is ignored. Now let

$$M = \{u \in D\colon i_k = k \text{ for each } k,\ 2 \leq k \leq n\}$$

(a set that is clearly not FA-recognizable). Then $(\mathbb{Q}/_{\mathbb{Z}}, +) \cong (M, f)$, where f is the binary operation on M whose graph is given by R.

For $(\mathbb{Q}, +)$, one combines this with an FA-representation of $(\mathbb{Z}, +)$, similar to the way it was done in Proposition 3.1. ⊣

For each prime p, the factorial representation of $1/p$ is a sum of length $p-1$, because p does not divide $i!$ for $i < p$. This is much longer than in the usual representations in number systems, where the length is $O(\log p)$. This enormous length is necessary for infinitely many primes (up to a logarithmic factor), by a result of F. Stephan and its corollary below. Since Stephan's result has not appeared in print, it will be presented here with a full proof. The proof exploits what can be saved of the explosion method in the case of $(\mathbb{Q}, +)$.

For a positive rational q, $|q|$ denotes the length of q in the given weak FA-presentation, not the absolute value.

THEOREM 3.12 (F. Stephan, 2003). *Assume that* $(\mathbb{Q}, +)$ *is weakly FA- presentable, via* (Σ, M, R). *Let*

$$E_n = \{1/p\colon p \text{ prime} \wedge |1/p| \leq n\}.$$

Then $|E_n| = o(n)$.

COROLLARY 3.13. *In any possible weak FA-presentation of* $(\mathbb{Q}, +)$, *for infinitely many primes* p,

$$1/p \textit{ has length} > p/_{2\log_e p}.$$

To obtain the Corollary, let p_k be the k-th prime and note that, by the prime number theorem, for each $\epsilon > 0$ and all sufficiently large k,

$$k \geq (1-\epsilon)p_k/_{\log_e p_k}.$$

Suppose for a contradiction that there is k_0 such that $1/p_k$ has length $\leq$ $p_k/2\log_e p_k$ for each $k \geq k_0$. Let $n_k = \lceil p_k/2\log_e p_k \rceil$, then $|S_{n_k}| \geq k - k_0$. By the prime number theorem, for all sufficiently large k we have $k - k_0 \geq n_k$. Thus $|S_{n_k}| \geq k - k_0 \geq n_k$, contrary to the Theorem.

We now prove Theorem 3.12.

PROOF. We write (M, f) additively since it is the image of $(\mathbb{Q}, +)$. Logarithms are taken to base $|\Sigma|$.

Let $u_0, u_1, \ldots$ be a listing of the prime numbers, in a way that $1/_{u_i} \leq$ $1/_{u_{i+1}}|$ for each i. Note that for each $m \in \mathbb{N}$, all the sums $\sum_{i<m} a_i/_{u_i}$ are distinct, where $(a_i)_{i<m}$ is a tuple of natural numbers such that $0 \leq a_i < u_i$.

To establish the Theorem, given $d \in \mathbb{N}$, we show that

$$\text{for almost all } n,\ |E_n| \leq (2n+2)/_{\log d}.$$

Given n, let $e_n = |E_n|$, so that $E_n = \{u_0, \dots, u_{e_n-1}\}$ by the choice of the sequence (u_i). Also $\lim_n e_n = \infty$. If n is so large that $e_n \geq d$, then there are at least d^{e_n-d} distinct sums of the form

$$\sum_{i<e_n \wedge d \leq u_i} a_i/u_i, \text{ where } a_i < d.$$

Next we estimate the length of a string representing such a sum, using Lemma 3.9 (but remember that M is written additively).

term	*bound on length*
$1/u_i$	n
a_i/u_i	$n + k\lceil \log d \rceil$
$\sum_{i<e_n \wedge d \leq u_i} a_i/u_i$	$L = n + k\lceil \log d \rceil + k\lceil \log e_n \rceil$

Since there are at least d^{e_n-d} distinct sums, we obtain $d^{e_n-d} \leq |\Sigma|^{L+1}$, or

$(e_n - d)\log d \leq n + 1 + k\lceil \log d \rceil + k\lceil \log e_n \rceil$, so
$e_n \leq (n+1)/\log d + d + k(2 + \lceil \log e_n \rceil / \log d)$.

If we actually pick n so large that $d \leq e_n/4$ and

$k(2 + \lceil \log e_n \rceil / \log d) \leq e_n/4$,

then we obtain $e_n/2 \leq (n+1)/\log d$, as required. ⊣

The same proof works for $\mathbb{Q}/\mathbb{Z}$, and a modification yields the corresponding result for the group $\bigoplus_{p \text{ prime}} \mathbb{Z}/p\mathbb{Z}$. Here one replaces $1/p$ by a generator of $\mathbb{Z}/p\mathbb{Z}$.

§4. Nonabelian FA-presentable groups.

4.1. Examples. If $\mathcal{C}$ is a class of groups closed under subgroups, one says that G is $\mathcal{C}$- *by-finite* if G has a subgroup of finite index in $\mathcal{C}$. Equivalently, one can require that G has a *normal* subgroup of finite index in $\mathcal{C}$.

If B is of finite index in A then A is f.g. iff B is. So the following theorem shows that in Proposition 3.2, one can remove the hyothesis that A is abelian in case the subgroup B is abelian and finitely generated.

THEOREM 4.1. [28] *Any f.g. abelian-by-finite group A is FA-presentable.*

PROOF. There is a subgroup $B \cong \mathbb{Z}^m$ that is normal in A. Then, for each $r \in A$, the action of r on B by conjugation is an automorphism of B, and hence given by multiplying argument $x \in \mathbb{Z}^m$ by a fixed matrix $R \in \mathrm{GL}_m(\mathbb{Z})$. The map $x \mapsto Rx$ is definable when viewed as a $2m$-ary relation on $(\mathbb{Z}, +)$, and hence can be recognized by an FA.

We modify the proof of Proposition 3.2, using the natural FA-presentation of $B \cong \mathbb{Z}^m$ given by Proposition 2.1 (ii). The only change is that now we have the identity

$$(r_i b)(r_j c) = r_{g(i,j)} b_{i,j} (r_j^{-1} b r_j) c,$$

which can be verified by an FA because of the remarks above. ⊣

For instance, the following non-abelian f.g. groups are abelian-by-finite and therefore FA-presentable.

EXAMPLES 4.2. (i) The dihedral group $D_{2\infty}$, given by the presentation $\langle a, d \mid d^2 = 1, d^{-1}ad = a^{-1}\rangle$.
(ii) The extension of $\mathbb{Z}$ by $\mathbb{Z}$ given by $\langle a, d \mid d^{-1}ad = a^{-1}\rangle$.

The group in (ii) is torsion free. In [22, Section 3], we give an example of an infinite f.g. abelian-by-finite group that coincides with its commutator subgroup.

4.2. Restrictions on FA-presentable groups. Each FA-presentable group is locally abelian-by-finite. In more detail:

THEOREM 4.3. [22] *Let G be an FA-presentable infinite group. Then each finitely generated subgroup H of G is abelian-by-finite. Moreover, the torsion-free rank of the abelian part of H is at most*

$$\log(|\Sigma|)(k+1),$$

where Σ is the alphabet of the FA-presentation of G, and k is the number of states of a nondeterministic FA recognizing the group operation.

Here the torsion-free rank is the maximum rank of a free abelian group that can be embedded.

The Theorem extends work of Oliver and Thomas [28], who showed that each finitely generated FA-presentable group is abelian-by-finite (and also the converse, Theorem 4.1 above). Theorem 4.3 would be an immediate consequence of the result in [28] if for each FA-presentation of a group G and for each finitely generated subgroup S of G, the set of representations of elements of S was FA-recognizable. However, a counterexample can be derived from recent work of Akiyama et al. [1]: for each prime $q > 1$, there is an FA-presentation of the abelian group $R_q = \{zq^{-i} \colon z \in \mathbb{Z}, i \in \mathbb{Z}\}$ where the representations of integers do not form an FA-recognizable subset (see [22] for more details). Recently, in [21] an FA-presentation of $\mathbb{Z} \times \mathbb{Z}$ was given where no non-trivial cyclic subgroup is FA-recognizable.

To give an idea of the proof of Theorem 4.3, recall the definition of nilpotent groups. Let $Z(G)$ denote the center of a group G. G is nilpotent of class 1 iff G is non-trivial and abelian. G is nilpotent of class $c+1$ iff $G/Z(G)$ is nilpotent of class c. We also need a version of the Heisenberg group, namely $\mathrm{UT}_3(\mathbb{Z}) = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$, which is isomorphic to the rank 2 free nilpotent group of class 2.

PROOF. *Step 1*. The argument begins as in [28]. By Lemma 3.9, any subgroup $H \leq G$ generated by $\{g_1, \ldots, g_r\}$ has polynomial growth, namely

$$\{t(g_1, \ldots, g_r) \colon t \in F(x_1, \ldots, x_n) \wedge |t| \leq n\}$$

has size polynomial in n. So by a deep result of Gromov [5], H is nilpotent-by-finite. If $G = H$, that is, when G itself is f.g. then one can now argue as follows: if G is not abelian-by-finite, then, by [23], G has an undecidable theory. But the theory of an FA-presentable structure is decidable, so G is abelian-by-finite. This is how the argument in [28] concludes.

Step 2. Instead we use the "Heisenberg alternative", which is not hard to verify using standard results on nilpotent groups: a f.g. nilpotent-by-finite group either embeds $\mathrm{UT}_3(\mathbb{Z})$ or is abelian-by-finite.

Step 3. The main new ingredient is to show that no group G in which $\mathrm{UT}_3(\mathbb{Z})$ can be embedded is FA-presentable: otherwise, we would obtain a weak FA-presentation of $(\mathbb{N}, \times)$, which cannot exist by Theorem 3.8. Here are some more details for this last step.

Recall that $[x, y]$ denotes the commutator $x^{-1}y^{-1}xy$, and that $C(x)$ is the centralizer of x. Note that $\mathrm{UT}_3(\mathbb{Z})$ has a presentation

$$\langle a, b, q \colon [a, b] = q, [a, q] = [b, q] = 1\rangle,$$

where

$$a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } q = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $[a^m, b^n] = q^{mn}$ for each $m, n \in \mathbb{Z}$. Mal'cev [16] uses these facts to interpret $(\mathbb{Z}, \times)$ in $\mathrm{UT}_3(\mathbb{Z})$. The domain is the center $\langle q\rangle_{gp}$. An integer m is represented by q^m. To define multiplication in a first-order way on $\langle q\rangle_{gp}$, with extra constant symbols for a, b, he uses the formula

$$\mu(x, y, z; a, b) \equiv \exists u, v \in C(q) \quad (x = [u, b] \wedge y = [a, v] \wedge z = [u, v]). \tag{2}$$

If $x = q^m$ and $y = q^n$, where $m, n \in \mathbb{Z}$, then $\mu(x, y, q^{mn}; a, b)$ holds in $\mathrm{UT}_3(\mathbb{Z})$, via the witnesses $u = a^m$ and $v = b^n$.

Now suppose for a contradiction that $\mathrm{UT}_3(\mathbb{Z})$ can be embedded into the FA-presentable group G. We view a, b, q as elements of G, and use a variant of Mal'cev coding to obtain a weak FA-presentation (Σ, M, R) of $(\mathbb{N}, \times)$, where Σ is the alphabet used for the FA-presentation of G, and $M = \{q^m \colon m \in \mathbb{N}\}$. To obtain R, one could simply try the ternary relation defined by μ in G, which can be FA-recognized by the query evaluation property in Subsection 2.2. However, μ only works in $\mathrm{UT}_3(\mathbb{Z})$, and could well become inadequate in the larger group G, because of undesired witnesses u, v. It turns out that these undesired witnesses can be avoided by adding the extra condition $C(b) \subseteq C(v)$ in the definition μ. The extra condition is satisfied for the intended witnesses, since they are of the form b^n, and $C(b) \subseteq C(b^n)$. $\dashv$

EXAMPLE 4.4. Consider the group G presented as follows. The generators are x, y_i, z_i $(i \in \mathbb{N})$, and the relations are

– $y_i^2 = z_i^2 = 1$, $[y_i, y_j] = [z_i, z_j] = 1$
– $z_i^{-1} x z_i = x y_i$
– $[z_i, y_j] = 1$ and $[y_j, x] = 1$ for any i, j.

This group is FA-presentable [22]. The maximum rank of a free abelian subgroup is 1. For instance, $U = \langle x \rangle_{gp}$ is such a subgroup. Note that U is not normal in G, in fact it has infinite index in its normal closure $\langle \{x\} \cup \{y_j : j \in \mathbb{N}\} \rangle_{gp}$. G has an abelian subgroup of finite index, namely $\langle \{x^2\} \cup \{z_i, y_i : i \in \mathbb{N}\} \rangle_{gp}$.

Much work remains to be done. We do not know any FA-presentable group other than the ones obtained by taking finite products of groups that are abelian-by-finite or a direct power of a finite group G (or some obvious variant of the latter, like the sequences of elements of G that are eventually constant). More specifically,

QUESTION 4.5. *Is each torsion-free FA-presentable group abelian-by-finite*?

QUESTION 4.6. *Is there an infinite FA-presentable group that is simple*?

4.3. FA-presentable rings. All rings will be rings with identity. *No* nontrivial examples are known, but we have some restrictions. For instance, in [14] it is shown that no infinite commutative ring without divisors of zero is FA-presentable (a ring has no divisors of zero if $xy = 0$ implies $x = 0$ or $y = 0$). As an application of the restriction on FA-presentable groups imposed by Theorem 4.3, we obtain a further limiting result for rings with identity. A ring R is *locally finite* if each finite subset generates a finite subring. For instance, the Boolean algebra $B_{\text{fin-cof}}$ from Subsection 2.4 can be viewed as an (FA-presentable) ring, which is locally finite. Not much is known about such rings. One easy fact is that, if $(R, \times)$ is locally finite as a semigroup, then R is already locally finite as a ring (see [22, Rmk. 4.5] for more details).

THEOREM 4.7. [22] *If R is an FA-presentable ring, possibly noncommutative, then R is locally finite.*

PROOF. $\mathrm{GL}_3(R)$ can be interpreted in R, as outlined in Subsection 2.2, and therefore is FA-presentable. If S is an infinite finitely generated subring of R, then let $H \leq \mathrm{GL}_3(R)$ be the group generated by the transvections over S (a transvection is a matrix whose main diagonal is 1 and that has at most one other non-zero entry, which is in S). Then H is f.g. One shows that H is not abelian-by-finite, which contradicts Theorem 4.3.

COROLLARY 4.8. *The only FA-presentable rings* (*commutative or not*) *without zero divisors are the finite fields.*

PROOF. Each finite ring without zero divisors is a division ring, and hence a field (Wedderburn's Theorem), so by Theorem 4.7, any FA-presentable ring without zero divisors is commutative. Now use the result from [14] mentioned at the beginning of this subsection.

QUESTION 4.9. *Are there FA-presentable commutative rings other than obvious variants of* $R^{(\omega)}$, *where* R *is a finite ring*?

(Obvious variants are, for instance, the sequences of elements of R that are eventually constant.) If so, we would also obtain further examples of FA-presentable groups, for instance the ones of the form $\mathrm{GL}_n(R)$ and $\mathrm{UT}_n(R)$.

§5. Structures presentable by Büchi automata. Büchi-presentable structures are a promising field of future research. They were first considered by Hodgson [9], who called them ω-automatic structures.

5.1. Büchi automata. A Büchi automaton is a (nondeterministic) finite automaton that takes as inputs infinite strings over its alphabet Σ. The recognized language is $\{w \in \Sigma^\omega$: *some computation of* $\mathcal{A}$ *infinitely often enters an accepting state when reading* $w\}$. See [34] for details on Büchi automata. Büchi proved that a language $L \subseteq \Sigma^\omega$ is Büchi-recognizable iff L is a finite union of languages of the form UV^ω, where $U, V \subseteq \Sigma^*$ are regular (see [34, Thm. 1.1]). If $V \subseteq \Sigma^*$ is nonempty and regular, then $|V^\omega| < 2^{\aleph_0}$ implies $V^\omega = \{\gamma\}^*$ for some finite string γ. (To see this, consider the equivalence relation on finite strings given by $\alpha \sim \beta \Leftrightarrow \exists i, j\ \alpha^i = \beta^j$. It can be shown that each equivalence class is of the form $\{\gamma\}^*$ for some γ. If $|V^\omega| < 2^{\aleph_0}$ then any two strings in V are equivalent, so $V^\omega = \{\gamma^\omega\}$ where $\{\gamma\}^*$ is the equivalence class containing V.)

Büchi's Theorem says that a subset of Σ^ω is Büchi-recognizable iff it is definable in $S1S_\Sigma$, the monadic second-order language of one successor over Σ (see [34, Thm. 3.1]). In particular, the Büchi-recognizable sets are closed under taking complements.

5.2. Büchi-presentable structures. By adapting the definition of FA-presentability, we obtain the notion of Büchi-presentability for structures (such structures are also called ω-automatic). Among the uncountable structures, an example of a Büchi-presentable structure is the Boolean algebra $(\mathcal{P}(\mathbb{N}), \emptyset, \mathbb{N}, \cup, \cap, ')$. Here the alphabet is $\{0, 1\}$, and we identify subsets of $\mathbb{N}$ with elements of $\{0, 1\}^\omega$. Other natural examples include $(\mathbb{R}, +)$, $(\mathbb{Z}_p, +)$, the p-adic integers under addition for a prime p, and $(\mathbb{Q}_p, +)$, the p-adic numbers under addition. The latter was obtained in [9, p. 53]. One can use a variant of the presentation of R_p given in Proposition 3.1 (iii). $(\mathbb{R}, +)$ and $(\mathbb{Q}_p, +)$ are interesting because both are the abelian group of a $\mathbb{Q}$-vector space of dimension $2^{\aleph_0}$, while it is unkown whether $(\mathbb{Q}, +)$ is FA-presentable; see Question 3.10.

Using methods from the proof of Büchi's Theorem, it can be shown that the nice properties of FA-presentable structures discussed in Subsection 2.2, like query evaluation and the decidability of theory, also hold for Büchi-presentable structures. See [2] for more details.

5.3. Multiple representations of elements. For both FA-presentability and Büchi-presentability, one may represent an element of the given structure by different strings; the equivalence relation E to represent the same element has to be FA-recognizable, or Büchi-recognizable, respectively. For instance, since the class *Fin* of strings in $\{0,1\}^\omega$ that are 0 from some position on is Büchi-recognizable, the dense Boolean algebra $\mathcal{D} = \mathcal{P}(\mathbb{N})/_{Fin}$ obtained by taking the quotient modulo this ideal of finite sets is Büchi-presentable. Since each Boolean algebra can be viewed as a commutative ring with identity, one also obtains interesting examples of non-abelian Büchi-presentable groups, for instance $GL_n(\mathcal{D})$ for fixed $n \geq 2$ (see Subsection 2.2). In contrast, no interesting examples of FA-presentable non-abelian groups are known at present; see the end of Subsection 4.2.

Allowing multiple representations of elements is natural and notationally convenient, but it can be avoided for FA presentations. Here, one implicitly has the length-lexicographical ordering of strings as a part of the presentation. This ordering is a wellordering of type ω, so, to avoid multiple representations of an element, one can modify the presentation, picking the least string from each equivalence class of E. For Büchi-presentable structures, it is not known at present whether multiple representations of elements can be avoided (the proof of a claim made to this end in [2] turned out to be incorrect). Note that by [32] the cardinality of a Büchi-presentable structure is either $2^{\aleph_0}$ or $\leq \aleph_0$, since the equivalence relation to represent the same element is Borel (even G_δ). However, it is not known whether in the countable case, the structure is already FA-presentable. (Added in proof: Barany, Kaiser and Rubin have announced an affirmative answer.)

§6. Quasi-axiomatizable groups.

We leave FA-presentable groups behind, and head towards the second manner of describing groups. To give some background, in this section we discuss to what extent a f.g. group is determined by its whole first-order theory. $\mathrm{Th}(G)$ contains the information whether G is nilpotent, or is torsion-free. However, many properties are not formalizable in first–order logic. For instance: being finitely generated, having the maximum condition (every subgroup is f.g.), and being simple. A first-order property of a group G is distinguished by the fact that it is *intrinsic*. One does not have to go beyond G (the elements and their relations) to verify it, while a property like the maximum condition also depends on the subsets of G, and therefore on the set-theoretical context.

If G is f.g. and infinite, to what extent is G determined by $\mathrm{Th}(G)$? That is, suppose $\mathrm{Th}(H) = \mathrm{Th}(G)$, which extra conditions are needed to conclude that $H \cong G$?

Recall from model theory that for groups U, V, we say that U is a proper elementary submodel of V, written $U \prec V$, if U is a proper submodel of V and the identity embedding of U into V preserves satisfaction of first order formulas (see [7]). Since G is infinite, there is a countable model H of $\mathrm{Th}(G)$ that is not finitely generated, namely $H = \bigcup G_i$, where

$$G = G_0 \prec G_1 \prec G_2 \prec \cdots$$

For each n, G_{n+1} is a countable model of the theory consisting of the elementary diagram of G_n, together with $\{c_{n+1} \neq \underline{g} \colon g \in G_n\}$, where c_{n+1} is a new constant symbol. In other words, we obtain G_{n+1} by adding a nonstandard element to G_n.

But, maybe, G is the only *finitely generated* model of $\mathrm{Th}(G)$?

DEFINITION 6.1. *An infinite f.g. group G is* quasi-axiomatizable *if, whenever H is a* f.g. *group with the same theory as G, then $G \cong H$.*

All f.g. abelian groups G are quasi-axiomatizable. For instance, $\mathbb{Z}^n$ is the only f.g. group G such that G is abelian, torsion free, and $|G \colon 2G| = 2^n$. These properties can be captured by an infinite axiom system.

A similar fact can be proved for torsion free nilpotent groups of class 2, but it breaks down at class 3. Here the whole theory is not always expressive enough to distinguish a particular one among the f.g. groups.

THEOREM 6.2 (Hirshon [6] and Oger [25]). (i) *Each f.g. torsion-free class-2 nilpotent group is quasi-axiomatizable.*

(ii) *There are f.g. torsion-free class-3 nilpotent groups G, H such that $\mathrm{Th}(G) = \mathrm{Th}(H)$, but $G \not\cong H$.*

Oger's part was to show that, for f.g. nilpotent G, H,

$$\mathrm{Th}(G) = \mathrm{Th}(H) \Leftrightarrow G \times \mathbb{Z} \cong H \times \mathbb{Z}.$$

The direction "$\Leftarrow$" is actually true for any groups G, H. Hirshon had asked for which groups A one can cancel $\mathbb{Z}$ from a direct product $A \times \mathbb{Z}$, in the sense that for each group B,

$$A \times \mathbb{Z} \cong B \times \mathbb{Z} \Rightarrow A \cong B.$$

This is true for any group A which is f.g. torsion-free *class-2* nilpotent, but not always true when A is f.g. torsion-free *class-3* nilpotent.

We need the hypothesis in Theorem 6.2 (i) that the group be torsion free: Zil'ber [35] showed that there are f.g. class-2 nilpotent groups G, H such that $\mathrm{Th}(G) = \mathrm{Th}(H)$, but $G \not\cong H$. Extending this, Oger [24, Cor. 5.6] showed that the class-2 nilpotent abelian-by-finite groups

$$G = \langle a, d \mid a^{25} = 1, d^{-1}ad = a^6 \rangle \text{ and } H = \langle a, d \mid a^{25} = 1, d^{-1}ad = a^{11} \rangle$$

have the same first-order theory. These groups had been studied previously, as an example of a pair of class-2 nilpotent groups that have the same finite quotients but are not isomorphic.

§7. Quasi-finitely axiomatizable groups. Now we are ready to discuss the case that a single first-order axiom is sufficient to distinguish a group among all the f.g. groups. Though the following concept was introduced in [19] for groups only, it makes sense for each structure in a finite signature. A first-order axiom provides a finite description of the structure, given the extra information that the structure is f.g.

DEFINITION 7.1. *Fix a finite signature. An infinite f.g. structure G is* quasi-finitely axiomatizable (QFA) *if there is a first–order sentence φ such that*

- $G \models \varphi$
- *if H is a f.g. structure in the same signature such that $H \models \varphi$, then $G \cong H$.*

We will survey results concerning this property in various classes of groups: abelian, nilpotent, metabelian, and (a particular type of) permutation groups. No abelian group is QFA. Examples of QFA groups in the further classes are the following.

- nilpotent groups: $\mathrm{UT}_3(\mathbb{Z})$
- metabelian groups: $\mathbb{Z}[1/m] \rtimes \mathbb{Z} = \langle a, d \mid d^{-1}ad = a^m \rangle$ for any $m \geq 2$ and $\mathbb{Z}/_{p\mathbb{Z}} \wr \mathbb{Z}$ for any prime p
- permutation groups: the subgroup of the group of permutations of $\mathbb{Z}$ generated by the successor function and the transposition $(0, 1)$.

The motivation in [19] for introducing the concept of a QFA group was to gauge the expressiveness of first–order logic in group theory. Only later, it became clear that this concept is also interesting from an algebraic point of view. If $\mathcal{E}$ is a class of groups, then the theory of $\mathcal{E}$, denoted $\mathrm{Th}(\mathcal{E})$, is the set of first–order sentences which hold in all members of $\mathcal{E}$. If $\mathcal{C} \subseteq \mathcal{D}$, then $\mathrm{Th}(\mathcal{C}) \supseteq \mathrm{Th}(\mathcal{D})$. The question studied in [19] is: for which proper inclusions $\mathcal{C} \subset \mathcal{D}$ of natural classes are the theories different? To answer this, one can use the *QFA criterion*:

if there is a QFA group G in $\mathcal{D} - \mathcal{C}$, then $\mathrm{Th}(\mathcal{C}) \supset \mathrm{Th}(\mathcal{D})$.

This is so because the negation of the axiom for G is in $\mathrm{Th}(\mathcal{C}) - \mathrm{Th}(\mathcal{D})$. Here are two applications of the criterion.

EXAMPLES 7.2. (i) Let $\mathcal{C}$ = "finite" and $\mathcal{D}$= "finitely presented with solvable word problem". The criterion applies, via the QFA group $\mathbb{Z}[1/2] \rtimes \mathbb{Z}$.

(ii) Let $\mathcal{C}$ = "finitely presented" and $\mathcal{D}$= "finitely generated". The criterion applies, via the QFA group $\mathbb{Z}/_{2\mathbb{Z}} \wr \mathbb{Z}$.

7.1. Abelian groups. No abelian group is QFA: by Szmielew's quantifier elimination for the theory of abelian groups (see [7, Thm. A.2.7]), each sentence φ which holds in an abelian group G also holds in $G \times \mathbb{Z}(p)$, for almost all primes p. If G is f.g. then $G \not\cong G \times \mathbb{Z}(p)$ for each prime p, so G is not QFA.

Oger [26, Thms. 2 and 3] extended the result to f.g. *abelian-by-finite* groups: such a group is never QFA. Thus the properties of being QFA and being FA-presentable are incompatible (for f.g. infinite groups, the only relevant case), by the result in [28] that each finitely generated FA-presentable group is abelian-by-finite.

7.2. Nilpotent groups. Oger and Sabbagh [27] characterized the property of being QFA for nilpotent groups, in a purely algebraic way. Informally speaking, G is QFA iff the center $Z(G)$ is not too large, in a sense to be specified. For any group G, let $G' = \langle [x, y] \colon x, y \in G \rangle$ be the commutator subgroup, and let

$$\Delta(G) = \{x \colon (\exists m > 0)\ x^m \in G'\}$$

be its isolator. $\Delta(G)$ is the least $N \lhd G$ such that $G/_N$ is torsion free and abelian.

THEOREM 7.3. [27] *Let G be infinite, f.g. and nilpotent. Then*

$$G \text{ is } QFA \Leftrightarrow Z(G) \subseteq \Delta(G).$$

The direction "$\Rightarrow$" holds for all f.g. groups. In particular, one obtains an alternative proof that no abelian group is QFA, because, if G is infinite f.g. abelian, then $Z(G) = G$ while $\Delta(G)$ is the finite torsion subgroup. The argument in [27] (for this direction) extends the one given above for abelian groups, by introducing ultraproducts.

Let us use Theorem 7.3 in order to see that the Heisenberg group $G = \mathrm{UT}_3(\mathbb{Z})$ (see Subsection 4.2) is QFA. This group is torsion free, and

$$Z(G) = G' = \begin{pmatrix} 1 & 0 & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus $\mathrm{UT}_3(\mathbb{Z})$ is QFA. This result was first obtained in a completely different way in [19, Thm. 5.1] using logic, in particular the Mal'cev interpretation of $(\mathbb{N}, +, \times)$ in $\mathrm{UT}_3(\mathbb{Z})$ already mentioned when we discussed the proof of Theorem 4.3. In comparison, the characterization in [27] leads further. For instance, it also shows that all non-abelian upper triangular groups over $\mathbb{Z}$, and all free nilpotent non-abelian groups are QFA.

The following counterexample shows that one cannot replace the condition $Z(G) \subseteq \Delta(G)$ in Theorem 7.3 by the weaker condition that $Z(G) \subseteq G'$. Fix $m \geq 2$. If $G = \begin{pmatrix} 1 & m\mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$, then $Z(G)$ is as before, but $G' = \begin{pmatrix} 1 & 0 & m\mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. G' does not include $Z(G)$, but $\Delta(G) = Z(G)$. G is not isomorphic to $\mathrm{UT}_3(\mathbb{Z})$, but QFA as well.

For f.g. nilpotent groups, the following are equivalent:

(i) $Z(G) \not\subseteq \Delta(G)$
(ii) *G has a subgroup of finite index with a direct factor isomorphic to $\mathbb{Z}$.*

The implication (i)⇒(ii) is true for all f.g. groups, by [26, Prop. 1]:

PROPOSITION 7.4. *Let G be a f.g. group such that there is an element $g \in Z(G) - \Delta(G)$. Then g has infinite order, and there is a subgroup $S \leq G$ such that $\langle \{g\} \cup S \rangle_{gp}$ equals the direct product $\langle g \rangle_{gp} \times S$ and has finite index in G.*

PROOF. Let $D = \Delta(G)$. Since $G/_D$ is f.g. torsion free abelian, there are $b, r_1, \dots, r_{k-1} \in G$ and $i \in \mathbb{N}$ such that $g = b^i$ and

$$\{Db, Dr_1, \dots, Dr_{k-1}\}$$

is a basis of $G/_D$. Let $S = D\langle r_1, \dots, r_{k-1} \rangle_{gp} \lhd G$, then $\langle b \rangle_{gp} S = G$ and $\langle b \rangle_{gp} \cap S = \{1\}$. Since $g \in Z(G)$, $\langle \{g\} \cup S \rangle_{gp}$ equals the direct product $\langle g \rangle_{gp} \times S$, and since $gb^{-i} \in D$, this direct product has index i in G. ⊣

The converse implication, (ii)⇒(i), is false in general, by Example 4.2 (iii), but true for f.g. nilpotent groups [26].

Oger [26, Cor. 7] showed that among the nilpotent (and also the nilpotent-by-finite) groups, the property of being QFA is closed under taking subgroups of finite index and under forming finite direct products.

7.3. Metabelian groups. A group G is *metabelian* if the commutator group $G' = \langle \{[x, y] \colon x, y \in G\} \rangle_{gp}$ is abelian. That is, the group has solvability length 2.

We will discuss two types of examples of metabelian QFA groups. The groups of the second type are one-relator groups, first studied by Baumslag and Solitar. The groups of the first type are not even finitely presented. We denote the cyclic group $\mathbb{Z}/_{m\mathbb{Z}}$ by $\mathbb{Z}(m)$.

THEOREM 7.5. (i) *For each prime p, the restricted wreath product $\mathbb{Z}(p) \wr \mathbb{Z}$ is QFA* [19, Thm. 2.3].
(ii) *For each $m \geq 2$, the group $H_m = \langle a, d \mid d^{-1}ad = a^m \rangle$ is QFA* [20, Thm. 2.2].

For any groups G, A, C, one says that $G = A \rtimes C$ (G is a *semidirect product* of A and C) if

$$AC = G, \ A \lhd G, \text{ and } A \cap C = \{1\}.$$

The restricted wreath product $\mathbb{Z}(p) \wr \mathbb{Z}$ is a semidirect product $A \rtimes C$, where $A = \bigoplus_{r \in \mathbb{Z}} \mathbb{Z}(p)^{(r)}$, each $\mathbb{Z}(p)^{(r)}$ is a copy of $\mathbb{Z}(p)$, and $C = \langle d \rangle_{gp}$ with d of infinite order. The element d acts on A by shifting, i.e., the copy $\mathbb{Z}(p)^{(r)}$ is mapped to the copy $\mathbb{Z}(p)^{(r+1)}$, for each $r \in \mathbb{Z}$.

H_m is a semidirect product of

$$A = \mathbb{Z}[1/m] = \{zm^{-i} \colon z \in \mathbb{Z}, i \in \mathbb{N}\}$$

by $\langle d \rangle$, where the action of d is given by $d^{-1}ud = um$.

F. Oger [26] has found further examples of QFA groups that are semidirect products $H = A \rtimes C$, with A abelian, and $C = \langle d \rangle_{gp}$ infinite cyclic. He uses some algebraic number theory. In his examples, A is free abelian of finite rank, while in the examples above, A is not f.g. A typical case is $A = \mathbb{Z}[u]$ where $u = 2 + \sqrt{3}$, and the action of d is given by $a \mapsto au$ for $a \in A$.

The proofs that the groups $G = A \rtimes C$ in (i) and (ii) are QFA follow the same scheme (and so does, to some extent, Oger's example). The group A is defined by a first-order formula. Let $C = C(d)$ be the centralizer of d, that is, $C = \{x : [x, d] = 1\}$. We write a conjunction $\psi(d) = (\mathrm{P1}) \wedge \cdots \wedge (\mathrm{Pk})$ of first-order properties that are satisfied by d in G, in such a way that G is characterized among the f.g. groups by the sentence $\exists d\ \psi(d)$.

(P1) The commutators form a subgroup,
(P2) A and C are abelian, and $G = A \rtimes C$,
(P3) $C - \{1\}$ acts on $A - \{1\}$ without fix points. That is, $[u, x] \neq 1$ for $u \in A - \{1\}, x \in C - \{1\}$,
(P4) $|C : C^2| = 2$.

Clearly these conditions can be formulated in the first-order language of groups. By (P1), G' is definable.

(i) Concerning $\mathbb{Z}_p \wr \mathbb{Z}$, we use the definition $A = \{g : g^p = 1\}$, and require in addition that $|A : G'| = p$ and no element in $C - \{1\}$ has order $< p$. The details can be found in [19].

(ii) Concerning H_m, we use the definition $A = \{g : g^{m-1} \in G'\}$. We fix a prime q not dividing m. The remaining conditions are the following.

(P5) $\forall u \in A\ [d^{-1}ud = u^m]$,
(P6) The map $u \mapsto u^q$ is 1-1 in A,
(P7) $x^{-1}ux \neq u^{-1}$ for $u \in A - \{1\}, x \in C$,
(P8) $|A : A^q| = q$,
(P9) $\forall g\ [g^i \neq d]$, for each i, $1 < i \leq m$.

It is not hard to verify that (H_m, d) satisfies these properties. Now suppose G is a f.g. group, and $d \in G$ satisfies (P1)–(P9). One first shows that d has infinite order. Let $R_m = \mathbb{Z}[1/m]$, viewed as a ring. A is turned into an R_m-module by defining $u(zm^{-i}) = d^i u^z d^{-i}$ $(u \in A, z \in \mathbb{Z}, i \in \mathbb{N})$. It can be shown that A is f.g. and torsion free as an R_m-module. Since R_m is a principal entire ring, we may conclude that A is free (see Lang [15, Thm. XV.2.2]), so A is isomorphic to the additive group of $(R_m)^k$ for some k. Then $|A : A^q| = q^k$ and hence $k = 1$ by (P8). Finally one uses (P7) to show that C is infinite cyclic. Thus $G \cong H_m$. Details are in [20]. ⊣

A. Khelif has announced that each free metabelian group of finite rank ≥ 2 is QFA [12].

7.4. QFA groups with complex word problem. The *word problem* $W(G)$ of a f.g. group G is the problem of deciding whether $t(x_1, \ldots, x_n) \in N$, where $G \cong F(x_1, \ldots, x_n)/N$ is a presentation of G. It is easy to see that, up to many-one equivalence, this is independent of the particular presentation. (For sets $X, Y \subseteq \mathbb{N}$, one says X is many-one reducible to Y if there is a computable function f such that $X = f^{-1}(Y)$.) The word problem of a QFA group can be of arbitrarily high complexity within the hyperarithmetical hierarchy. On the other hand, the atomic diagram of any QFA structure (and hence the word problem of any QFA group) is hyperarithmetical [17].

To obtain those complex groups, we use the following concept. A set $S \subseteq \omega$ is called an *arithmetical singleton* if there exists a formula $\varphi(X)$ in the language of arithmetic, extended by a new unary predicate symbol X, such that for each $P \subseteq \mathbb{N}$, $\varphi(P)$ is true in the standard model of arithmetic if and only if $P = S$. Examples include all arithmetical sets, but also $\mathrm{Th}(\mathbb{N}, +, \times)$ (where we assume an effective encoding of sentences by natural numbers). One can define a jump $\emptyset^{(\alpha)}$ for each recursive ordinal α, and it is an arithmetical singleton. Thus arithmetical singletons exist arbitrarily high in the hyperarithmetical hierarchy, and on the other hand, each arithmetical singleton is hyperarithmetical.

THEOREM 7.6. [17] *For each arithmetical singleton $S \subseteq 3\mathbb{N}^+$, there exists a 2–generated QFA group G_S whose word problem $W(G_S)$ has the same complexity as S (namely, $S \equiv_T W(G_S)$).*

G_S is the subgroup of the permutations of $\mathbb{Z}$ generated by the successor function and

$$p_S = (0,1) \cdot \prod_{k \in S} (k, k+1, k+2). \tag{3}$$

Let $\mathrm{Sym}_{fin}(\mathbb{Z})$ be the group of permutations of $\mathbb{Z}$ with finite support. Since $p_S^3 = (0,1)$, we have $\mathrm{Sym}_{fin}(\mathbb{Z}) \leq G_S$. In particular, $G_\emptyset$ is generated by $\mathrm{Sym}_{fin}(\mathbb{Z})$ and successor. Clearly, $G_\emptyset = \mathrm{Sym}_{fin}(\mathbb{Z}) \rtimes \langle d \rangle_{gp}$ where d is the successor function and its action on $\mathrm{Sym}_{fin}(\mathbb{Z})$ is given by shifting. So we have obtained a further example of a QFA group, a permutation group analogous to the examples in Subsection 7.3.

COROLLARY 7.7. *The group $G_\emptyset = \mathrm{Sym}_{fin}(\mathbb{Z}) \rtimes \mathbb{Z}$ is QFA.*

No purely algebraic proof of this fact is known.

All the examples we have seen are far from being simple groups.

QUESTION 7.8. *Is there a simple QFA group*?

7.5. Prime groups. The following notion is from model theory. A structure G is *prime* if G is isomorphic to an elementary submodel of each H such that $\mathrm{Th}(G) = \mathrm{Th}(H)$. If a theory has a prime model then it is unique up to isomorphism. For instance, $(\mathbb{Q}, +)$ and the Prüfer groups $\mathbb{Z}(p^\infty)$, where p is a prime number, are prime models. (The theories are ω_1-categorical here.) However, various theories of groups fail to have a prime model, for instance $\mathrm{Th}(\mathbb{Z}, +)$ and $\mathrm{Th}(F_2)$, where F_2 is the free group of rank 2 (see [18] for the latter).

It is a result of model theory that a countable structure in a finite signature G is prime iff each realized type is principal [7] iff the orbit of each tuple (under the automorphisms of G) is definable by a first order formula without parameters. This leads to the following, more algebraic characterization of being prime for f.g. groups [27]: there is a generating tuple $\overline{g}$ whose orbit is definable. Note that this looks quite a bit like the QFA definition. We will compare these two properties of groups.

Using Theorem 7.3, Oger and Sabbagh [27] have shown that if G is a nilpotent f.g. group, then G is QFA iff G is prime. This result was extended to nilpotent-by-finite groups in Oger [26].

Since there are only countably many QFA groups, the next Theorem implies that not all prime groups are QFA.

THEOREM 7.9 (Nies [20]). *There are uncountably many non-isomorphic f.g. groups that are prime.*

In fact the permutation groups G_S as above provide those examples, for sets S whose elements are sufficiently far apart, but not arithmetical singletons any longer. One shows that S can be recovered from $\mathrm{Th}(G_S)$, so there are uncountably many different theories and hence uncountably many nonisomorphic prime models. The *class* is QFA in the sense that it consists of the f.g. groups satisfying a sentence α.

It is currently open whether each QFA group is prime. However, all the examples of QFA groups discussed above are prime. For $G_\emptyset$ this comes out of the proof of Theorem 7.9. Khelif [12] showed it for the groups in Theorem 7.5; see Subsection 7.7 below. On the other hand, also in [12], he gave an example of a structure $\mathbf{A}$ that is QFA but not prime, namely the ordered abelian group $\mathbb{Z}[1/2]$, with the extra unary operation $x \mapsto 2x$. To prove that $\mathbf{A}$ is QFA, he used the linear order to ensure torsion freeness, and then argued along the lines of the proof of Theorem 7.5(ii).

QUESTION 7.10. *Is each QFA group prime*?

7.6. QFA rings. All rings in this subsection are commutative rings with identity. O. Belegradek (2004) raised the question which f.g. rings are QFA. Note that each f.g. ring is noetherian (each ideal is finitely generated as an ideal), since $\mathbb{Z}[X_1, \dots, X_n]$ is noetherian (see [15]), and $\mathbb{Z}[X_1, \dots, X_n]$ is the free ring in n variables. It follows that each f.g. ring R is finitely presented, and each ideal of R is parameter definable. $\mathbb{Q}(X)$ is an example of a noetherian but not f.g. ring.

The first result in the direction of answering Belegradek's question was the following.

THEOREM 7.11 (Sabbagh 2004). $(\mathbb{Z}, +, \times)$ *is* QFA.

To this, first note that the ordering is definable, since for each $x \in \mathbb{Z}$, $x \geq 0$ iff x is the sum of four squares (Lagrange's theorem). Using a coding mechanism for $(\mathbb{N}, +, \times)$, for instance the Gödel β function, the factorial function f is definable in $\mathbb{Z}$, by a formula $\varphi(x, y)$ without parameters. Sabbagh characterized $(\mathbb{Z}, +, \times)$ among the f.g. rings, and in fact among the noetherian rings, by the following first-order conditions:

(P1) The axioms of ordered rings, where the ordering is given by declaring the sums of four squares to be the non-negative elements,
(P2) the interval $(0, 1)$ is empty, and
(P3) the function f defined by φ satisfies $f(x) > 0$ and $(x + 1)f(x) = f(x + 1)$, for each $x \geq 0$.

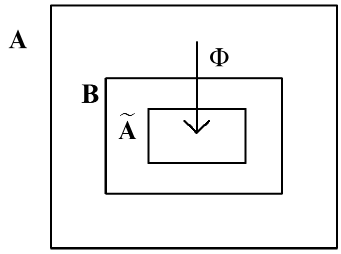
Suppose a ring H satisfies these axioms. For each $n \in \mathbb{N}$, let $\underline{n}$ denote $1^H + 1^H + \dots 1^H$ (n times). If $H \not\cong \mathbb{Z}$, then H has a non-standard element c, that is, $c > \underline{n}$ for each $n \in \mathbb{N}$. For each $n \in \mathbb{N}$, let $a_n = f^H(c - \underline{n})$. Applying (P3) to $x = c - \underline{n}$, we have $a_n(c - \underline{n} + 1) = a_{n-1}$ for each $n > 0$. Thus, in H, a_n divides a_{n-1} but a_{n-1} does not divide a_n since $c - \underline{n} + 1 > 1$. Hence the ideal generated by $\{a_n : n \in \mathbb{N}\}$ is not finitely generated, and H is not noetherian. $\dashv$

Belegradek has modified the proof in order to make it purely number theoretic. Instead of the the Gödel β function, he directly uses the Chinese remainder theorem (on which the β function is based).

7.7. Bi-interpretability with the integers. Khelif realized that one can use bi-interpretability of a f.g. structure **A** with $(\mathbb{Z}, +, \times)$ as a general method to prove that **A** is QFA and prime. Somewhat later, Scanlon independently used this method to show that each f.g. field is QFA. The method had already been used implicitly in [17] to prove Theorem 7.6.

Interpretability (Subsection 2.2) of a structure **B** in a structure **A** is a property of **B** up to isomorphism. Here we will actually consider the isomorphic copy of **B** that is *defined* in **A** by the relevant collection of formulas. For instance, recall the example of an interpretation of $(\mathbb{Z}, +)$ in $(\mathbb{N}, +)$ in Subsection 2.2; the actual copy of $(\mathbb{Z}, +)$ defined in $(\mathbb{N}, +)$ is the structure whose domain consists of pairs of natural numbers, whose addition is componentwise and where equality is the equivalence relation on pairs given there.

All first-order formulas in this subsection are allowed to contain parameters. Suppose structures $\mathbf{A}, \mathbf{B}$ in finite signatures are given, as well as interpretations of **A** in **B** and vice versa. Then an isomorphic copy $\widetilde{\mathbf{A}}$ of **A** can be defined in **A**, by "decoding" **A** from the copy of **B** defined in **A**. Similarly, an isomorphic copy $\widetilde{\mathbf{B}}$ of **B** can be defined in **B**. An isomorphism $\Phi \colon \mathbf{A} \cong \widetilde{\mathbf{A}}$ can be viewed as a relation on **A** (since the elements of $\widetilde{\mathbf{A}}$ are represented by matrices of elements of **A**), and similarly for an isomorphism $\mathbf{B} \cong \widetilde{\mathbf{B}}$. We say that **A** and **B** are *bi-interpretable* (with parameters) if there are such isomorphisms that are first-order definable. For the details of the definition, see [7, Ch. 5]. The figure below illustrates the situation on the **A**-side.



Via bi-interpretability with $(\mathbb{Z}, +, \times)$, Khelif [12] showed that the groups in Theorem 7.5 are prime, and gave new proofs that they are QFA.

We will be a bit more general here and consider bi-interpretability of a structure $\mathbf{A}$ in a finite signature with the structure

$$\mathbf{Z}_S = (\mathbb{Z}, +, \times, S),$$

where $S \subseteq \mathbb{N}$. We give an equivalent formulation of bi-interpretability in this case, stating that each element of $\mathbf{A}$ can be represented by an element of a copy of $\mathbf{Z}_S$ defined in $\mathbf{A}$. Recall that all first-order definitions may be with parameters.

Proposition 7.12. *Let $S \subseteq \mathbb{N}$ and let $\mathbf{A}$ be a structure in a finite signature. Then the following are equivalent.*

(i) *$\mathbf{A}$ is bi-interpretable with $\mathbf{Z}_S$*
(ii) *$\mathbf{A}$ can be interpreted in $\mathbf{Z}_S$, and there is a copy $\mathbf{M}$ of $\mathbf{Z}_S$ definable in $\mathbf{A}$, together with a definable injective map $f : \mathbf{A} \to \mathbf{M}$.*

Proof. (i) $\Rightarrow$ (ii): Let $\mathbf{M}$ be the copy of $\mathbf{Z}_S$ defined in $\mathbf{A}$. As before, let $\widetilde{\mathbf{A}}$ be the copy of $\mathbf{A}$ defined within $\mathbf{A}$ itself, via $\mathbf{M}$, and let $\Phi\colon \mathbf{A} \to \widetilde{\mathbf{A}}$ be a definable isomorphism. Since $\widetilde{\mathbf{A}}$ can be interpreted in $\mathbf{Z}_S$, there is an injective map $g\colon \widetilde{\mathbf{A}} \to \mathbf{Z}_S$ which is arithmetical in S, and hence definable in $\mathbf{A}$ (when thinking of $\mathbf{Z}_S$ as its copy $\mathbf{M}$ defined in $\mathbf{A}$). Then $f = g \circ \Phi\colon \mathbf{A} \to \mathbf{Z}_S$ is a definable injective map as required.

(ii) $\Rightarrow$ (i): To show that the isomorphism $\Psi\colon \mathbf{Z}_S \cong \widetilde{\mathbf{Z}}_S$ is definable in $\mathbf{Z}_S$, notice that the successor function on $\widetilde{\mathbf{Z}}_S$ is definable in $\mathbf{Z}_S$. Then Ψ is arithmetical in S, and hence definable in $\mathbf{Z}_S$.

It remains to obtain an isomorphism $\Phi\colon \mathbf{A} \to \widetilde{\mathbf{A}}$ that is definable in $\mathbf{A}$. As before, we think of $\mathbf{Z}_S$ as its copy $\mathbf{M}$ defined in $\mathbf{A}$. Thus $\widetilde{\mathbf{Z}}_S$ can also be also viewed as defined in $\mathbf{A}$. Since the map $f : \mathbf{A} \to \mathbf{Z}_S$ is definable in $\mathbf{A}$, the corresponding map $\widetilde{f} : \widetilde{\mathbf{A}} \to \widetilde{\mathbf{Z}}_S$ is definable in $\widetilde{\mathbf{A}}$, and hence in $\mathbf{A}$. Moreover, $\Psi\colon \mathbf{Z}_S \cong \widetilde{\mathbf{Z}}_S$ is definable in $\mathbf{A}$. Now we obtain the required isomorphism Φ as the composition of the maps

$$\mathbf{A} \xrightarrow{f} \mathbf{Z}_S \xrightarrow{\Psi} \widetilde{\mathbf{Z}}_S \xrightarrow{\widetilde{f}^{-1}} \widetilde{\mathbf{A}}. \qquad \dashv$$

Here is an example of how to apply (ii)$\Rightarrow$(i) of the previous Proposition (without the subset S).

THEOREM 7.13. [12] *The ring* $\mathbb{Z}[X]$ *is bi-interpretable with* $(\mathbb{Z}, +, \times)$ *in parameters.*

PROOF. We fulfill (ii) where $\mathbf{A} = \mathbb{Z}[X]$. To define a copy $\mathbf{M}$ of $(\mathbb{Z}, +, \times)$ in the ring $\mathbb{Z}[X]$, one simply shows that $\mathbb{Z}$ is a definable subset of $\mathbb{Z}[X]$. For this, note that for each $P \in \mathbb{Z}[X]$,

$$\mathbb{Z}[X]/(P) \cong \mathbb{Z} \Leftrightarrow P \text{ has the form } \pm X + c \text{ for some } c \in \mathbb{Z}.$$

By Theorem 7.11, the ring $\mathbb{Z}$ is QFA , so one can define the class $\mathcal{C}$ of polynomials of the form $\pm X + c$ (this argument is due to Nies). Now $\mathbb{Z} = \{U - V : U, V \in \mathcal{C} \wedge U, V \text{ have the same sign}\}$, and $U, V \in \mathcal{C}$ have the same sign iff $(U + V)/2 \in \mathcal{C}$ or $(U + V + 1)/2 \in \mathcal{C}$. Thus, $\mathbb{Z}$ is definable $\mathbb{Z}[X]$ (even without parameters).

To interpret $\mathbb{Z}[X]$ in $\mathbb{Z}$, one encodes a polynomial P in an effective way by some natural number n_P. Let E be the binary partial function mapping (n, λ) to $P(\lambda)$ in case $n = n_P$ (where $n \in \mathbb{N}$ and $\lambda \in \mathbb{Z}$). Then E is computable, and hence definable in $\mathbb{Z}$.

To obtain an injective map $f : \mathbb{Z}[X] \to \mathbb{Z}$, one shows that the map $P \mapsto n_P$ is definable in $\mathbb{Z}[x]$:

$$\begin{aligned} n = n_P &\Leftrightarrow P \text{ and the polynomial encoded by } n \text{ evaluate the same} \\ &\Leftrightarrow \text{for each } \lambda \in \mathbb{Z},\ P - E(n, \lambda) \text{ vanishes at } \lambda \\ &\Leftrightarrow \forall \lambda \in \mathbb{Z}\ (X - \lambda) \mid (P - E(n, \lambda)). \end{aligned}$$

The last statement can be expressed by a first-order formula with parameter X. Now apply Proposition 7.12, for $S = \emptyset$. $\dashv$

Given (ii) of Proposition 7.12, since the range of f is definable in $\mathbf{A}$, one can modify the first-order definition of f in order to make f a bijection. Then, one can replace the elements of $\mathbf{M}$ by their pre-images under f, in order to even make f the identity on $\mathbf{A}$. Thus, $\mathbf{A}$ is bi-interpretable with $\mathbf{Z}_S$ iff there is a structure with the *same* domain $\mathbf{B} = (A; \oplus, \otimes, U)$ such that $\mathbf{B} \cong \mathbf{Z}_S$, and each of

- the relations and functions of $\mathbf{A}$ and
- $\oplus, \otimes, U$

are mutually definable from the other, using a list of parameters $\overline{p}$.

Let $\mathbf{M}_{\overline{p}}$ denote the copy of $\mathbf{Z}_S$ defined in this way in $\mathbf{A}$ via the list of parameters $\overline{p}$. What happens for some other list $\overline{q}$? A first-order condition $\alpha_0(\overline{q})$ expresses that

(a) $\mathbf{M}_{\overline{q}}$ has domain $\mathbf{A}$,
(b) $\mathbf{M}_{\overline{q}}$ satisfies sufficiently many basic axioms of arithmetic and
(c) the relations and functions of $\mathbf{A}$ are defined by the appropriate formulas, from the point of view of $\mathbf{M}_{\overline{q}}$.

In the following, all lists of parameters satisfy the condition α_0. In general, $\mathbf{M}_{\overline{q}}$ may be nonstandard, that is, its algebraic structure may not be isomorphic to the ring $\mathbb{Z}$. However, $\mathbb{Z}$ is embedded into $\mathbf{M}_{\overline{q}}$, being isomorphic to the ring generated by 1, since we assume $\mathbf{M}_{\overline{q}}$ satisfies basic properties of arithmetic. This copy of $\mathbb{Z}$ inside $\mathbf{M}_{\overline{q}}$ is called the *standard part* of $\mathbf{M}_{\overline{q}}$.

Bi-interpretability with $\mathbf{Z}_S$ can be used to obtain prime and QFA structures. Recall the definition of an arithmetical singleton from Subsection 7.4. A version of the following theorem without the set S was first proved in [12].

THEOREM 7.14. *Suppose the structure* $\mathbf{A}$ *in a finite signature is bi-interpretable with* $\mathbf{Z}_S$, *where* $S \subseteq \mathbb{N}$. *Then*

(i) $\mathbf{A}$ *is a prime model.*
(ii) *If* $\mathbf{A}$ *is finitely generated and* S *is an arithmetical singleton, then* $\mathbf{A}$ *is QFA.*

PROOF. (i) We find a first-order condition $\alpha_{st}(\overline{q})$ that extends $\alpha_0(\overline{q})$ and ensures that $\mathbf{M}_{\overline{q}}$ is standard. There is a list of parameters $\overline{p}$ such that $\mathbf{M}_{\overline{p}}$ is standard. For a general list $\overline{q}$, the standard part of $\mathbf{M}_{\overline{q}}$ is in $\Sigma^0_k(S)$ for a fixed k, relative to $\mathbf{M}_{\overline{p}}$ (here we need that the domain of $\mathbf{M}_{\overline{p}}$ is all of A). We do not know $\overline{p}$, but still we may quantify over a class of subsets of $\mathbf{A}$ that includes the standard part of $\mathbf{M}_{\overline{q}}$, namely those sets that are $\Sigma^0_k(U)$ relative to some $\mathbf{M}_{\overline{r}} = (A; \oplus, \otimes, U)$. In this way, a formula $\alpha_{st}(\overline{q})$ expresses in first-order logic that the standard part of $\mathbf{M}_{\overline{q}}$ is equal to $\mathbf{M}_{\overline{q}}$. By (c) in the condition $\alpha_0(\overline{q})$, the formula α_{st} defines the orbit of $\overline{p}$. It is now easy to see that each orbit of a tuple under the automorphisms of $\mathbf{A}$ is definable by a first order formula without parameters. Thus, by Subsection 7.5, $\mathbf{A}$ is prime.

(ii) exploits ideas from [17]. Let $\overline{p}$ be a sequence of elements from $\mathbf{A}$ such that $\mathbf{M}_{\overline{p}}$ is standard.

CLAIM 7.15. *There is a first-order condition* $\beta(\overline{r})$, *extending* $\alpha_0(\overline{r})$, *such that* $\mathbf{A} \models \beta(\overline{p})$ *and, whenever* $\mathbf{B}$ *is a f.g. structure in the same signature as* $\mathbf{A}$ *and* $\mathbf{B} \models \beta(\overline{r})$, *then* $\mathbf{M}_{\overline{r}}$ *is standard.*

If S is an arithmetical singleton, then a condition $\gamma(\overline{r})$ extending $\beta(\overline{r})$ expresses that $\mathbf{M}_{\overline{r}} \cong \mathbf{Z}_S$, by incorporating the description of S. So by (c) in the condition $\alpha_0(\overline{r})$, $\mathbf{A}$ is QFA via the axiom $\varphi \equiv \exists \overline{r}\, \gamma(\overline{r})$.

It remains to prove the claim. Note that, when choosing (b) in the condition α_0 appropriately, if $\mathbf{B} \models \alpha_0(\overline{r})$ then we can encode in $\mathbf{M}_{\overline{r}}$ finite objects such as terms for the signature of $\mathbf{A}$, or tuples of elements of $\mathbf{B}$. There is a definable function E such that, in $\mathbf{A}$, $E(n, u; \overline{p}) = b$ whenever $n \geq 0$ codes a term $t(x_1, \dots, x_k)$, u codes the tuple $b_1, \dots, b_k$ and $t(b_1, \dots, b_k) = b$. (This function is definable since finite objects can be encoded in $\mathbf{M}_{\overline{p}}$, such as the intermediate values occurring in a term evaluation.) Beyond $\alpha_0(\overline{r})$, the formula $\beta_0(\overline{r})$ expresses that E describes term evaluation correctly in a structure $\mathbf{B}$, with respect to coding of terms in $\mathbf{M}_{\overline{r}}$. This formula has the initial clauses $\forall m \forall i\, [m$ codes variable $x_i \;\;\&\;\; i < |u| \rightarrow E(m, u; \overline{r}) = u_i]$, as well as inductive clauses for each function symbol. For instance, if f is a unary function symbol, then β contains the clause $\forall n, m\, \forall u\; [m$ codes $t \;\;\&$ n codes $f(t) \rightarrow f(E(m, u; \overline{r}) = E(n, u; \overline{r})]$.

For each $g, v, \overline{r}$, let $\mu(g, v; \overline{r})$ be the least code number $n \in \mathbf{M}_{\overline{r}}$ of a term t such that $E(n, g; \overline{r}) = v$. If $\mathbf{B}$ is f.g., $\mathbf{B} \models \beta(\overline{r})$, g codes a generating tuple $b_1, \dots, b_k$ of $\mathbf{B}$ ($k \in \mathbb{N}$) and $n \in \mathbf{M}_{\overline{r}}$ codes a term $t(x_1, \dots, x_k)$, then $E(n, g; \overline{r})$ is the correct value $t(b_1, \dots, b_k)$. Thus $\mu(g, v; \overline{r})$ is defined and is a standard non-negative element of $\mathbf{M}_{\overline{r}}$. Let $L(h; \overline{r})$ be the set of those $m \in \mathbf{M}_{\overline{r}}$, $m \geq 0$, such that $m < \mu(h, v; \overline{r})$ for some v, then for g as before, $L(g; \overline{r})$ equals $P_{\overline{r}}$, the set of non-negative elements in the standard part of $\mathbf{M}_{\overline{r}}$. So $P_{\overline{r}}$ is the intersection of all nonempty sets $L(h, \overline{r})$ that have no greatest element. Let $\beta(\overline{r})$ be the conjunction of $\beta_0(\overline{r})$ and the assertion that $P_{\overline{r}}$ is the set of non-negative elements in $\mathbf{M}_{\overline{r}}$. Clearly $\mathbf{A} \models \beta(\overline{p})$. Thus the formula $\beta(\overline{r})$ establishes the claim. $\dashv$

Khelif used his version of Theorem 7.14, without the set S, to conclude from Theorem 7.13 that $\mathbb{Z}[X]$ is prime and QFA. For a further application, the group G_S given in (3) is bi-interpretable with $\mathbf{Z}_S$ (without the extra condition on S that the elements be sufficiently far apart). Thus, we obtain a new proof of the result from [17, Thm. 3] that G_S is QFA if S is an arithmetical singleton, and, improving the result from [20], that the group G_S is prime for each $S \subseteq \mathbb{N}$. The interpretation of $\mathbf{Z}_S$ in G_S is given in [17, Section 2]. We have to first-order define a copy $\mathbf{M}$ of $\mathbf{Z}_S$ in G_S. The domain of $\mathbf{M}$ can be defined without parameters (the elements are equivalence classes of certain pairs of transpositions). So each $g \in G_S$ operates on $\mathbf{M}$ via conjugation, and can thereby be viewed as a permutation $\widehat{g}$ of $\mathbf{M}$. Let w be the successor function on $\mathbb{Z}$ and let p_S be as in (3). We use $\widehat{w}$ and $\widehat{p}_S$ as parameters to define the structure of $\mathbf{M}$. To obtain the injective map $f : G_S \to \mathbf{M}$ in (ii) of Proposition 7.12, we map each $g \in G_S$ to a code $n \in \mathbf{M}$ of a term t such that $t(\widehat{p}_S, \widehat{w}) = \widehat{g}$.

Theorem 7.14 has several other applications, but it does not cover all the known examples: the group $\mathrm{UT}_3(\mathbb{Z})$ is both QFA and prime ([19], also see Subsection 7.2), but Khelif [12] has shown the following.

Theorem 7.16. $\mathrm{UT}_3(\mathbb{Z})$ *is not bi-interpretable with* $\mathbb{Z}$.

Proof. We use the fact that, in a sense, $\mathrm{UT}_3(\mathbb{Z})$ has many automorphisms fixing the center. First some general remarks. If a structure $\mathbf{A}$ is bi-interpretable with the ring $\mathbb{Z}$ via a particular interpretation $\mathbf{M}_{\overline{p}} \cong \mathbb{Z}$, in the sense of (ii) of Proposition 7.12, then one can also base the bi-interpretation on any other interpretation $\mathbf{N}_{\overline{q}} \cong \mathbb{Z}$ in $\mathbf{A}$, because the isomorphism $\mathbf{M}_{\overline{p}} \cong \mathbf{N}_{\overline{q}}$ is definable in $\mathbf{A}$ (to see this, note that the isomorphism is definable in the structure $\mathbf{B} \cong \mathbf{Z}_S$ mentioned above that has the same domain as $\mathbf{A}$; see the proof of Theorem 7.14 (i)). Thus, if $\mathrm{UT}_3(\mathbb{Z})$ is bi-interpretable with $\mathbb{Z}$, then we may as well assume that $\mathbf{M}_{\overline{p}}$ is the copy of $\mathbb{Z}$ obtained by Mal'cev coding (see Subsection 4.2) where the domain is the center and $\overline{p} = (a, b)$. Let R be a nonstandard elementary extension of the ring $\mathbb{Z}$ with only countably many automorphisms, which can for instance be obtained by first taking *any* nonstandard extension and then letting R be the closure of a nonstandard element under definable Skolem functions. Let $\mathbf{M}^R_{\overline{p}}$ be the structure coded by $\overline{p}$ in the group $G = \mathrm{UT}_3(R)$, then $\mathbf{M}^R_{\overline{p}} \cong R$. G has only countably many automorphisms, since otherwise the stabilizer of $\overline{p}$ in $\mathrm{Aut}(G)$, that is $\{\Phi \in \mathrm{Aut}(G) \colon \forall i\, \Phi(p_i) = p_i\}$, would be uncountable, and this stabilizer is isomorphic to $\mathrm{Aut}(R)$.

On the other hand, by [11, Thm. 11.5], R is recursively saturated, being a nonstandard model of $\mathrm{Th}(\mathbb{Z})$, whence the divisible part of $(R, +)$ is a $\mathbb{Q}$-vector space of infinite dimension. Since the divisible part of an abelian group is a direct factor, this gives uncountably many bilinear maps $F \colon R \times R \to R$ when R is viewed as a $\mathbb{Z}$-module. For each such F, we have a corresponding automorphism Φ_F of $G = \mathrm{UT}_3(R)$: let ρ be the projection $G \to G/_{Z(G)} \cong R \times R$. Since $Z(G) \cong R$, $F \circ \rho$ can be viewed as a map $G \to Z(G)$. Let $\Phi_F(x) = xF(\rho(x))$. It is easily verified that Φ_F is an automorphism of G. Since $x^{-1}\Phi_F(x) = F(\rho(x))$, one can recover F from Φ_F. So $\mathrm{Aut}(R)$ is uncountable, contradiction. $\dashv$

The argument goes through for $\mathbf{Z}_S$ instead of $\mathbb{Z}$, where $S \subseteq \mathbb{N}$, since one can still find R as before. Thus $\mathrm{UT}_3(\mathbb{Z})$ is not even bi-interpretable with any structure $\mathbf{Z}_S$.

REFERENCES

[1] S. Akiyama, C. Frougny, and J. Sakharovitch, *Powers of rationals modulo* 1 *and rational base systems*, preprint, 2005.

[2] A. Blumensath and E. Grädel, *Finite presentations of infinite structures*: *automata and interpretations*, ***Theory of Computing Systems***, vol. 37 (2004), pp. 641–674.

[3] J. Cannon et al., ***Word processing in groups***, Jones and Bartlett Publishers, Boston, MA, 1992.

[4] L. Fuchs, ***Infinite Abelian groups***, vol. 2, Academic Press, 1973.

[5] M. Gromov, *Groups of polynomial growth and expanding maps*, ***Publications Mathématiques IHÉS***, vol. 53 (1981), pp. 53–78.

[6] R. Hirshon, *Some cancellation theorems with applications to nilpotent groups*, ***Journal of Australian Mathematical Society*** (***series A***), vol. 23 (1977), pp. 147–165.

[7] W. Hodges, Model Theory, Cambridge University Press, Cambridge, 1993.

[8] B. R. Hodgson, ***Théories décidables par automate fini***, Ph.D. thesis, University of Montreal, 1976.

[9] ———, *Théories décidables par automate fini*, ***Annales des Sciences Mathématiques du Quebec***, vol. 7 (1983), pp. 39–57.

[10] M. Kargapolov and J. Merzljakov, ***Fundamentals of the theory of groups***, Springer-Verlag, 1979.

[11] R. Kaye, ***Models of Peano Arithmetic***, Oxford University Press, Oxford, 1991.

[12] A. Khelif, *Bi-interpretabilité et structures QFA*: *étude des groupes résolubles et des anneaux commutatifs*, to appear.

[13] B. Khoussainov and A. Nerode, *Automatic presentations of structures*, ***Logic and computational complexity*** (D. Leivant, editor), Lecture Notes in Computer Science, vol. 960, Springer-Verlag, 1995, pp. 367–392.

[14] B. KHOUSSAINOV, A. NIES, S. RUBIN, and F. STEPHAN, *Automatic structures: richness and limitations*, ***Proceedings of the 19th IEEE Symposium on Logic in Computer Science***, Lecture Notes in Computer Science, Springer-Verlag, 2004, pp. 110–119.

[15] S. LANG, ***Algebra***, Addison-Wesley, 1965.

[16] A. MAL'CEV, *On a correspondence between rings and groups*, ***American Mathematical Society Translations***, vol. 45 (1965), pp. 221–231.

[17] A. MOROZOV and A. NIES, *Finitely generated groups and first-order logic*, ***Journal of the London Mathematical Society***, vol. 71 (2005), no. 2, pp. 545–562.

[18] A. NIES, *Aspects of free groups*, ***Journal of Algebra***, vol. 263 (2003), pp. 119–125.

[19] ———, *Separating classes of groups by first-order formulas*, ***International Journal of Algebra and Computation***, vol. 13 (2003), pp. 287–302.

[20] ———, *Comparing quasi-finitely axiomatizable groups and prime groups*, ***Journal of Group Theory***, to appear.

[21] A. NIES and P. SEMUKHIN, *Finite automaton presentable abelian groups*, ***Proceedings of LFCS 2007***, to appear.

[22] A. NIES and R. THOMAS, *Finite automaton presentable groups and rings*, ***Journal of Algebra***, to appear.

[23] G. A. NOSKOV, *The elementary theory of a finitely generated almost solvable group*, ***Izvestiya Akademiya Nauk SSSR Seriya Matematika***, vol. 47 (1983), no. 3, pp. 498–517.

[24] F. OGER, *Équivalence élémentaire entre groupes finis-par-abéliens de type fini*, ***Commentarii Mathematici Helvetici***, vol. 57 (1982), no. 3, pp. 469–480.

[25] F. OGER, *Cancellation and elementary equivalence of finitely generated finite-by-nilpotent groups*, ***Journal of the London Mathematical Society***, vol. 30 (1991), pp. 293–299.

[26] ———, *Quasi-finitely axiomatizable groups and groups which are prime models*, ***Journal of Group Theory***, vol. 9 (2006), no. 1, pp. 107–116.

[27] F. OGER and G. SABBAGH, *Quasi-finitely axiomatizable nilpotent groups*, ***Journal of Group Theory***, vol. 9 (2006), no. 1, pp. 95–106.

[28] G. P. OLIVER and R. M. THOMAS, *Automatic presentations for finitely generated groups*, ***STACS 2005*** (V. Diekert and B. Durand, editors), Lecture Notes in Computer Science, vol. 3404, Springer-Verlag, 2005, pp. 693–704.

[29] D. ROBINSON, ***A course in the theory of groups***, Springer-Verlag, 1988.

[30] S. RUBIN, *Automatically presentable structures*, to appear.

[31] T. SCANLON, *Infinite finitely generated fields are bi-interpretable with N*, to appear.

[32] J. SILVER, *Counting the number of equivalence classes of Borel and coanalytic equivalence relations*, ***Annals of Pure and Applied Logic***, vol. 18 (1980), pp. 1–28.

[33] M. SIPSER, ***Introduction to the theory of computation***, PWS Publishing Company, 1997.

[34] W. THOMAS, *Automata on infinite objects*, ***Handbook of theoretical computer science*** (Jan van Leeuwen, editor), vol. A, Elsevier Science Publishers B.V., 1990, pp. 135–186.

[35] B. I. ZILBER, *An example of two elementarily equivalent but not isomorphic finitely generated metabelian groups*, ***Algebra i Logika***, vol. 10 (1971), pp. 309–315.

DEPARTMENT OF COMPUTER SCIENCE
AUCKLAND UNIVERSITY
AUCKLAND, NEW ZEALAND
E-mail: andre@cs.auckland.ac.nz