The additive group of the rationals is not automatic

Todor Tsankov

Université Pierre et Marie Curie – Paris 6

Logic Colloquium, Sofia 2009

Adding integers

```
3287648732782634093274983274987329847234
♢♢♢♢♢♢♢♢♢♢♢♢49823749871107407344398738
────────────────────────────────────────
3287648732782683917024854382394674245972
```

Adding integers

3287648732782634093274983274987329847234

◊◊◊◊◊◊◊◊◊◊◊◊49823749871107407344398738

3287648732782683917024854382394674245972

Question

What other structures have nice encodings that make the operations similarly simple to compute (using only local information)?

Automatic structures

Definition (Khoussainov–Nerode)

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

Automatic structures

Definition (Khoussainov–Nerode)

A countable relational structure $(M; R_1, \dots, R_k)$ is called **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 $f^{-1}(R_1), \dots, f^{-1}(R_k)$ are regular.

- We can also include languages with function symbols by considering the graphs of the functions.
- What does it mean for $f^{-1}(R_i)$ to be regular?

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

- f may only be a surjection but then $f^{-1}(=)$ must be regular.

Basic properties

Regular languages are stable under Boolean operations and projections, so, in particular, for every first order formula $\phi(\bar{x})$, the set

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

is regular.

Basic properties

Regular languages are stable under Boolean operations and projections, so, in particular, for every first order formula $\phi(\bar{x})$, the set

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

is regular.

Moreover, there is a simple algorithm that computes an automaton recognizing A_ϕ from the automata defining the structure and ϕ.

This property distinguishes automatically presentable structures from recursively presentable ones (whose theories are, in general, not decidable).

Very few automatic structures

If one allows rich algebraic structure in the language, the only automatic structures are the trivial ones:

- (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 $\mathbf{N}$;
- (KNRS) every automatic integral domain is finite.

Very few automatic structures

If one allows rich algebraic structure in the language, the only automatic structures are the trivial ones:

- (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 $\mathbf{N}$;
- (KNRS) every automatic integral domain is finite.

For groups, one has the following:

- (Oliver–Thomas) A *finitely generated* group is automatic iff it is **abelian-by-finite** (has an abelian subgroup of finite index). This is a simple consequence of Gromov's theorem and a theorem of Romanovskiĭ characterizing the polycyclic-by-finite groups with a decidable first order theory.
- (Nies–Thomas) Every finitely generated subgroup of an automatic group is abelian-by-finite.

Those results show that the natural class to restrict one's attention to is the class of abelian groups.

Automatic abelian groups

Examples of automatic groups:

- $\mathbf{Z}$;
- $(\mathbf{Z}/p\mathbf{Z})^{<\omega}$;
- $\mathbf{Z}(p^\infty) = \{x \in \mathbf{Q}/\mathbf{Z} : \exists n\ p^n \cdot x = 0\}$;
- $\mathbf{Z}[1/m] = \{a/m^k : a, k \in \mathbf{Z}\}$;
- finite direct sums of those;
- (Nies–Semukhin) finite extensions and "automatic amalgamations," for example,

$$\langle p_1^{-\infty} e_1, p_2^{-\infty} e_2, q^{-\infty}(e_1 + e_2)\rangle \leq \mathbf{Q}^2, \quad \text{where } \mathbf{Q}^2 = \langle e_1, e_2 \rangle.$$

Automatic abelian groups

Examples of automatic groups:

- $\mathbf{Z}$;
- $(\mathbf{Z}/p\mathbf{Z})^{<\omega}$;
- $\mathbf{Z}(p^\infty) = \{x \in \mathbf{Q}/\mathbf{Z} : \exists n\ p^n \cdot x = 0\}$;
- $\mathbf{Z}[1/m] = \{a/m^k : a, k \in \mathbf{Z}\}$;
- finite direct sums of those;
- (Nies–Semukhin) finite extensions and "automatic amalgamations," for example,

$$\langle p_1^{-\infty} e_1, p_2^{-\infty} e_2, q^{-\infty}(e_1 + e_2)\rangle \le \mathbf{Q}^2, \quad \text{where } \mathbf{Q}^2 = \langle e_1, e_2\rangle.$$

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

- every group containing $\mathbf{Z}^{<\omega}$;
- $\mathbf{Z}(p^\infty)^{<\omega}$.

The additive group of the rationals

Question (Khoussainov, 1996)

Does the additive group of $\mathbf{Q}$ admit an automatic presentation?

The additive group of the rationals

Question (Khoussainov, 1996)

Does the additive group of $\mathbf{Q}$ admit an automatic presentation?

Theorem

No.

The answer is not particularly surprising but new techniques were needed to prove the result.

Basic limitations of automatic structures

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

Lemma

Suppose that Z is an automatic abelian group, where addition is recognized by an automaton of size k. Then for every $x, y \in Z$,

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

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

Additive sets with small sumsets

What are the finite sets $A \subseteq \mathbf{Z}$ for which the sumset $A + A$ is small?

Since for a "random" set $A \subseteq \mathbf{Z}$, $|A + A| \sim |A|^2$, a natural notion of smallness is $|A + A| = O(|A|)$.

Examples:

- Arithmetic progressions:

$$A = \{0, 1, 2, 3, 4, 5\}, \quad A + A = \{0, \ldots, 10\}, \quad |A + A| \sim 2|A|;$$

- More generally, multidimensional progressions:

$$A = \{0, 1, 2,\ 10, 11, 12,\ \ldots,\ 90, 91, 92\}, \quad |A + A| \sim 2^2|A|.$$

Additive sets with small sumsets

What are the finite sets $A \subseteq \mathbf{Z}$ for which the sumset $A + A$ is small?

Since for a "random" set $A \subseteq \mathbf{Z}$, $|A + A| \sim |A|^2$, a natural notion of smallness is $|A + A| = O(|A|)$.

Examples:

- Arithmetic progressions:

$$A = \{0, 1, 2, 3, 4, 5\}, \quad A + A = \{0, \dots, 10\}, \quad |A + A| \sim 2|A|;$$

- More generally, multidimensional progressions:

$$A = \{0, 1, 2, \; 10, 11, 12, \; \dots, \; 90, 91, 92\}, \quad |A + A| \sim 2^2|A|.$$

Quite amazingly, these are essentially the only examples.

Freiman's theorem

A **progression** in an abelian group G is a triple (S, P, ϕ), where S is a parallelepiped in $\mathbf{Z}^d$ ($[0, N_1) \times \cdots \times [0, N_d)$), $P \subseteq G$ and $\phi\colon S \to P$ is an affine surjection:

$$P = \phi(S) = \{v_0 + \sum_{i=1}^{d} a_i v_i : 0 \leq a_i < N_i\}, \quad \text{where } v_0, v_1, \ldots, v_d \in G.$$

The number d is called the **rank** of the progression.

Theorem (Freiman, 1966)

Let $C > 0$. Then there exist constants K and d such that for every torsion-free abelian group G and for all finite sets $A \subseteq G$ such that $|A + A| < C|A|$, there exists a progression P of rank at most d such that $P \supseteq A$ and $|P|/|A| \leq K$.

Automatic groups and progressions

Hence, we can conclude that for any torsion-free abelian group, the sets $D^{\leq n}$ are (efficiently contained in) progressions of bounded rank.

In this way, one can see immediately that any group of infinite rank is not automatic: indeed, if $P \subseteq G$ is a progression of rank d, then $\operatorname{rank}\langle P \rangle \leq d + 1$, so it is not possible that progressions of bounded rank exhaust a group of infinite rank.

Even though $\mathbf{Q}$ has rank 1, one can exploit divisibility by large primes to produce a contradiction.

Automatic groups and progressions

Hence, we can conclude that for any torsion-free abelian group, the sets $D^{\leq n}$ are (efficiently contained in) progressions of bounded rank.

In this way, one can see immediately that any group of infinite rank is not automatic: indeed, if $P \subseteq G$ is a progression of rank d, then $\operatorname{rank}\langle P \rangle \leq d + 1$, so it is not possible that progressions of bounded rank exhaust a group of infinite rank.

Even though $\mathbf{Q}$ has rank 1, one can exploit divisibility by large primes to produce a contradiction.

For example, consider the following progression:

$$\{0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad 100\}.$$

Automatic groups and progressions

Hence, we can conclude that for any torsion-free abelian group, the sets $D^{\leq n}$ are (efficiently contained in) progressions of bounded rank.

In this way, one can see immediately that any group of infinite rank is not automatic: indeed, if $P \subseteq G$ is a progression of rank d, then $\operatorname{rank}\langle P \rangle \leq d + 1$, so it is not possible that progressions of bounded rank exhaust a group of infinite rank.

Even though $\mathbf{Q}$ has rank 1, one can exploit divisibility by large primes to produce a contradiction.

For example, consider the following progression:

$$\{0, \quad 1/p, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad 100\}.$$

Now it is difficult to contain the resulting set in a 1-dimensional progression.

Open questions

The proof shows that the following groups are not automatic:

- torsion-free groups that are p-divisible for infinitely many primes p;
- torsion groups of the form $\bigoplus_{p \in I} \mathbf{Z}(p^\infty)$, where I is an infinite set of primes (in particular, $\mathbf{Q}/\mathbf{Z}$ when one takes I to be the set of all primes).

Open questions

The proof shows that the following groups are not automatic:

- torsion-free groups that are p-divisible for infinitely many primes p;
- torsion groups of the form $\bigoplus_{p \in I} \mathbf{Z}(p^\infty)$, where I is an infinite set of primes (in particular, $\mathbf{Q}/\mathbf{Z}$ when one takes I to be the set of all primes).

However, it remains open whether the following group of rank 1 is automatic:

$$\langle 1/p : p \text{ prime} \rangle \leq \mathbf{Q}.$$

It is also perhaps not infeasible to characterize all automatic abelian groups; this would give an interesting class of "finitistic" abelian groups (groups of finite rank that only "use finitely many primes" in their definition).