Finite automata presentable Abelian groups

Lutz H. Strüngmann
(joint work with Gábor Braun)

Ilmenau, 5^{th} of November 2011

Contents

1. Basic definitions and first examples
2. The main result and its proof
3. Concluding remarks

Adding integers

$$
\begin{array}{r}
1001110101000101110101001101010010101111 \\
\Diamond\Diamond\Diamond\Diamond\Diamond\Diamond\Diamond\Diamond\Diamond\Diamond\Diamond\Diamond 1011001010001101010101110100 \\
\hline
1001110101001000100111110000101000100011
\end{array}
$$

$\Longrightarrow$ We observe that only local information is needed to compute the addition !

$\Longrightarrow$ Are there other structures with such nice encodings?

Adding integers

```
1001110101000101110101001101010010101111
◊◊◊◊◊◊◊◊◊◊◊◊1011001010001101010101110100
----------------------------------------
1001110101001000100111110000101000100011
```

$\Longrightarrow$ We observe that only local information is needed to compute the addition !

$\Longrightarrow$ Are there other structures with such nice encodings?

Adding integers

$$
\begin{array}{r}
1001110101000101110101001101010010101111 \\
\diamond\diamond\diamond\diamond\diamond\diamond\diamond\diamond\diamond\diamond\diamond\diamond 10110010100011010101110100 \\
\hline
1001110101001000100111110000101000100011
\end{array}
$$

$\Longrightarrow$ We observe that only local information is needed to compute the addition !

$\Longrightarrow$ Are there other structures with such nice encodings?

Finite automata presentable structures

The following definition goes back to Khoussainov and Nerode

Definition

A countable relational structure $(M, R_1, \cdots, R_k)$ is called FAP (Finite Automata Presentable) or automatic if there exists a finite alphabet Σ, a regular language $D \subseteq \Sigma^*$, and a bijection $f : D \to M$ such that the relations $f^{-1}(R_1), \cdots, f^{-1}(R_k)$ are regular.

- Note that function symbols can be by considered as their graphs and can therefore be included in the language.
- What does it mean for $f^{-1}(R_i)$ to be regular?

$$f^{-1}(R_i) \subseteq D^s \subseteq (\Sigma^*)^s \to ((\Sigma \cup \{\Diamond\})^s)^*.$$

Finite automata presentable structures

The following definition goes back to Khoussainov and Nerode

Definition

A countable relational structure $(M, R_1, \cdots, R_k)$ is called FAP (Finite Automata Presentable) or automatic if there exists a finite alphabet Σ, a regular language $D \subseteq \Sigma^*$, and a bijection $f : D \to M$ such that the relations $f^{-1}(R_1), \cdots, f^{-1}(R_k)$ are regular.

- Note that function symbols can be by considered as their graphs and can therefore be included in the language.
- What does it mean for $f^{-1}(R_i)$ to be regular?

$$f^{-1}(R_i) \subseteq D^s \subseteq (\Sigma^*)^s \to ((\Sigma \cup \{\Diamond\})^s)^*.$$

Finite automata presentable structures

The following definition goes back to Khoussainov and Nerode

Definition

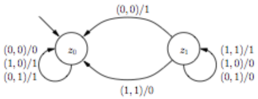
A countable relational structure $(M, R_1, \cdots, R_k)$ is called FAP (Finite Automata Presentable) or automatic if there exists a finite alphabet Σ, a regular language $D \subseteq \Sigma^*$, and a bijection $f : D \to M$ such that the relations $f^{-1}(R_1), \cdots, f^{-1}(R_k)$ are regular.

- Note that function symbols can be by considered as their graphs and can therefore be included in the language.
- What does it mean for $f^{-1}(R_i)$ to be regular?

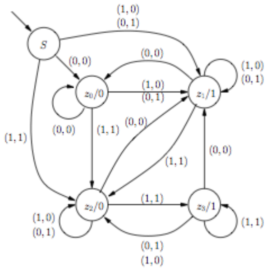
$$f^{-1}(R_i) \subseteq D^s \subseteq (\Sigma^*)^s \to ((\Sigma \cup \{\Diamond\})^s)^*.$$

Adding integers revisited

Two finite automata adding integers



Mealy automaton



Moore automaton

Some remarks

- Regular languages are stable under Boolean operations and projections. Thus definable relations yield regular sets again. Example: If $\varphi(\bar{x})$ is first order formula, then the set

$$A\varphi = \{\bar{a} \in D^s : M \models \varphi(f(\bar{a}))\}$$

  is regular.
- The above is effective, i.e. there is a simple algorithm that computes an automaton recognizing $A\varphi$ from the automata defining the structure and φ.

Some remarks

- Regular languages are stable under Boolean operations and projections. Thus definable relations yield regular sets again. Example: If $\varphi(\bar{x})$ is first order formula, then the set

$$A\varphi = \{\bar{a} \in D^s : M \models \varphi(f(\bar{a}))\}$$

  is regular.
- The above is effective, i.e. there is a simple algorithm that computes an automaton recognizing $A\varphi$ from the automata defining the structure and φ.

The isomorphism problem

- The isomorphism problem for automatic structures is complete for Σ_1^1
- (Kuske) The isomorphism problem and the elementary equivalence problem for automatic equivalence relations are complete for Π_1^0.
- (Kuske) The isomorphism problem for automatic linear orders and for automatic trees are complete for Σ_1^1.

Is the definition very restrictive?

- (Khoussainov-Nies-Rubin-Stephan) Every infinite automatic Boolean algebra is a finite product of copies of the algebra of all finite and cofinite subsets of $\mathbb{N}$.
- (Khoussainov-Nies-Rubin-Stephan) Every automatic integral domain is finite.

$\Longrightarrow$ Rich algebraic structure implies few automatic structures

Is the definition very restrictive?

- (Khoussainov-Nies-Rubin-Stephan) Every infinite automatic Boolean algebra is a finite product of copies of the algebra of all finite and cofinite subsets of $\mathbb{N}$.
- (Khoussainov-Nies-Rubin-Stephan) Every automatic integral domain is finite.

$\Longrightarrow$ Rich algebraic structure implies few automatic structures

Is the definition very restrictive?

- (Khoussainov-Nies-Rubin-Stephan) Every infinite automatic Boolean algebra is a finite product of copies of the algebra of all finite and cofinite subsets of $\mathbb{N}$.
- (Khoussainov-Nies-Rubin-Stephan) Every automatic integral domain is finite.

$\Longrightarrow$ Rich algebraic structure implies few automatic structures

What about groups?

- (Oliver-Thomas) A finitely generated group is automatic iff it is abelian-by-finite (has an abelian subgroup of finite index).
- (Nies-Thomas) Every finitely generated subgroup of an automatic group is abelian-by-finite.

$\Longrightarrow$ It is natural to look at the class of Abelian groups !

What about groups?

- (Oliver-Thomas) A finitely generated group is automatic iff it is abelian-by-finite (has an abelian subgroup of finite index).
- (Nies-Thomas) Every finitely generated subgroup of an automatic group is abelian-by-finite.

$\Longrightarrow$ It is natural to look at the class of Abelian groups !

What about groups?

- (Oliver-Thomas) A finitely generated group is automatic iff it is abelian-by-finite (has an abelian subgroup of finite index).
- (Nies-Thomas) Every finitely generated subgroup of an automatic group is abelian-by-finite.

$\Longrightarrow$ It is natural to look at the class of Abelian groups !

FAP Abelian groups

Here are some examples of FAP Abelian groups (with addition of course)

- $\mathbb{Z}$
- $(\mathbb{Z}/p\mathbb{Z})^{(\omega)}$
- $\mathbb{Z}(p^\infty) = \{x \in \mathbb{Q}/\mathbb{Z} : \exists n \text{ with } p^n x = 0\}$
- $\mathbb{Z}[1/m] = \{\frac{a}{m^k} : a, k \in \mathbb{Z}\}$
- Finite direct sums of the above groups
- (Nies-Semukhin) Finite extensions and automatic amalgamations

FAP Abelian groups

Here are some examples of FAP Abelian groups (with addition of course)

- $\mathbb{Z}$
- $(\mathbb{Z}/p\mathbb{Z})^{(\omega)}$
- $\mathbb{Z}(p^\infty) = \{x \in \mathbb{Q}/\mathbb{Z} : \exists n \textit{ with } p^n x = 0\}$
- $\mathbb{Z}[1/m] = \{\frac{a}{m^k} : a, k \in \mathbb{Z}\}$
- Finite direct sums of the above groups
- (Nies-Semukhin) Finite extensions and automatic amalgamations

FAP Abelian groups

Here are some examples of FAP Abelian groups (with addition of course)

- $\mathbb{Z}$
- $(\mathbb{Z}/p\mathbb{Z})^{(\omega)}$
- $\mathbb{Z}(p^\infty) = \{x \in \mathbb{Q}/\mathbb{Z} : \exists n \textit{ with } p^n x = 0\}$
- $\mathbb{Z}[1/m] = \{\frac{a}{m^k} : a, k \in \mathbb{Z}\}$
- Finite direct sums of the above groups
- (Nies-Semukhin) Finite extensions and automatic amalgamations

FAP Abelian groups

Here are some examples of FAP Abelian groups (with addition of course)

- $\mathbb{Z}$
- $(\mathbb{Z}/p\mathbb{Z})^{(\omega)}$
- $\mathbb{Z}(p^{\infty}) = \{x \in \mathbb{Q}/\mathbb{Z} : \exists n \textit{ with } p^n x = 0\}$
- $\mathbb{Z}[1/m] = \{\frac{a}{m^k} : a, k \in \mathbb{Z}\}$
- Finite direct sums of the above groups
- (Nies-Semukhin) Finite extensions and automatic amalgamations

FAP Abelian groups

Here are some examples of FAP Abelian groups (with addition of course)

- $\mathbb{Z}$
- $(\mathbb{Z}/p\mathbb{Z})^{(\omega)}$
- $\mathbb{Z}(p^\infty) = \{x \in \mathbb{Q}/\mathbb{Z} : \exists n \text{ with } p^n x = 0\}$
- $\mathbb{Z}[1/m] = \{\frac{a}{m^k} : a, k \in \mathbb{Z}\}$
- Finite direct sums of the above groups
- (Nies-Semukhin) Finite extensions and automatic amalgamations

FAP Abelian groups

Here are some examples of FAP Abelian groups (with addition of course)

- $\mathbb{Z}$
- $(\mathbb{Z}/p\mathbb{Z})^{(\omega)}$
- $\mathbb{Z}(p^\infty) = \{x \in \mathbb{Q}/\mathbb{Z} : \exists n \textit{ with } p^n x = 0\}$
- $\mathbb{Z}[1/m] = \{\frac{a}{m^k} : a, k \in \mathbb{Z}\}$
- Finite direct sums of the above groups
- (Nies-Semukhin) Finite extensions and automatic amalgamations

Examples:

- G FAP and $G \subseteq H$ such that H/G is finite, then H is FAP.
  In particular, many almost completely decomposable groups, i.e.

$$\langle R_1 \oplus R_2 \oplus \cdots \oplus R_n, g_1, \cdots, g_m \rangle \textit{ with } R_i \subseteq \mathbb{Q}.$$

- $\langle p_1^{-\infty} e_1, p_2^{-\infty} e_2, q^{-\infty}(e_1 + e_2) \rangle \subseteq \mathbb{Q}^2$ where $\mathbb{Q}^2 = \langle e_1, e_2 \rangle$

Non-examples (Khoussainov-Nies-Rubin-Stephan):

- Every torsion-free Abelian group of infinite rank
- $\mathbb{Z}(p^{(\infty)})^{(\omega)}$.
- (Tsankov) The group of rationals $\mathbb{Q}$ and any torsion-free Abelian group divisible by infinitely many primes.

Examples:

- G FAP and $G \subseteq H$ such that H/G is finite, then H is FAP.
  In particular, many almost completely decomposable groups, i.e.

$$\langle R_1 \oplus R_2 \oplus \cdots \oplus R_n, g_1, \cdots, g_m \rangle \text{ with } R_i \subseteq \mathbb{Q}.$$

- $\langle p_1^{-\infty} e_1, p_2^{-\infty} e_2, q^{-\infty}(e_1 + e_2) \rangle \subseteq \mathbb{Q}^2$ where $\mathbb{Q}^2 = \langle e_1, e_2 \rangle$

Non-examples (Khoussainov-Nies-Rubin-Stephan):

- Every torsion-free Abelian group of infinite rank
- $\mathbb{Z}(p^{(\infty)})^{(\omega)}$.
- (Tsankov) The group of rationals $\mathbb{Q}$ and any torsion-free Abelian group divisible by infinitely many primes.

Examples:

- G FAP and $G \subseteq H$ such that H/G is finite, then H is FAP.
  In particular, many almost completely decomposable groups, i.e.

$$\langle R_1 \oplus R_2 \oplus \cdots \oplus R_n, g_1, \cdots, g_m \rangle \text{ with } R_i \subseteq \mathbb{Q}.$$

- $\langle p_1^{-\infty} e_1, p_2^{-\infty} e_2, q^{-\infty}(e_1 + e_2) \rangle \subseteq \mathbb{Q}^2$ where $\mathbb{Q}^2 = \langle e_1, e_2 \rangle$

Non-examples (Khoussainov-Nies-Rubin-Stephan):

- Every torsion-free Abelian group of infinite rank
- $\mathbb{Z}(p^{(\infty)})^{(\omega)}$.
- (Tsankov) The group of rationals $\mathbb{Q}$ and any torsion-free Abelian group divisible by infinitely many primes.

Examples:

- G FAP and $G \subseteq H$ such that H/G is finite, then H is FAP.
  In particular, many almost completely decomposable groups, i.e.

$$\langle R_1 \oplus R_2 \oplus \cdots \oplus R_n, g_1, \cdots, g_m \rangle \ \textit{with}\ R_i \subseteq \mathbb{Q}.$$

- $\langle p_1^{-\infty} e_1, p_2^{-\infty} e_2, q^{-\infty}(e_1 + e_2) \rangle \subseteq \mathbb{Q}^2$ where $\mathbb{Q}^2 = \langle e_1, e_2 \rangle$

Non-examples (Khoussainov-Nies-Rubin-Stephan):

- Every torsion-free Abelian group of infinite rank
- $\mathbb{Z}(p^{(\infty)})^{(\omega)}$.
- (Tsankov) The group of rationals $\mathbb{Q}$ and any torsion-free Abelian group divisible by infinitely many primes.

Motivating question

Looking at subgroups of the rational numbers as additive group we see that

1. $\mathbb{Z}$ is FAP
2. $\mathbb{Z}[1/m]$ is FAP for any natural number m
3. $\mathbb{Q}$ is not FAP

But there $2^{\aleph_0}$ more subgroups of the rationals ! Are they FAP? For instance what about the following group

$$R = \left\langle \frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}, \dots \right\rangle$$

Motivating question

Looking at subgroups of the rational numbers as additive group we see that

1. $\mathbb{Z}$ is FAP
2. $\mathbb{Z}[1/m]$ is FAP for any natural number m
3. $\mathbb{Q}$ is not FAP

But there $2^{\aleph_0}$ more subgroups of the rationals ! Are they FAP? For instance what about the following group

$$R = \left\langle \frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}, \cdots \right\rangle$$

Motivating question

Looking at subgroups of the rational numbers as additive group we see that

1. $\mathbb{Z}$ is FAP
2. $\mathbb{Z}[1/m]$ is FAP for any natural number m
3. $\mathbb{Q}$ is not FAP

But there $2^{\aleph_0}$ more subgroups of the rationals ! Are they FAP? For instance what about the following group

$$R = \left\langle \frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}, \cdots \right\rangle$$

Inhalt

1 Basic definitions and first examples

2 The main result and its proof

3 Concluding remarks

The main result

Here is what we can prove so far.....

Theorem

Every FAP torsion-free Abelian group is an extension of a finite-rank free group by a direct sum of finitely many $\mathbb{Z}(p^\infty)$.

Especially, the FAP torsion-free Abelian groups of rank 1 are the rings $\mathbb{Z}[1/n]$.

Main ingredient in the proof by Tsankov

Lemma

For every FAP Abelian group G, there exist a sequence of finite subsets A_n of G, a constant C_1 and a function $h\colon \mathbb{N} \to \mathbb{N}$ such that:

1. $\bigcup_{n=0}^{\infty} A_n = G$;
2. $0 \in A_0$ *and* $| A_0 | \geq 2$;
3. $A_n + A_n \subseteq A_{n+1}$;
4. $| A_{n+1} | \leq C_1 | A_n |$;
5. *For every* $x \in A_n$ *and* $m \in \mathbb{N}$ *with* $m \mid x$ *in G there is a* $y \in A_{n+h(m)}$ *with* $x = my$. *(If G is torsion-free, this means* $m^{-1}A_n \subseteq A_{n+h(m)}$.*)*

For $D \subseteq \Sigma^*$, let $D^{\leq n} = \{w \in D : len(w) \leq n\}$.

Lemma

Suppose that G is an FAP Abelian group, where addition is recognized by an automaton of size k. Then for every $x, y \in G$,

$$len(x + y) \leq max\{len(x), len(y)\} + k$$

Hence, $D^{\leq n} + D^{\leq n} \subseteq D^{\leq n+k}$ for all n.

Lemma

If D is a regular language, then for each k, there exists C such that $\mid D^{\leq n+k} \mid \leq C \mid D^{\leq n} \mid$ for all n.

In particular, $\mid D^{\leq n} + D^{\leq n} \mid \leq C \mid D^{\leq n} \mid$.

For $D \subseteq \Sigma^*$, let $D^{\leq n} = \{w \in D : len(w) \leq n\}$.

Lemma

Suppose that G is an FAP Abelian group, where addition is recognized by an automaton of size k. Then for every $x, y \in G$,

$$len(x + y) \leq max\{len(x), len(y)\} + k$$

Hence, $D^{\leq n} + D^{\leq n} \subseteq D^{\leq n+k}$ for all n.

Lemma

If D is a regular language, then for each k, there exists C such that $| D^{\leq n+k} | \leq C | D^{\leq n} |$ for all n.

In particular, $| D^{\leq n} + D^{\leq n} | \leq C | D^{\leq n} |$.

For $D \subseteq \Sigma^*$, let $D^{\leq n} = \{w \in D : len(w) \leq n\}$.

Lemma

Suppose that G is an FAP Abelian group, where addition is recognized by an automaton of size k. Then for every $x, y \in G$,

$$len(x + y) \leq max\{len(x), len(y)\} + k$$

Hence, $D^{\leq n} + D^{\leq n} \subseteq D^{\leq n+k}$ for all n.

Lemma

If D is a regular language, then for each k, there exists C such that $| D^{\leq n+k} | \leq C | D^{\leq n} |$ for all n.

In particular, $| D^{\leq n} + D^{\leq n} | \leq C | D^{\leq n} |$.

An idea of the proof of the main theorem

The idea is the following:

- First prove a finite version of Tsankov's Lemma
- Use this to prove a local version replacing $\mathbb{Q}$ by the finite group $\mathbb{Z}/p\mathbb{Z}$
- Use the local version to prove the main result

An idea of the proof of the main theorem

The idea is the following:

- First prove a finite version of Tsankov's Lemma
- Use this to prove a local version replacing $\mathbb{Q}$ by the finite group $\mathbb{Z}/p\mathbb{Z}$
- Use the local version to prove the main result

An idea of the proof of the main theorem

The idea is the following:

- First prove a finite version of Tsankov's Lemma
- Use this to prove a local version replacing $\mathbb{Q}$ by the finite group $\mathbb{Z}/p\mathbb{Z}$
- Use the local version to prove the main result

Proposition (finite version)

Given a constant C_1 there are integers $d, K \in \mathbb{Z}^+$ and a constant $C \geq C_1$ such that the following hold for any sequence $p_0, \ldots, p_d$ of primes and integers $h(p_i)$ with

$$p_{i-1} > p_i C^{h(p_i)d} d^{Cd^4} \qquad i = 1, \ldots, d \tag{1}$$

$$p_d > C(4dK)^d. \tag{2}$$

There is no sequence $A_0, \ldots, A_{h(p_0)+\cdots+h(p_d)+1}$ of finite subsets of a torsion-free abelian group G such that

1. $0 \in A_0$ and $| A_0 | \geq 2$;
2. $| A_{n+1} | \leq C_1 | A_n |$ for $n \leq h(p_0) + \cdots + h(p_d)$;
3. $A_n + A_n \subseteq A_{n+1}$ for $n \leq h(p_0) + \cdots + h(p_d)$;
4. $\langle A_n \rangle \cap p_i G \subseteq p_i \langle A_{n+h(p_i)} \rangle$ and $p_i \langle A_n \rangle \subsetneq \langle A_n \rangle \cap p_i G$ for $n + h(p_i) \leq h(p_0) + \cdots + h(p_d)$.

Proposition (local version)

Given a constant C_1 there are integers $d, K \in \mathbb{Z}^+$ and a constant $C \geq C_1$ such that the following hold for any sequence $p_0, \ldots, p_d$ of primes and integers $h(p_i)$ with

$$p_{i-1} > p_i C^{h(p_i)d} d^{Cd^4} \qquad i = 1, \ldots, d \tag{3}$$

$$p_d > C(4dK)^d. \tag{4}$$

There is a p^* such that for any prime $p \geq p^*$, there is no sequence $A_0, \ldots, A_{h(p_0)+\cdots+h(p_d)+1}$ of finite subsets of $\mathbb{Z}/p\mathbb{Z}$ such that

1. $0 \in A_0$, $2 \leq |A_0| \leq C_1$
2. $|A_{n+1}| \leq C_1|A_n|$ for $n \leq h(p_0) + \cdots + h(p_d)$
3. $A_n + A_n \subseteq A_{n+1}$ for $n \leq h(p_0) + \cdots + h(p_d)$
4. $p_i^{-1} A_n \subseteq A_{n+h(p_i)}$ for $n + h(p_i) \leq h(p_0) + \cdots + h(p_d)$.

Inhalt

1 Basic definitions and first examples

2 The main result and its proof

3 Concluding remarks

Wildness

Theorem

There are arbitrarily 'difficult' FAP Abelian groups in the following sense:

Given a natural number n and a prime p there are indecomposable almost completely decomposable groups G of arbitrary large finite rank with regulating quotient of exponent p^n.

This shows that the FAP groups behave 'wild'.....

Open question

By our main result every FAP torsion-free Abelian group G has to be the extension of a finite rank free group by a finite direct sum of Prüfer groups.

However: Every pure finite rank subgroup of the additive group of the ring of p-adic numbers J_p is of this form.

Since there are only countably many finite automata......

Question

Which finite rank pure subgroup of the additive group of the ring of p-adic integers are FA-presentable?

Open question

By our main result every FAP torsion-free Abelian group G has to be the extension of a finite rank free group by a finite direct sum of Prüfer groups.

However: Every pure finite rank subgroup of the additive group of the ring of p-adic numbers J_p is of this form.

Since there are only countably many finite automata......

Question

Which finite rank pure subgroup of the additive group of the ring of p-adic integers are FA-presentable?

Open question

By our main result every FAP torsion-free Abelian group G has to be the extension of a finite rank free group by a finite direct sum of Prüfer groups.

However: Every pure finite rank subgroup of the additive group of the ring of p-adic numbers J_p is of this form.

Since there are only countably many finite automata......

Question

Which finite rank pure subgroup of the additive group of the ring of p-adic integers are FA-presentable?