The search for FA presentable groups

André Nies
The University of Auckland

September 26, 2021

Abstract.

A group G is finite automata (FA) presentable if there is a regular set representing its domain, in such a way that the group operations can also be recognized by finite automata. Examples of such groups include the integers with addition, A^ω for any finite group A, and Prüfer groups C_{p^∞}. Several results restricting such groups have been obtained: e.g. N. and Thomas (2008) showed that each finitely generated subgroup is virtually abelian, and Tsankov (2011) solved a long standing conjecture by showing that $(\mathbb{Q}, +)$ is not FA presentable.

In contrast, N. and Semukhin (2009) gave examples of torsion-free indecomposable Abelian groups of rank ≥ 2 that are FA presentable. Their examples involved divisibility by several primes. It is still open whether a group of this kind can be obtained as a subgroup of $(\mathbb{Z}[1/p])^n$. We will report some potential progress on this question from ongoing work with Berdinsky, and with Lupini.

Outside the abelian, N. and Stephan (Logic Blog, 2019 and 2020) have recently given examples of FA presentable groups that are central extensions of one abelian group by another; e.g. extending $\mathbb{Z}/p\mathbb{Z}^\infty$ by $\mathbb{Z}/p\mathbb{Z}$ where $\mathbb{Z}/p\mathbb{Z}$ denotes the cyclic group of p elements. We will explain the connection between FA presentability of a central extension of FA presentable groups and of the corresponding 2-cocycle, and also give an example, varying the one above, where the 2-cocycle is so complex that the extension is not FA presentable. All these examples are torsion groups. It is open whether each torsion-free FA presentable group is virtually abelian.

I. Background on FA presentable structures

Definition of FA presentable (or automatic) structures

A countable structure in a finite signature is finite-automaton presentable (or automatic) if

- the elements of the domain can be represented by the strings in a regular language D, in such a way that
- finite automata can also check if the atomic relations hold.

Note that $s = t$ for terms s, t is an atomic relation.
So we allow equality to be a nontrivial equivalence relation.

Some detail of the definition

- For checking the relations, the strings representing elements are written on tracks.
- The FAs utilize symbols such as $\begin{smallmatrix} a \\ b \\ a \end{smallmatrix}$ or $\begin{smallmatrix} c \\ b \\ \lozenge \end{smallmatrix}$ in the powers of the given alphabet.
- If necessary one extends some tracks by $\lozenge$'s to get them to the same lengths.

- The definition was introduced in a thesis of Hodgson (1976) for a new proof of decidability of the theory of $(\mathbb{N}, +)$;
- Khoussainov/Nerode (1995) founding paper of the area.

Example: $(\mathbb{N}, +)$

We represent numbers in binary, with the least significant digit first.

0 is represented by the empty string. Thus

- The alphabet is $\{0, 1, \Diamond\}$
- The domain consists of the strings ending in 1, and the empty string
- A finite automaton checks the correctness of the sum via the carry bit procedure, where the carry bit moves to the right. $\Diamond$ is treated like 0.
- E.g. the automaton checks 5+22=27 by accepting the string

$$\begin{array}{ccccc} 1 & 0 & 1 & \Diamond & \Diamond \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{array}$$

Model checking problem, interpretations

- Given an FA presented structure $\mathcal{A}$ and a formula ϕ (possibly with parameters), one can effectively determine an FA recognizing the relation on $\mathcal{A}$ defined by ϕ (model checking).
- The proof is by induction on $|\phi|$. To deal with existential quantifiers, one uses that each NFA is equivalent to a DFA.
- One can also use quantifiers $\exists^\infty x$ in the formula ϕ.
- This uses that any FA presentation implicitly contains the regular relation "x is longer than y" on the domain.

Proposition

If a structure is first-order interpretable in an FA presentable structure, then it is FA presentable as well.

II. Complexity of the isomorphism relation

Complexity of the isomorphism relation on classes of FA presentable structures

FA presentable structures of various types have been studied, including:
Boolean algebras, graphs, groups (in particular, abelian) and rings.

- Some classes of FA presentable structures turn out to be very complex, in the sense that it is hard to detect if two members are isomorphic. This can be undecidable (e.g. for eqrels), and in the worst case, Σ_1^1 complete!
- In the opposite direction, one can try to classify all structures in the class. If success, one can try show that the isomorphism problem is decidable.

Classifying Boolean Algebras

Let W be the Boolean algebra of finite or cofinite subsets of $\mathbb{N}$.

Theorem (Khoussainov, Nies, Rubin, Stephan, 2004)

An infinite Boolean algebra B is FA presentable $\iff$ $B \cong W^n$ for some n.

In particular, the dense countable Boolean algebra is not FA presentable.

Corollary

The isomorphism problem for FA presented Boolean algebras is decidable.

Proof.

- Given an FA presentation of a structure A in the signature of Boolean algebras, one can decide if A is a Boolean algebra
- One computes the largest n such that $A \models$ "there are n disjoint elements with infinitely many atoms below."
- This n essentially determines A up to isomorphism.

$\square$

Towards deciding the complexity of isomorphism

For several interesting classes, for instance FA presentable groups, abelian groups, and rings, we cannot yet determine the complexity of the isomorphism relation.

We can approach the problem from two opposite directions:

- Find examples of structures in that class
- prove results limiting structures in the class.

Complex classes

Theorem (Khoussainov, Nies, Rubin, Stephan)

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).

- The proof can be modified to obtain undirected graphs instead of successor trees
- These can be coded into commutative monoids and lattices of height 4, preserving FA presentability
- So the isomorphism problem for FA presentable structures in all these classes is Σ_1^1-complete.

III. FA presentable groups:

Examples, constructions

FA presentable groups: Examples

The following are FA presentable:

- $(\mathbb{Z}, +)$
- For $k \in \mathbb{N}, k \geq 2$,
$$R_k = \mathbb{Z}[1/k] = \{z/k^i \,:\, z \in \mathbb{Z}, i \in \mathbb{N}\}.$$
- Prüfer groups $\mathbb{Z}(k^\infty) = R_k/\mathbb{Z}$
- $S^{(\omega)}$ where S is finite group

FA presentations of these groups

- For $\mathbb{Z}(k^\infty)$ the alphabet is $\{0, \ldots, k-1, \Diamond\}$. Elements are represented by strings, with most significant digit first. The domain consists of the strings ending in 1, and the empty string represent 0.
- A finite automaton checks the correctness of the sum, via the carry bit procedure, where the carry goes to the left. The leftmost carry is ignored. For instance, if $k = 2$,

$$[5/8]+[1/2]=[1/8] \text{ is verified thus: } \quad \begin{array}{ccc} 1 & 0 & 1 \\ 1 & \Diamond & \Diamond \\ \hline 0 & 0 & 1 \end{array}$$

- For $\mathbb{Z}[\frac{1}{k}]^+$, the domain consists of strings with two tracks, the first for the integers in binary, and the second for the fractional part.
- The leftmost carry moves from second track to the first.

Three constructions of new FA presentable groups

We show how to obtain new FA presentable (mostly abelian) groups G from given ones.
Each time we will provide an example of an application.

Three constructions

- G is an abelian group with an FA -presentable subgroup of finite index.
- G is the sum of two FA presentable subgroups of an abelian group L, with regular intersection.
- G is a central extension of one abelian group by another, with regular 2-cocycle.

Construction 1: FA -presentable subgroup of finite index

Let G be an abelian group with an FA presentable subgroup of finite index. Then G is FA presentable.

We use this to show that an example from Fuchs [1971,2015] is FA presentable.

- Let $\mathbf{e}_0, \mathbf{e}_1$ be the standard base of $\mathbb{Q}^2$.
- For $\mathbf{a} \in \mathbb{Q}^2$, let $p^{-\infty}\mathbf{a} := \{\mathbf{a}, p^{-1}\mathbf{a}, p^{-2}\mathbf{a}, \ldots\}$.
- Thus, $\langle p^{-\infty}\mathbf{a}\rangle \cong (\mathbb{Z}[\frac{1}{p}], +)$ for $\mathbf{a} \neq 0$.
- Fix distinct primes p_0, p_1, q.
- Let G be the group generated by $p_0^{-\infty}\mathbf{e}_0 \cup p_1^{-\infty}\mathbf{e}_1 \cup q^{-1}(\mathbf{e}_0 + \mathbf{e}_1)$
- G is FA presentable because its subgroup $\langle p_0^{-\infty}\mathbf{e}_0, p_1^{-\infty}\mathbf{e}_1\rangle$ has finite index in it.

G is not a proper direct product (Fuchs).

Construction 2: sum of two FA presented subgroups

Let A, B be FA presented subgroups of an abelian group L.
Suppose that

$$U = \{\langle x, -x\rangle : x \in A \cap B\}$$

is a regular subset of $A \times B$.
Then the subgroup $G = A + B$ of L is FA presentable.

Proof: $G \cong$ the amalgam $A \times B/U$. So G can be interpreted in the FA presentable structure $(A \times B, +, U)$. Q.e.d.

- E.g. let $L = \mathbb{Q}, A = R_2, B = R_3$. Then $U \cong \mathbb{Z}$ and $G \cong R_6$.
- The FA-representation obtained is different from the one of R_6 in base 6: in the latter case R_2 is not a regular subgroup.

An FA presentable rigid abelian group of rank 2

Recall: sum of two FA presented subgroups

L abelian, $A, B \leq L$ FA presented, $\{\langle x, -x\rangle : x \in A \cap B\}$ regular $\Rightarrow G = A + B$ is FA presentable.

$L = \mathbb{Q}^2$, $\mathbf{e}_0, \mathbf{e}_1$ standard base of $\mathbb{Q}^2$, distinct primes p_0, p_1, q.

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

Since $A \cap B = \mathbb{Z}(\mathbf{e}_0 + \mathbf{e}_1)$, $\{\langle x, -x\rangle : x \in A \cap B\}$ is regular.

So $G = A + B$ is FA presentable.

- G has rank 2, and the only endomorphisms are the trivial ones, multiplication by an integer.
- This implies each subgroup of finite index is indecomposable.

Construction 3: Central extensions of FA presented abelian groups

- Let N, Q be FA presentable abelian groups.
- Let E be a central extension of Q by N, given by an exact sequence $0 \to N \to E \to Q \to 0$ with $N \leq Z(E)$ (the centre).
- Suppose some 2-cocycle $c\colon Q \times Q \to N$ describing this extension is FA recognizable.

Then E is FA-presentable.

Proof: E can be constructed as the set $Q \times N$ with the operation

$$(q_0, r_0) \cdot (q_1, r_1) = (q_0 + q_1, r_0 + r_1 + c(q_0, q_1)).$$

So E can be interpreted in the FA presentable two-sorted structure

$$(Q \sqcup N, +_Q, +_N, c).$$

How to determine a 2-cocycle $c\colon Q \times Q \to N$

Given: exact sequence $0 \to N \to E \to Q \to 0$ with $N \leq Z(E)$.

- Pick a set T of coset representatives for N in E.
- Fix a bijection $f\colon Q \to T$. Write $\overline{q} = f(q)$.
- The 2-cocycle is given by

$$c(q_0, q_1) \colon = \overline{q_0} \cdot \overline{q_1} \cdot (\overline{q_0 + q_1})^{-1} \in N.$$

  - Choosing a different set of coset representatives leads to an equivalent 2-cocycle. I.e., their difference is a “2-coboundary”, which merely describes the direct product $Q \times N$.
  - $\mathrm{Ext}(Q, N)$ is the abelian group of extensions of Q by N up to equivalence, namely “ 2-cocycles/ 2-coboundaries”.
  - To obtain an FA presentation for E, one has to choose T right, so that c can be computed by an FA.

Apply Construction 3 to obtain an FA presentable group E that does not have an abelian subgroup of finite index (N., Thomas 08).
E has generators x, y_i, z_k $(i, k \in \mathbb{N})$ subject to the relations

$$y_i^2 = z_k^2 = 1 \qquad [y_i, z_k] = [y_i, x] = 1 \qquad z_i^{-1} x z_i = x y_i$$

We have an exact sequence $0 \to N \to E \to Q \to 0$ where
$N = Z(E) = \langle x^2, \{y_i\}_{i \in \mathbb{N}} \rangle$, $Q := E/N = \langle v \rangle \times \langle z_i \rangle$, here $v^2 = 1$.

- Elements of Q have normal form $q_{s,\alpha} = v^s \cdot \prod_i z_i^{\alpha_i}$ where $s = 0, 1$ and α is a bit string (thought to be extended by 0s if necessary).
- Write $\overline{q_{s,\alpha}} = x^s \prod_i z_i^{\alpha_i} \in E$.
- Some FA can compute c using that $z_i x = x z_i y_i$:
- the 2-cocycle is

$$c(q_{s,\alpha}, q_{t,\beta}) = \overline{q_{s,\alpha}} \cdot \overline{q_{t,\beta}} \cdot (\overline{q_{s,\alpha} + q_{t,\beta}})^{-1} = x^{2s+t} \prod_i y_i^{\gamma_i}$$

where $\gamma_i = (s + 2t)\alpha_i + (s + t)\beta_i \mod 2$.

Unitriangular groups

For a ring R with 1, let

$$\mathrm{UT}_3(R) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in R \right\}.$$

This is nilpotent group of class 2. If $R = C_n$ or $R = \mathbb{Z}$, it is generated by x_0, x_1, z where

$$x_0 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, x_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The centre is $\langle z \rangle$, and we have $[x_0, x_1] = y$.

In the following fix a prime $p \neq 2$. Define nilpotent-2 groups G_p, H_p, L_p of exponent p as variants of $\mathrm{UT}_3(\mathbb{Z}/p\mathbb{Z})$.
They have infinitely many generators x_i, $i \in \mathbb{N}$. Write $y_{i,k} = [x_i, x_k]$. These are in the centre.

- G_p: all the $y_{i,k}$, $i < k$, are equal to an element $z \neq 1$.
- H_p: we have $y_{i,k} = z_k$ for $i < k$ and the z_k are linearly independent over $\mathbb{Z}/p\mathbb{Z}$.
- L_p : the $y_{i,k}$ for $i < k$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$. So L_p is the free nilpotent-2 group of rank ∞ and exponent p.

Theorem (N. and Stephan, 2020)

- G_p and H_p are FA presentable.
- L_p is not FA presentable.

G_p is FA presentable by the cocycles method

For G_p we have $[x_i, x_k] = z$ for $i < k$. We have an exact sequence $0 \to N \to G_p \to Q \to 0$; $N = Z(G_p) = \langle z \rangle$, $Q := G_p/N = \langle x_i \rangle$.

- Elements of Q have the normal form $q_\alpha = \prod_i x_i^{\alpha_i}$ where α is a sequence of digits $0, \ldots, p-1$, the last one not 0.
- Write $\overline{q_\alpha} = \prod_i x_i^{\alpha_i} \in E$.
- The 2-cocycle $c\colon Q \times Q \to N$ is $c(q_\alpha, q_\beta) = z^{\sum_{k>0} \alpha_k (\sum_{i=0}^{k-1} \beta_i)}$ where arithmetic is modulo p. To see this, use that $x_k x_i z = x_i x_k$ in E:
- calculate $\prod_k x_k^{\alpha_k} \prod_i x_i^{\beta_i}$ by, for decreasing positive k, moving $x_k^{\alpha_k}$ to the right past the $x_i^{\beta_i}$ for $i = 0, \ldots, k-1$. Each such move creates a factor $z^{\alpha_k \beta_i}$ in $c(q_\alpha, q_\beta)$.
- An FA can compute c. Its input has tracks α and β; the state of the FA records $\sum_{r \geq k > 0} \alpha_k (\sum_{i=0}^{k-1} \beta_i)$ for increasing r.

H_p is FA presentable

For H_p we have $[x_i, x_k] = z_k$ for $i < k$ where the z_k are l.i.

- The 2-cocycle is

$$c(q_\alpha, q_\beta) = \prod_{k>0} z_k^{\alpha_k (\sum_{i<k} \beta_i)}.$$

- It can be computed by an FA similar to the one above:
- Record $\sum_{i<k} \beta_i$ in the state, and write $\alpha_k \sum_{i<k} (\beta_i)$ as an exponent of z_k. (Recall arithmetic is mod p.)

IV. FA presentable groups:

Non-examples, restrictions

L_p is not FA presentable

Recall that L_p is the group where the $y_{i,k} = [x_i, x_k]$ for $i < k$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$.

Theorem (N. and Stephan, 2020)

The group L_p is not FA presentable.

- The idea is that in any presentation, the strings representing the $y_{i,k}$ are short.
- Hence their linear combinations are also short.
- There are too many short linear combinations for the number of strings available.

For detail see Logic Blog 2020, available at arxiv.org/abs/2101.09508

A strong restriction on the f.g. subgroups

Recall that for a class $\mathcal{C}$, a group is virtually $\mathcal{C}$ if it has a subgroup of finite index in $\mathcal{C}$.
Oliver and Thomas (2005) proved that each finitely generated FA presentable group is virtually abelian. The following improves this result.

Theorem (Nies, Thomas, 2008)

- Each finitely generated subgroup of an FA presentable group G is virtually abelian.
- In fact, the torsion-free rank of the abelian part is at most $\log(|\Sigma|)(k+1)$, where Σ is the alphabet and k is the number of states of an FA recognizing the group operation.

Theorem (Recall)

Each finitely generated subgroup of an FA presentable group G is virtually abelian.

- Any subgroup H of G generated by $\{g_1, \ldots, g_r\}$ has polynomial growth, namely

  $$\{t(g_1, \ldots, g_r) : |t| \leq n\} \text{ has size polynomial in } n.$$

  So by a famous result of Gromov, it is virtually nilpotent.
- a finitely generated virtually nilpotent group either embeds $\mathrm{UT}_3(\mathbb{Z})$ or is virtually abelian.
- If G embeds $\mathrm{UT}_3(\mathbb{Z})$ then G is not FA presentable.

Restrictions on torsion free abelian groups

Tsankov (2008) proved that $(\mathbb{Q}, +)$ is not FA presentable, and more generally, any FA presentable torsion free abelian group is only divisible by finitely many primes. This used Freiman's 1966 theorem (additive combinatorics)

Using similar methods:

Theorem (Braun and Strüngmann, 2011)

Each FA presentable torsion free abelian group G is an extension of a finite direct sum of Prüfer groups $\mathbb{Z}(k^\infty)$ by a f.g. free abelian group. I.e. there is exact sequence $0 \to \mathbb{Z}^n \to G \to \bigoplus_i \mathbb{Z}(k_i^\infty) \to 0$.

In particular, if G has rank 1 then $G = \mathbb{Z}[1/k]$ for some k.

FA presentable subgroups of $(\mathbb{Z}[1/p])^n$

- We still don't know if some FA presentable indecomposable subgroup $U \leq (\mathbb{Z}[1/p])^n$ exists, where U has rank ≥ 2. The following might help to resolve this.
- Recent work with Berdinsky, and separately with Lupini (Logic Blog 2021), focusses on $\mathrm{Ext}(\mathbb{Z}(p^\infty), \mathbb{Z})$, the group of extensions of the Prüfer group $\mathbb{Z}(p^\infty)$ by $\mathbb{Z}$, and also $\mathrm{Ext}(\mathbb{Z}[\frac{1}{p}], \mathbb{Z})$.
- The following effectivizes a well-known classical theorem; see e.g. Fuchs 2015, Cor 9.3.15.

Theorem (Lupini and N., see Logic Blog 2021)

The group of p-adic integers is computably isomorphic to $\mathrm{Ext}(\mathbb{Z}(p^\infty), \mathbb{Z})$:
from the p-adic one can effectively determine a 2-cocycle.