Finite automata presentable abelian groups*

André Nies¹ and Pavel Semukhin²

- Department of Computer Science, University of Auckland, New Zealand, andre@cs.auckland.ac.nz
- Department of Computer Science, University of Auckland, New Zealand, pavel@cs.auckland.ac.nz

Abstract. We give new examples of FA presentable torsion-free abelian groups. Namely, for every $n \ge 2$, we construct a rank n indecomposable torsion-free abelian group which has an FA presentation. We also construct an FA presentation of the group $(\mathbb{Z}, +)^2$ in which every nontrivial cyclic subgroup is not FA recognizable.

1 Introduction

The study of finite-automata (FA) presentable, or automatic, structures began in the works by Hodgson [5,6] and then carried on in Khoussainov and Nerode [7]. A structure is called FA presented if its domain and atomic relations are recognized by finite automata operating synchronously on their input. So, these structures have finite presentations. The class of automatic structures is of special interest in the field of theoretical computer science. One of the reasons for this is that the first-order theory of an FA presentable structure is decidable, and in fact the model checking problem is decidable. For instance, Hodgson [5,6] was the first to use this property to give a new proof of the decidability of Presburger arithmetic $\operatorname{Th}(\mathbb{N},+)$.

There is a complete description of FA presentable structures in the classes of Boolean algebras [9] and well-ordered sets [3], but for another classes of structures such as groups, rings, linear orders, etc., the situation is far from clear. For example, it is unknown whether the group of rationals under addition has an FA presentation. In [8] Khoussainov and Rubin posed the problem of characterizing automatic abelian groups (Problem 4).

In this paper we describe a new method for constructing FA presentable abelian groups and monoids using the notion of amalgamated product. We show that under certain conditions the amalgamated product of FA presentable groups or monoids is itself FA presentable. We then use this method to give new examples of FA presentable torsion-free abelian groups. The only known examples of such groups were $(\mathbb{Z},+)$, $(R_p,+)$ (the group of rationals with denominators powers of p), and their finite direct products. Our examples are indecomposable and strongly indecomposable torsion-free abelian groups.

^{*} This research was partially supported by the Marsden Fund of New Zealand, grant no. UOA-319.

In the last section we will construct an FA presentation of the group $(\mathbb{Z}, +)^2$ which is new in the sense that any nontrivial cyclic subgroup in that presentation is not FA recognizable.

We now give formal definitions that will be used in this paper.

Definition 1.1. Let Σ be a finite alphabet, and $\bar{a} = (a_1, \ldots, a_k)$ be a tuple of words from Σ^* . A **convolution** of \bar{a} is a word in alphabet $(\Sigma \cup \{\Box\})^k$ which is constructed by placing the words a_1, \ldots, a_k one under another and adding a special symbol \Box at the end of the words to get the same length. For example,

$$Conv(01, 1011, 100) = \begin{array}{c} 0 \ 1 \ \square \ \square \\ 1 \ 0 \ 1 \ 1 \\ 1 \ 0 \ 0 \ \square \end{array}$$

A convolution of a relation $R \subseteq (\Sigma^*)^k$ is defined as $\operatorname{Conv}(R) = \{\operatorname{Conv}(\bar{a}) : \bar{a} \in R\}$.

Definition 1.2. A relation $R \subseteq (\Sigma^*)^k$ is **FA** recognizable, or regular, if Conv(R) is recognized by a finite automaton.

Definition 1.3. A structure $A = (A; R_1, \ldots, R_n, f_1, \ldots, f_m)$ is **FA** presented if, for a finite alphabet Σ , $A \subseteq \Sigma^*$ is an FA recognizable set of word in Σ^* , and all the relations R_1, \ldots, R_n together with the graphs of operations f_1, \ldots, f_m are recognized by finite automata.

A structure A is **FA** presentable if it is isomorphic to an FA presented structure.

In some cases to prove that a given structure is FA presentable we will not construct its automatic presentation explicitly. Instead we give its first-order interpretation in a structure already known to be FA presented. The description of this method together with formal definitions and proofs can be found in [2].

2 An FA presentation of the group R_p

Definition 2.1. Let R_p be the subgroup of $(\mathbb{Q}, +)$ consisting of elements of the form k/p^i .

In the literature R_p is also denoted by $\mathbb{Q}^{(p)}$ (for example, see [4]) or $\mathbb{Z}[1/p]$. The next theorem shows that R_p is FA presentable, and we will use this particular presentation of R_p in section 5 to construct new examples of FA presentable abelian groups.

Theorem 2.1. R_p is FA-presentable.

First, we will construct an automatic presentation of R_p^+ , the submonoid of R_p consisting of elements greater than or equal to 0. Later we describe how to obtain an FA presentation of the entire group R_p from the one for R_p^+ .

The alphabet of the FA presentation for R_p^+ will be $\Sigma = \{\binom{n}{m} : n \in \{0,1\} \text{ and } m \in \{0,\ldots,p-1\}\}$. Every element $z \in R_p^+$ will be represented by two lines of digits,

n_1	n_2	 n_k
m_1	m_2	 m_k

where $n_1n_2\ldots n_k$ represents the integral part of z in binary presentation with the least significant digit first, and $m_1m_2\ldots m_k$ represents the fractional part of z in base p with the most significant digit first. If needed, we put additional zeros to the right to make the lengths of integral and fractional part equal. For example, if p=3 then the element $14\frac{17}{27}\in R_3^+$ is represented by

$$\begin{array}{c|c|c} 0 & 1 & 1 & 1 \\ \hline 1 & 2 & 2 & 0 \\ \end{array}$$

Let the domain D of an FA presentation of R_p^+ consist of all words in Σ^* not ending in $\binom{0}{0}$, except for $\binom{0}{0}$ itself which represents 0. Clearly, D is FA recognizable.

Let Add be the graph of the addition operation. We prove that Add is FA recognizable. First, we construct an auxiliary automaton \mathcal{A} whose alphabet is $(\Sigma \cup \{\Box\})^3$. The states of \mathcal{A} are q_0 , (0,0), (0,1), (1,0), (1,1), where q_0 is an initial state and (0,0) is a final state. The state (α,β) means that we have a carry bit α in the addition of integral parts, and a carry bit β in the addition of fractional parts.

The transitions of \mathcal{A} are defined below. It is assumed there that the special symbol \square is identical to the symbol $\binom{0}{0}$.

There is a transition from q_0 to (α, β) with the label $\left(\binom{n_1}{m_1}, \binom{n_2}{m_2}, \binom{n_3}{m_3}\right)^{\top}$ if and only if

$$\begin{cases} n_1 + n_2 = 2\alpha + n_3 \\ m_1 + m_2 + \beta = m_3 \end{cases} \text{ or } \begin{cases} n_1 + n_2 + 1 = 2\alpha + n_3 \\ m_1 + m_2 + \beta = p + m_3 \end{cases}.$$

This means that from the first letter of the input \mathcal{A} guesses the carry bit from the fractional part to the integral part: in the first case the carry bit is 0, while in the second case the carry bit is 1.

There is a transition from (α, β) to (α', β') with the label $(\binom{n_1}{m_1}, \binom{n_2}{m_2}, \binom{n_3}{m_3})^{\top}$ if and only if

$$\begin{cases} n_1 + n_2 + \alpha = 2\alpha' + n_3 \\ m_1 + m_2 + \beta' = p\beta + m_3 \end{cases}$$

Now as one can see $\operatorname{Conv}(Add) = L(\mathcal{A}) \cap \operatorname{Conv}(D^3)$. Therefore, since D^3 is FA recognizable, then so is Add.

Let us define an FA presentation for R_p . Consider the presentation of R_p^+ given above; let $\pi: D^2 \to D^2$ be the following function

$$\pi(x,y) = \begin{cases} (x-y,0) & \text{if } x \geqslant y, \\ (0,y-x) & \text{if } x < y. \end{cases}$$

Note that the graph of π is an FA recognizable subset of D^4 since it can be defined in terms of Add and \leq relations which are FA recognizable in our presentation of R_p^+ . Now the domain of the FA presentation of R_p is

$$\{(x,y): x,y \in D \text{ and } (x=0 \lor y=0)\}$$

with addition operation defined as

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$
 if and only if $(x_3, y_3) = \pi(x_1 + x_2, y_1 + y_2)$.

3 Amalgamations of monoids and abelian groups

Before turning to abelian groups let us consider commutative monoids which have cancellation property, namely, a + c = b + c implies a = b for all elements a, b, c. In what follows, by **monoid** we will mean **commutative monoid with cancellation property**.

Proposition 3.1. Let M, N, and U be monoids, and $f: U \to M$, $g: U \to N$ be isomorphic embeddings. Consider the direct product $M \times N$ of the monoids and a relation \sim_U on $M \times N$ defined as follows:

$$(x_0, y_0) \sim_U (x_1, y_1) \iff \exists u, v \in U \ (x_0 + f(u) = x_1 + f(v) \land y_0 + g(u) = y_1 + g(v))$$

Then \sim_U is a congruence on $M \times N$, and $M \oplus_U N$, the **amalgamated product** of M and N over U, is the quotient structure $M \times N/\sim_U$, which also is a commutative monoid with cancellation property.

Proof. It is straightforward to show that \sim_U is a congruence, and that $M \oplus_U N$ is a commutative monoid. We prove that it possesses cancellation property. Suppose $(x_0, y_0) + (z, w) \sim_U (x_1, y_1) + (z, w)$; then $x_0 + z + f(u) = x_1 + z + f(v)$ and $y_0 + w + g(u) = y_1 + w + g(v)$ for some $u, v \in U$. Since M and N possess cancellation property, we have that $x_0 + f(u) = x_1 + f(v)$ and $y_0 + g(u) = y_1 + g(v)$, that is $(x_0, y_0) \sim_U (x_1, y_1)$.

We will use the notation $\langle x,y\rangle_U$ to denote the equivalence class of $(x,y)\in M\times N$ with respect to \sim_U .

Proposition 3.2. Let $M \oplus_U N$ be an amalgameted product of monoids M and N over U. Then there are submonoids \widetilde{M} and \widetilde{N} in $M \oplus_U N$ such that $\widetilde{M} \cong M$, $\widetilde{N} \cong N$, and $M \oplus_U N = \widetilde{M} + \widetilde{N}$.

Proof. Let $\widetilde{M} = \{\langle x, 0 \rangle_U : x \in M\}$ and $\widetilde{N} = \{\langle 0, y \rangle_U : y \in N\}$; as one can see, \widetilde{M} and \widetilde{N} are submonoids of $M \oplus_U N$, and $M \oplus_U N = \widetilde{M} + \widetilde{N}$. Consider the mappings $\varphi : M \to \widetilde{M}$ and $\psi : N \to \widetilde{N}$ such that $\varphi(x) = \langle x, 0 \rangle_U$ and

П

 $\varphi(y) = \langle 0, y \rangle_U$. Clearly, φ and ψ are epimorphisms. Let us show, for instance, that φ is one-to-one. Suppose $\langle x, 0 \rangle_U = \langle x', 0 \rangle_U$; then x + f(u) = x' + f(v) and g(u) = g(v) for some $u, v \in U$. Therefore, u = v and the cancellation property implies that x = x'.

In the case of abelian groups we can define the notion of amalgamated product in a slightly different manner.

Definition 3.1. Let A, B, and U be abelian groups and $f: U \to A$, $g: U \to B$ be isomorphic embeddings. Then $A \oplus_U B$, the **amalgamated product** of A and B over U, is the quotient group $A \oplus B/\widetilde{U}$, where $\widetilde{U} = \{(f(u), g(u)) \mid u \in U\}$.

The next proposition is the strengthening of 3.2 for abelian groups.

Proposition 3.3. Let $A \oplus_U B$ be an amalgameted product of A and B over U. Then there are subgroups \widetilde{A} and \widetilde{B} in $A \oplus_U B$ such that $\widetilde{A} \cong A$, $\widetilde{B} \cong B$, $A \oplus_U B = \widetilde{A} + \widetilde{B}$ and $\widetilde{A} \cap \widetilde{B} \cong U$.

Proof. By definition $A \oplus_U B = A \oplus B/\widetilde{U}$. Let $\widetilde{A} = \{(a,0) + \widetilde{U} \mid a \in A\}$ and $\widetilde{B} = \{(0,b) + \widetilde{U} \mid b \in B\}$. As one can see, $A \oplus_U B = \widetilde{A} + \widetilde{B}$ and $\widetilde{A} \cong A$, $\widetilde{B} \cong B$. We now prove that $\widetilde{A} \cap \widetilde{B} \cong U$. Let $x \in \widetilde{A} \cap \widetilde{B}$, then $x = (a,0) + \widetilde{U}$ and $x = (0,b) + \widetilde{U}$; hence $(a,-b) \in \widetilde{U}$ and a = f(u), b = -g(u). Therefore, $x = (f(u),0) + \widetilde{U}$ and $\widetilde{A} \cap \widetilde{B} = \{(f(u),0) + \widetilde{U} \mid u \in U\}$, which is isomorphic to U.

Remark 3.1. The intersection $M \cap N$ of the submonoids of $M \oplus_U N$ defined in the proof of Proposition 3.2 does not necessarily isomorphic to U. To show this let M, N, U be $(\mathbb{N},+)$, and f, g be the identity embeddings. As one can see, $M \oplus_U N$ is isomorphic to $(\mathbb{Z},+)$ because $\langle x,y\rangle_{\mathbb{N}} = \langle x',y'\rangle_{\mathbb{N}}$ iff x-y=x'-y', and we can identify $\langle x,y\rangle_{\mathbb{N}}$ with $x-y\in\mathbb{Z}$. In this case \widetilde{M} and \widetilde{N} correspond to the submonoids of non-negative and non-positive numbers respectively. Thus $\widetilde{M} \cap \widetilde{N} = \{\langle 0,0\rangle_{\mathbb{N}}\} \not\cong \mathbb{N}$.

The converse of 3.3 also holds.

Proposition 3.4. Let L be an abelian group, A, B subgroups of L, and $U = A \cap B$. Then

$$A + B \cong A \oplus_{U} B$$
,

where the embeddings f, g of U into A and B are the identity mappings.

Proof. In this case $A \oplus_U B = A \oplus B/\widetilde{U}$, where $\widetilde{U} = \{(u, u) \mid u \in U\}$. Let $\varphi : A \oplus_U B \to A + B$ be defined as follows:

$$\varphi((a,b) + \widetilde{U}) = a - b.$$

We show that φ is an isomorphism. First, note that it is well defined: if $(a,b)+\widetilde{U}=(a',b')+\widetilde{U}$ then (a-a',b-b')=(u,u) for some $u\in U$; therefore a-b=(a'+u)-(b'+u)=a'-b'.

It is easy to see that φ is an epimorphism. We now prove that it is one-to-one. Let a-b=a'-b'; then $a-a'=b-b'\in A\cap B=U.$ Therefore, $(a-a',b-b')=(u,u)\in \widetilde{U}$ and $(a,b)+\widetilde{U}=(a',b')+\widetilde{U}.$

Remark 3.2. If M, N, and U are abelian groups then both definitions of amalgamated product, that is the one for groups and the one for monoids, give us the same structure $M \oplus_U N$.

4 Constructions of FA presentable monoids and abelian groups

In this section we will prove a version of Proposition 3.2 for FA presentable structures.

Theorem 4.1. If M, N, and U are FA presented monoids and $f: U \to M$, $g: U \to N$ are isomorphic embeddings that are FA recognizable subsets of $U \times M$ and $U \times N$ respectively, then the amalgamated product $M \oplus_U N$ is FA presentable. Moreover, $M \oplus_U N$ contains FA recognizable submonoids \widetilde{M} and \widetilde{N} such that $\widetilde{M} \cong M$, $\widetilde{N} \cong M$ and $M \oplus_U N = \widetilde{M} + \widetilde{N}$.

Proof. We prove that $M \oplus_U N$ is FA presentable by constructing an interpretation of it in the FA presentable structure $E = M \sqcup N \sqcup U$ enriched with unary predicates for subsets M, N, U and binary predicates R_f and R_g for the graphs of f and g. Let R^M and R^N be the graphs of the addition operation in M and N respectively.

The domain for $M \oplus_U N$ is defined in E^2 by the formula $\Delta(x_0, y_0) = M(x_0) \wedge N(y_0)$. Addition is defined by

$$\Phi(x_0, y_0, x_1, y_1, x_2, y_2) = R^M(x_0, x_1, x_2) \wedge R^N(y_0, y_1, y_2).$$

Equality is defined by

$$\epsilon(x_0, y_0, x_1, y_1) = \exists u, v \ (U(u) \land U(v) \land x_0 + f(u) = x_1 + f(v)$$
$$\land y_0 + g(u) = y_1 + g(v)$$

or more formally

$$\epsilon(x_0, y_0, x_1, y_1) = \exists u, v, w_0, w_1, w_2, w_3, z_0, z_1 \ (U(u) \land U(v) \land R_f(u, w_0)$$

$$\land R_f(v, w_1) \land R_g(u, w_2) \land R_g(v, w_3) \land R^M(x_0, w_0, z_0)$$

$$\land R^M(x_1, w_1, z_0) \land R^N(y_0, w_2, z_1) \land R^N(y_1, w_3, z_1)).$$

From the proof of Proposition 3.2 it follows that \widetilde{M} and \widetilde{N} are defined by the formulas

$$(z_0, z_1) \in \widetilde{M} \iff \exists x, u, v \ (M(x) \land U(u) \land U(v) \land$$

$$z_0 + f(u) = x + f(v) \land z_1 + g(u) = g(v)),$$

$$(z_0, z_1) \in \widetilde{N} \iff \exists y, u, v \ (N(y) \land U(u) \land U(v) \land$$

$$z_0 + f(u) = f(v) \land z_1 + g(u) = y + g(v)).$$

Theorem 4.2. Let A and B be abelian groups such that B is a subgroup of A and |A:B| is finite. If B is FA presentable, then so is A.

Proof. Let r_0, \ldots, r_k be representatives of the cosets of B in A. Then there are a function $g: \{0, \ldots, k\}^2 \to \{0, \ldots, k\}$ and elements $b_{ij} \in B$ with the following property: for every i and j,

$$r_i + r_j = r_{g(i,j)} + b_{ij}.$$

We may assume that the FA presentation of B uses an alphabet Σ , such that $0, \ldots, k \notin \Sigma$, and that the domain of this presentation is $D \subseteq \Sigma^*$. Let the alphabet of the FA presentation of A be $\Sigma \cup \{0, \dots, k\}$. Each 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,

$$(r_i + b_1) + (r_j + b_2) = r_{g(i,j)} + b_{ij} + b_1 + b_2.$$

Hence the graph of addition operation can be recognized by a finite automaton.

Example 4.1 (Two different presentations of R_6). Consider the presentation of R_6 described in Section 2. We will show that R_6 in this presentation does not have FA recognizable subgroup isomorphic to R_2 . Suppose M is an FA recognizable subgroup of R_6 and $M \cong R_2$. Let $M^+ = \{(x,0) : (x,0) \in M\}$; then M^+ is FA recognizable and $M^+ \cong R_2^+$. Note that we can identify the FA presentation of R_6^+ and the FA recognizable submonoid of R_6 with domain $\{(x,0):(x,0)\in R_6\}$. This implies that R_6^+ has an FA recognizable submonoid isomorphic to R_2^+ . Now if $M^+ \leq R_6^+$ is isomorphic to R_2^+ , then for some $n_0, k_0 \in \mathbb{N}$

$$M^{+} = \frac{n_0}{6^{k_0}} \cdot R_2^{+} = \left\{ \frac{n_0 n 3^k}{6^{k_0 + k}} : k, n \in \mathbb{N} \right\}.$$

For each k and let α_k be the smallest element of M^+ of the length $k_0 + k$ in this presentation. Obviously, $\alpha_k = n_0 3^k 6^{-(k_0+k)}$ and it has the form

where

$$\lim_{k \to \infty} \frac{length(r_k)}{(k+k_0)} = \log_6 3. \tag{1}$$

Choosing sufficiently large k we will have enough leading zeros in the presentation of α_k to pump this string. This will give us a contradiction with the formula (1). Therefore, M^+ is not FA recognizable, and M is not FA recognizable too.

On the other hand, R_6 is isomorphic to $R_2^+ \oplus_{\mathbb{N}} R_3^+$. Indeed, $R_2^+ \oplus_{\mathbb{N}} R_3^+ = \{\langle x,y \rangle_{\mathbb{N}} : (x,y) \in R_2^+ \times R_3^+ \}$ and

$$\langle x, y \rangle_{\mathbb{N}} = \langle x', y' \rangle_{\mathbb{N}}$$
 if and only if $x - y = x' - y'$.

Let $z = m/6^k \in R_6$; there are $m_0, m_1 \in \mathbb{Z}$ such that $m = 3^k m_0 - 2^k m_1$; then $z = m_0/2^k - m_1/3^k = (m_0/2^k + l) - (m_1/3^k + l)$ for any $l \in \mathbb{Z}$. Choosing sufficiently large l we see that z = x - y, where $x \in R_2^+$, $y \in R_3^+$. Therefore, the mapping that sends $\langle x, y \rangle_{\mathbb{N}}$ to $x - y \in R_6$ gives us desired isomorphism.

Consider FA presentations for R_2^+ and R_3^+ described in Section 2. Recall that the integral part of every element is presented in base 2 both in R_2^+ and R_3^+ . Thus if we take FA presentation of $\mathbb N$ in base 2, then the graphs of the identity embeddings $f:\mathbb N\to R_2^+$ and $g:\mathbb N\to R_3^+$ will be FA recognizable. Therefore, by Theorem 4.1, R_6 has an FA presentation which contains FA recognizable submonoids isomorphic to R_2^+ and R_3^+ . Now if $M^+\subseteq R_6$ is a submonoid isomorphic to R_2^+ then $M=M^+\cup -M^+$ is a subgroup isomorphic to R_2 . Clearly, M is definable in terms of M^+ and addition. Therefore, this presentation of R_6 contains FA recognizable subgroups isomorphic to R_2 and R_3 . It is different from the presentation given in Section 2, in the sense that there is no automatic isomorphism between them.

5 Indecomposable FA presentable abelian groups

We describe rank n torsion-free abelian groups, G_n and H_n , which are indecomposable and strongly indecomposable respectively. We then show how to apply the methods from the previous section to prove that they are FA presentable.

In what follows we will use expressions like $p^{-\infty}a$ as an abbreviation for an infinite set $p^{-1}a, p^{-2}a, \cdots$. For every $n \ge 2$, let G_n be a subgroup of \mathbb{Q}^n generated by $p_1^{-\infty}e_1, \ldots, p_n^{-\infty}e_n, q^{-1}(e_1+\cdots+e_n)$, where q, p_1, \ldots, p_n are different primes and e_1, \ldots, e_n are linear independent elements in \mathbb{Q}^n considered as a \mathbb{Q} -vector space. An example of such a group was found in [4, vol. 2, §88, Exercise 2].

Theorem 5.1. The group G_n is indecomposable for all $n \ge 2$.

Proof. First, note that every $x \in G_n$ has the form

$$x = (p_1^{-k_1}m_1 + q^{-1}s)e_1 + \dots + (p_n^{-k_n}m_n + q^{-1}s)e_n,$$

where $m_1, \ldots, m_n, s \in \mathbb{Z}$ and $k_1, \ldots, k_n \in \mathbb{N}$. Let $E_j = \langle p_j^{-\infty} e_j \rangle$ where $1 \leq j \leq n$. We show that the groups E_j are fully invariant in G_n , i.e. $\varphi(E_j) \subseteq E_j$ for any endomorphism φ of G_n . Let $x \in E_j$ and $\varphi(x) = \sum s_i e_i$. In G_n , x is divisible by all powers of p_j , and so is $\varphi(x)$. Hence, $s_i = 0$ for $i \neq j$ and $\varphi(x) = s_j e_j$.

Take any $i \neq j$. As mentioned above, s_j has the form $p_j^{-k_j}m_j + q^{-1}s$ and s_i has the form $p_i^{-k_i}m_i + q^{-1}s$. Since $s_i = 0$, $q^{-1}s$ must be an integer. Therefore, $\varphi(x) = s_j e_j$ belongs to E_j .

Now suppose that $G_n = A \oplus B$. If $x \in G_n$, then x has the unique form x = a + b, where $a \in A$, $b \in B$. Define the following endomorphisms of G_n :

 $\varphi^A(x) = a$ and $\varphi^B(x) = b$, where x = a + b. Obviously, $x = \varphi^A(x) + \varphi^B(x)$. If $x \in E_j$ then $\varphi^A(x) \in E_j \cap A$ and $\varphi^B(x) \in E_j \cap B$, since E_j is fully invariant. This means that $E_j = (E_j \cap A) \oplus (E_j \cap B)$.

Note that E_i is indecomposable, because it has rank 1. Therefore, $E_i \subseteq A$ or $E_j \subseteq B$. Assume there exists $1 \leqslant k < n$ such that $E_1, \ldots, E_k \subseteq A$ and $E_{k+1}, \ldots, E_n \subseteq B$. Let $q^{-1}(e_1 + \cdots + e_n) = a + b$, where $a \in A$ and $b \in B$. Then $e_1 + \dots + e_k + e_{k+1} + \dots + e_n = qa + qb$. Since $e_1 + \dots + e_k \in A$ and $e_{k+1} + \dots + e_n \in B$ we have that $a = q^{-1}(e_1 + \dots + e_k)$.

We show that this is impossible. Let $a = (p_1^{-k_1}m_1 + q^{-1}s)e_1 + \dots + (p_n^{-k_n}m_n + q^{-1}s)e_n$; since $p_n^{-k_n}m_n + q^{-1}s = 0$, $q^{-1}s$ must be an integer. Hence $p_1^{-k_1}m_1 + q^{-1}s = 0$.

 $q^{-1}s = 0$ cannot be equal to q^{-1} .

So we can assume that $E_1, \ldots, E_n \subseteq A$. If $B \neq \mathbf{0}$ then let $b \in B$ be a nonzero element. Then there exists n > 0 such that $nb \in \langle e_1, \dots, e_n \rangle \subseteq E_1 + \dots + E_n \subseteq A$, which is impossible because $nb \neq 0$ and nb is an element of B. Therefore, $B = \mathbf{0}$.

Definition 5.1 ([1]). A torsion-free abelian group A is strongly indecom**posable** if whenever $0 \neq k \in \mathbb{N}$ and $kA \leq B \oplus C \leq A$ then $B = \mathbf{0}$ or $C = \mathbf{0}$.

The group H_n from the next theorem was introduced in [1, Example 2.4].

Theorem 5.2. The group $H_n = \langle p_1^{-\infty} e_1, \dots, p_n^{-\infty} e_n, q^{-\infty} (e_1 + \dots + e_n) \rangle$ is strongly indecomposable for all $n \ge 2$.

Proof. First, we show that any endomorphism of H_n is the same as multiplication by an integer. Let $x \in H_n$, by an argument similar to one in the beginning of the proof of Theorem 5.1, one can show that if x is divisible in H_n by all powers of p_i , then x has the form $mp_i^{-k}e_i$.

Now let $\hat{e}_1 = -e_1, \dots, \hat{e}_{n-1} = -e_{n-1}, \hat{e}_n = e_1 + \dots + e_n$. Then $e_n = \hat{e}_1 + \dots$ $\cdots + \widehat{e}_n$ and we can write

$$H_n = \langle p_1^{-\infty} \widehat{e}_1, \dots, p_{n-1}^{-\infty} \widehat{e}_{n-1}, \ p_n^{-\infty} (\widehat{e}_1 + \dots + \widehat{e}_n), \ q^{-\infty} \widehat{e}_n) \rangle.$$

Therefore, if x is divisible in H_n by any power of q then it has the form $mq^{-k}\widehat{e}_n =$ $mq^{-k}(e_1+\cdots+e_n).$

Let φ be an endomorphism of H_n ; $\varphi(e_i) = r_i e_i$ where $r_i = m_i p_i^{-k_i}$, because $\varphi(e_i)$ is divisible by any power of p_i . Hence $\varphi(e_1 + \cdots + e_n) = \sum r_i e_i$. On the other hand, since $\varphi(e_1 + \cdots + e_n)$ is divisible by all powers of q, it has the form $mq^{-k}(e_1+\cdots+e_n)$. Therefore, each r_i is equal to an integer number r and $\varphi(x) = rx$. Since the group is torsion-free, every nonzero endomorphism is one-to-one.

To conclude the proof we will show that if a torsion-free abelian group A has only one-to-one nonzero endomorphisms then it is strongly indecomposable. Assume that there are $k \neq 0$ and nonzero groups B and C such that $kA \leq$ $B \oplus C \leq A$. Let ψ be an endomorphism of $B \oplus C$ defined as follows: if x = b + cwhere $b \in B$, $c \in C$ then $\psi(x) = b$. Then the mapping φ defined by $\varphi(x) = \psi(kx)$ is an endomorphism of A. Take any $0 \neq c \in C$, then $\varphi(c) = \psi(kc) = 0$ and,

therefore, φ is not one-to-one. Note that φ is also nonzero, since if $0 \neq b \in B$ then $\varphi(b) = kb \neq 0$.

Theorem 5.3. The group G_n is FA presentable.

Proof. Since R_p is FA presentable, the direct sum $R_{p_1} \oplus \cdots \oplus R_{p_n}$ is also FA presentable. Note that $R_{p_1} \oplus \cdots \oplus R_{p_n}$ is a subgroup of finite index in G_n . Hence, by Theorem 4.2, G_n is also FA presentable.

Remark 5.1. Note that unlike G_n , the group H_n is not an extension of finite index of any known example of an FA presentable group. To show that it is FA presentable we will use the method of amalgameted products described in section 4.

Theorem 5.4. The group H_n is FA presentable.

Proof. First, let us show that H_n is isomorphic to $(R_{p_1}^+ \times \cdots \times R_{p_n}^+) \oplus_{\mathbb{N}} R_q^+$, an amalgamated product of monoids $R_{p_1}^+ \times \cdots \times R_{p_n}^+$ and R_q^+ over \mathbb{N} , where the isomorphic embeddings $f: \mathbb{N} \to R_{p_1}^+ \times \cdots \times R_{p_n}^+$ and $g: \mathbb{N} \to R_q^+$ are chosen as follows: for all $m \in \mathbb{N}$, $f(m) = (m, \dots, m)$ and g(m) = m.

Every element of $(R_{p_1}^+ \times \cdots \times R_{p_n}^+) \oplus_{\mathbb{N}} R_q^+$ is of the form $\langle (a_1, \dots, a_n), b \rangle_{\mathbb{N}}$, where $a_i \in R_{p_i}^+$, for $i = 1, \dots, n$, and $b \in R_q^+$. Suppose that

$$\langle (a_1,\ldots,a_n),b\rangle_{\mathbb{N}}=\langle (a'_1,\ldots,a'_n),b'\rangle_{\mathbb{N}}$$

then there are $u, v \in \mathbb{N}$ such that

$$\begin{cases} (a_1 + u, \dots, a_n + u) = (a'_1 + v, \dots, a'_n + v) \\ b + u = b' + v. \end{cases}$$

This implies that $a_i - b = a'_i - b'$ for all i = 1, ..., n. Thus we can correctly define a function h on $(R_{p_1}^+ \times \cdots \times R_{p_n}^+) \oplus_{\mathbb{N}} R_q^+$ such that

$$h(\langle (a_1,\ldots,a_n),b\rangle_{\mathbb{N}}) = (a_1-b)e_1 + \cdots + (a_n-b)e_n.$$

As one can see, the range of h is a subset of H_n , and h is a homomorphism. To show that it is one-to-one, assume that

$$h(\langle (a_1,\ldots,a_n),b\rangle_{\mathbb{N}})=h(\langle (a'_1,\ldots,a'_n),b'\rangle_{\mathbb{N}});$$

then

$$(a_1 - b)e_1 + \dots + (a_n - b)e_n = (a'_1 - b')e_1 + \dots + (a'_n - b')e_n.$$

Therefore, $a_i - a_i' = b - b' \in R_{p_i} \cap R_q$ for i = 1, ..., n. Since $R_{p_i} \cap R_q = \mathbb{Z}$ there is $w \in \mathbb{Z}$ such that

$$\begin{cases} (a_1, \dots, a_n) = (a'_1 + w, \dots, a'_n + w) \\ b = b' + w. \end{cases}$$

So $\langle (a_1,\ldots,a_n),b\rangle_{\mathbb{N}}=\langle (a'_1,\ldots,a'_n),b'\rangle_{\mathbb{N}}.$

Now to prove that h is onto, consider an element $z \in H_n$; it must be of the form

$$z = \left(\frac{m_1}{p_1^{k_1}} + \frac{l}{q^r}\right)e_1 + \dots + \left(\frac{m_n}{p_n^{k_n}} + \frac{l}{q^r}\right)e_n.$$

for integers m_i , l, and natural numbers k_i , r. Obviously,

$$\frac{m_i}{p_i^{k_i}} + \frac{l}{q^r} = \left(\frac{m_i}{p_i^{k_i}} + t\right) - \left(-\frac{l}{q^r} + t\right)$$

for any $t \in \mathbb{Z}$. Choosing sufficiently large t we can make all $a_i = m_i/p_i^{k_i} + t$ and $b = -l/q^r + t$ to be positive. In this case $\langle (a_1, \ldots, a_n), b \rangle_{\mathbb{N}}$ is an element of $(R_{p_1}^+ \times \cdots \times R_{p_n}^+) \oplus_{\mathbb{N}} R_q^+$ and $h(\langle (a_1, \ldots, a_n), b \rangle_{\mathbb{N}}) = z$. Therefore, the range of h is H_n , and hence it is an isomorphism.

Consider FA presentations of monoids $R_{p_1}^+,\ldots,R_{p_n}^+$, and R_q^+ described in Section 2. From this we can easily construct an FA presentation of $R_{p_1}^+\times\cdots\times R_{p_n}^+$ by putting strings representing elements of $R_{p_i}^+$ one under another in a column using an extra padding symbol when necessary. Recall that the integral part of an element of $R_{p_i}^+$ or R_q^+ is presented in base 2. Therefore, if we consider the presentation of \mathbb{N} in base 2, then the graphs of isomorphic embeddings $f:\mathbb{N}\to R_{p_1}^+\times\cdots\times R_{p_n}^+$ and $g:\mathbb{N}\to R_q^+$ will be FA recognizable. Now, by Theorem 4.1, the structure $(R_{p_1}^+\times\cdots\times R_{p_n}^+)\oplus_{\mathbb{N}}R_q^+$ is FA presentable, and as shown above it is isomorphic to H_n .

6 A new FA presentation of \mathbb{Z}^2

Let $(\mathbb{Z}, +)$ be the group of integers under addition. In this section we will construct an FA presentation of $(\mathbb{Z}, +)^2$ in which no nontrivial cyclic subgroup is FA recognizable.

Consider $\mathbb{Z}[x]/\langle p_3\rangle$, the quotient of the polynomial ring $\mathbb{Z}[x]$ with respect to the ideal generated by $p_3(x) = x^2 + x - 3$. We will use the notation $p(x) \sim q(x)$ to denote that $p_3(x)$ divides p(x) - q(x).

Remark 6.1. In the construction described below we can use any polynomial of the form $x^2 + x - q$, for a prime $q \ge 3$, instead of $p_3(x)$.

Let $A = (\mathbb{Z}[x]/\langle p_3 \rangle, +)$ be the additive group of the ring $\mathbb{Z}[x]/\langle p_3 \rangle$. It is not hard to see that A is isomorphic to \mathbb{Z}^2 , since every polynomial in $\mathbb{Z}[x]$ is equivalent over $\langle p_3 \rangle$ to a linear polynomial kx + l, which can be identified with a pair $(k, l) \in \mathbb{Z}^2$.

We say that a polynomial $a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ is in **reduced form** (or briefly **reduced**) if $|a_i| \leq 2$ for all $i \leq n$.

Proposition 6.1. For every $p(x) \in \mathbb{Z}[x]$, there is a reduced polynomial $\widetilde{p}(x)$ equivalent to it.

Proof. This can be proved by induction: assume that p(x) is in reduced form and show that $p(x) \pm x^n$ is equivalent to a reduced polynomial. It is enough to consider $p(x) \pm 1$. Note that if $p_0(x)$ and $p_1(x)$ are in reduced form and have non-negative coefficients then $p_0(x) - p_1(x)$ is reduced. Moreover, any reduced p(x) is equal to the difference of such $p_0(x)$ and $p_1(x)$. So, it is enough to consider the case when p(x) is reduced and has non-negative coefficients and show that p(x) + 1 is equivalent to a reduced polynomial with non-negative coefficients.

We will actually prove a stronger statement: if p(x) is a reduced polynomial with non-negative coefficients then $p(x) + (a_1x + a_0)$, where $0 \le a_0, a_1 \le 2$, is equivalent to a polynomial of the same sort. The proof is now by induction on the degree of p(x).

Let us write p(x) as $p(x) = p_1(x)x^2 + (b_1x + b_0)$; now using the fact that $3 \sim x^2 + x$ we have

$$p(x) + (a_1x + a_0) = p_1(x)x^2 + (a_1 + b_1)x + (a_0 + b_0)$$
$$\sim (p_1(x) + r_1x + (r_0 + r_1))x^2 + c_1x + c_0,$$

where

$$c_0 = \begin{cases} a_0 + b_0, & \text{if } a_0 + b_0 < 3\\ a_0 + b_0 - 3, & \text{otherwise} \end{cases} \qquad r_0 = \left[\frac{a_0 + b_0}{3}\right],$$

$$c_1 = \begin{cases} a_1 + b_1 + r_0, & \text{if } a_1 + b_1 + r_0 < 3\\ a_1 + b_1 + r_0 - 3, & \text{otherwise} \end{cases} \qquad r_1 = \left[\frac{a_1 + b_1 + r_0}{3}\right].$$

Here [v] is the integral part of v, defined by

$$[v] = \begin{cases} \max\{k \in \mathbb{Z} : k \leqslant v\} & \text{if } v \geqslant 0, \\ \min\{k \in \mathbb{Z} : v \leqslant k\} & \text{if } v < 0. \end{cases}$$

For example, [1.5] = 1 and [-1.5] = -1. Note that $0 \le c_0, c_1 \le 2$ and $0 \le r_0, r_1 \le 1$. By induction, $p_1(x) + r_1x + (r_0 + r_1)$ is equivalent to a reduced polynomial with non-negative coefficients; hence so is p(x).

We now give an automatic presentation for the group A. The alphabet of the presentation is $\Sigma = \{-2, -1, 0, 1, 2\}$. Each reduced polynomial $a_n x^n + \cdots + a_0$ is represented by a word $a_0 \dots a_n \in \Sigma^*$. We say that two words $a_0 \dots a_n$ and $b_0 \dots b_m$ from Σ^* are **equivalent** if $a_n x^n + \cdots + a_0 \sim b_m x^m + \cdots + b_0$.

This equivalence relation is FA recognizable. An algorithm for checking it is as follows. Given two words $a_0
ldots a_0
ldots b_m$; we can assume that n = m since one can always add extra zeros to the right. The algorithm needs to remember two carries r_0 , r_1 ; initially $r_0 = r_1 = 0$. Note that since $3 \sim x + x^2$, whenever we subtract 3 from any digit we need to add 1 to the next two digits in order to get an equivalent word. That is why we need two carries here.

Now for every i = 0, ..., n do the following. Check if 3 divides $a_i - b_i + r_0$. If 'no' then the words are not equivalent. If 'yes' then let $r_0^{\text{old}} = r_0$, $r_1^{\text{old}} = r_1$;

redefine

$$r_0 = r_1^{\text{old}} + \frac{a_i - b_i + r_0^{\text{old}}}{3}, \qquad r_1 = \frac{a_i - b_i + r_0^{\text{old}}}{3},$$

and go to step i+1. If we reach in this way step n then the words are equivalent if and only if $a_n - b_n + r_0 = 0$ and $r_1 = 0$.

Since at every step $|r_0| \leq 4$ and $|r_1| \leq 2$, this algorithm requires a constant amount of memory. Now it is not hard to construct a finite automaton recognizing the equivalence.

Consider the following order on Σ : -2 < -1 < 0 < 1 < 2. It naturally extents to the length-lexicographical order on Σ^* , denoted as $<_{llex}$. Let the domain of the FA presentation of A be

$$Dom(A) = \{ w \in \Sigma^* : (\forall u <_{llex} w) \ u \text{ is not equivalent to } w \}.$$

This set is FA recognizable since $<_{llex}$ is an FA recognizable relation.

To define addition on $\operatorname{Dom}(A)$ consider the relation R(x,y,z) such that if $x=a_0\ldots a_k,\,y=b_0\ldots b_l$ then $z=c_0\ldots c_n$ is obtained from x and y by applying the following algorithm. Again, let $r_0,\,r_1$ be two carries that are initially zero. At every step i starting from 0, let c_i be such that $|c_i|<3$,

$$c_i \equiv a_i + b_i + r_0 \pmod{3}$$

and c_i has the same sign as $a_i + b_i + r_0$. Let $r_0^{\text{old}} = r_0$, $r_1^{\text{old}} = r_1$. Now redefine

$$r_0 = r_1^{\text{old}} + \left[\frac{a_i + b_i + r_0^{\text{old}}}{3}\right], \qquad r_1 = \left[\frac{a_i + b_i + r_0^{\text{old}}}{3}\right],$$

and go to step i + 1.

For example, if x=2211 and y=22 then this algorithm produces z=120021. By construction, if R(x,y,z) holds then the polynomial corresponding to z is equivalent over $\langle p_3 \rangle$ to the sum of polynomials represented by x and y. It is easy to see that at every step $|r_0| \leq 4$ and $|r_1| \leq 2$. Thus, as before, R can be recognized by a finite automaton.

Let Add(x, y, z) be defined as

$$Add = \{(x, y, z) : x, y, z \in Dom(A) \text{ and } \exists w \ (R(x, y, w) \land w \text{ is equivalent to } z)\}.$$

Since Dom(A), R, and the equivalence relation are FA recognizable Add is also FA recognizable. Obviously, Add is the graph of addition operation on Dom(A), and the FA presented structure (Dom(A), Add) is isomorphic to A.

Our next goal is to show that no nontrivial cyclic subgroup in this presentation of \mathbb{Z}^2 is FA recognizable.

Lemma 6.1. Let p(x) and q(x) be reduced polynomials such that $p(x) \sim q(x)$ and $x^k \mid p(x)$, then $x^k \mid q(x)$.

Proof. Suppose that $x^k \nmid q(x)$; then $p(x) - q(x) = x^l(a_0 + a_1x + \cdots)$, where l < k, $|a_0| \leq 2$, and $a_0 \neq 0$. Since $3 \nmid a_0$, $p_3(x) = x^2 + x - 3$ cannot divide p(x) - q(x), which gives a contradiction.

For $p(x) \in \mathbb{Z}[x]$, consider the set of all words in Σ^* that represent polynomials equivalent to p(x). All these words start with the same number of zeros. So we say that p(x) starts with k zeros in reduced form if there is $w \in \Sigma^*$ representing p(x) that starts with k zeros.

The following lemma will be used several times later on.

Lemma 6.2. Let n be an integer, then $3^k \mid n$ if and only if n starts with k zeros in reduced form.

Proof. Suppose that $3^k \mid n$; then $n = 3^k m \sim x^k (x+1)^k m$. Taking a reduced form for $(x+1)^k m$ and multiplying it by x^k we obtain a reduced form for n that starts with k zeros; thus n starts with k zeros in reduced form.

The other implication can be proved by induction on k. First, suppose that n starts with 0 in reduced form and n=3m+r, where $0 < r \le 2$. Take any reduced form for 3m. Since it starts with 0, n=3m+r has a reduced form that starts with $r \ne 0$. This contradicts our assumption, and hence $3 \mid n$.

It is not hard to see that if p(x) starts with exactly k zeros in reduced form, and q(x) starts with exactly l zeros, then a reduced form for p(x)q(x) starts with exactly k+l zeros. Now suppose that n starts with k+1 zeros in reduced form; then n=3m and m starts with k zeros, because $3\sim 011$ starts with one 0. By induction, $3^k\mid m$, and so we have $3^{k+1}\mid n$.

Let $\alpha = (\sqrt{13} - 1)/2$ be the positive root of $p_3(x) = x^2 + x - 3$. Consider a mapping $F : \mathbb{Z}[x] \to \mathbb{R}$ such that $F : p(x) \mapsto p(\alpha)$. Obviously,

$$(p+q)(\alpha) = p(\alpha) + q(\alpha)$$
 and $(pq)(\alpha) = p(\alpha)q(\alpha)$.

Furthermore, if $p(x) \sim q(x)$ then $p(\alpha) = q(\alpha)$, since $p(\alpha) - q(\alpha) = p_3(\alpha)r(\alpha) = 0$. Consider an arbitrary nontrivial cyclic subgroup in our presentation of \mathbb{Z}^2 . It has the form

$$\langle w \rangle = \{ n \cdot w : \ n \in \mathbb{Z} \}$$

for some $w \in \text{Dom}(A)$. Let q(x) be the polynomial that corresponds to w. Note that $q(\alpha) \neq 0$ since w represents nonzero element. Indeed, by applying the Euclidean algorithm one can see that there are polynomials s, r with $\deg(r) < 2$ such that $q = s \cdot p_3 + r$. Moreover, since the leading coefficient of p_3 is 1, s and r have integer coefficients. Now if $q(\alpha) = 0$, then $r(\alpha) = 0$, which implies that r = 0 since α is irrational. So $q = s \cdot p_3$ is equivalent to 0.

Suppose that $\langle w \rangle$ is recognized by a finite automaton with d states. We know that $3^d \cdot w \in \langle w \rangle$ starts with d zeros in reduced form. So let $3^d \cdot w$ be equivalent to $0^d v \in \text{Dom}(A)$. By pumping lemma, there are $s_0, s_1, t \in \mathbb{N}$ with $t \neq 0$ such that $0^d v = 0^{s_0} 0^t 0^{s_1} v$ and $w_k = 0^{tk + s_0 + s_1} v \in \langle w \rangle$ for all $k \geqslant 0$.

Ц

Let $q_k(x)$ be the polynomial that corresponds to w_k . Since $w_k \in \langle w \rangle$, we have that $w_k \sim n_k \cdot w$ for some $n_k \in \mathbb{Z}$. If w starts with m zeros, then n_k starts with at least $tk - m + s_0 + s_1$ zeros in reduced form; thus $3^{tk - m + s_0 + s_1} \mid n_k$.

The fact that w_k is equivalent to $n_k \cdot w$ implies that $q_k(\alpha) = n_k q(\alpha)$. Now, on the one hand,

$$|q_k(\alpha)| \le 2(1 + \alpha + \dots + \alpha^{|w_k| - 1})$$

$$= 2\frac{\alpha^{|w_k|} - 1}{\alpha - 1} \le 8\alpha^{|w_k|} = 8\alpha^{s_0 + s_1 + |v|}\alpha^{tk} = C_0\alpha^{tk}.$$

On the other hand,

$$|q_k(\alpha)| = |n_k||q(\alpha)| \geqslant 3^{tk}3^{s_0+s_1-m}|q(\alpha)| = C_13^{tk}.$$

Thus

$$C_1 3^{tk} \leqslant C_0 \alpha^{tk}$$
 for all $k \geqslant 0$,

which is impossible because $\alpha < 3$. Therefore, $\langle w \rangle$ is not FA recognizable.

References

- D. Arnold, Finite Rank Torsion Free Abelian Groups and Rings (Springer-Verlag, 1982).
- 2. A. Blumensath, E. Grädel, Automatic structures, 15th Annual IEEE Symposium on Logic in Computer Science (Santa Barbara, CA, 2000), 51–62, IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.
- 3. C. Delhommé, Non-automaticity of ω^{ω} , 2001, manuscript.
- 4. L. Fuchs, Infinite Abelian Groups, vol. 1, 2 (Academic Press, 1970, 1973).
- B. R. Hodgson, Théories décidables par automate fini, PhD Thesis, University of Montreal, 1976.
- 6. B. R. Hodgson, Théories décidables par automate fini, Annales de Sciences Mathématiques, 7:39–57, 1983.
- B. Khoussainov, A. Neorde, Automatic presentations of structures, in D. Leivant (ed.), Logic and Computational Complexity (LNCS 960, Springer-Verlag, 1995), 367–392.
- 8. B. Khoussainov, S. Rubin, Automatic structures: overview and future directions. Weighted automata: theory and applications (Dresden, 2002), *J. Autom. Lang. Comb.*, 2:287–301, 8 (2003).
- 9. 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* (IEEE Computer Society, 2004), 110–119.