Lecture 15
Automatic Structures

Logic and Proof
3 June 2019

Prof James Worrell
University of Oxford

Overview

Today:

- Structures whose universe and relations are regular languages
- Gives automata-based decision procedures for the theory of those structures similar to quantifier elimination

Relational structures

Definition

A σ-structure $\mathcal{A}$ is **relational** if σ only consists of relation symbols.

Relational structures

Definition

A σ-structure $\mathcal{A}$ is **relational** if σ only consists of relation symbols.

- Every structure $\mathcal{A}$ has relational variant obtained by replacing every $f_{\mathcal{A}}\colon U_{\mathcal{A}}^k \to U_{\mathcal{A}}$ with relation

$$F_{\mathcal{A}} = \{(a_1, \ldots, a_k, b) \in U_{\mathcal{A}}^{k+1} : f_{\mathcal{A}}(a_1, \ldots, a_k) = b\}$$

- Example: $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is replaced by

$$\{(i, j, k) \in \mathbb{N}^3 : i + j = k\}$$

- Constants are functions of arity zero, get replaced by singleton relation
- Only consider relational structures in this lecture

Word convolutions

Want to represent relations by words over some alphabet

Given alphabet Σ with $\# \notin \Sigma$, define $\Sigma_{\#} := \Sigma \cup \{\#\}$

Word convolutions

Want to represent relations by words over some alphabet

Given alphabet Σ with $\# \notin \Sigma$, define $\Sigma_\# := \Sigma \cup \{\#\}$

For words $w_1, w_2, \ldots, w_n \in \Sigma^*$,

- Let $w_i = a_{i,1} a_{i,2} \cdots a_{i,\ell_i}$, hence $|w_i| = \ell_i$
- Let $\ell = \max\{\ell_1, \ldots, \ell_n\}$
- Set $a_{i,j} := \#$ for all $\ell_i < j \leq \ell$ and $1 \leq i \leq n$

Word convolutions

Want to represent relations by words over some alphabet

Given alphabet Σ with $\# \notin \Sigma$, define $\Sigma_\# := \Sigma \cup \{\#\}$

For words $w_1, w_2, \ldots, w_n \in \Sigma^*$,

- Let $w_i = a_{i,1} a_{i,2} \cdots a_{i,\ell_i}$, hence $|w_i| = \ell_i$
- Let $\ell = \max\{\ell_1, \ldots, \ell_n\}$
- Set $a_{i,j} := \#$ for all $\ell_i < j \leq \ell$ and $1 \leq i \leq n$
- The **convolution** of $w_1, \ldots, w_n$ is

$$w_1 \otimes w_2 \otimes \cdots \otimes w_n \in (\Sigma_\#^n)^* := (a_{1,1}, \ldots, a_{n,1})(a_{1,2}, \ldots, a_{n,2}) \cdots (a_{1,\ell}, \ldots, a_{n,\ell})$$

Word convolutions

Want to represent relations by words over some alphabet

Given alphabet Σ with $\# \notin \Sigma$, define $\Sigma_\# := \Sigma \cup \{\#\}$

For words $w_1, w_2, \ldots, w_n \in \Sigma^*$,

- Let $w_i = a_{i,1} a_{i,2} \cdots a_{i,\ell_i}$, hence $|w_i| = \ell_i$
- Let $\ell = \max\{\ell_1, \ldots, \ell_n\}$
- Set $a_{i,j} := \#$ for all $\ell_i < j \leq \ell$ and $1 \leq i \leq n$
- The **convolution** of $w_1, \ldots, w_n$ is

$$w_1 \otimes w_2 \otimes \cdots \otimes w_n \in (\Sigma_\#^n)^* \\ := (a_{1,1}, \ldots, a_{n,1})(a_{1,2}, \ldots, a_{n,2}) \cdots (a_{1,\ell}, \ldots, a_{n,\ell})$$

Example

$$abba \otimes abaabba = \left[\begin{smallmatrix} a \\ a \end{smallmatrix}\right] \left[\begin{smallmatrix} b \\ b \end{smallmatrix}\right] \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right] \left[\begin{smallmatrix} a \\ a \end{smallmatrix}\right] \left[\begin{smallmatrix} \# \\ b \end{smallmatrix}\right] \left[\begin{smallmatrix} \# \\ b \end{smallmatrix}\right] \left[\begin{smallmatrix} \# \\ a \end{smallmatrix}\right]$$

Automatic relations

Definition

A relation $R \subseteq (\Sigma^*)^n$ is **automatic** if the language

$$L_R := \{w_1 \otimes w_2 \otimes \cdots \otimes w_n : (w_1, \ldots, w_n) \in R\}$$

is regular.

Automatic relations

Definition

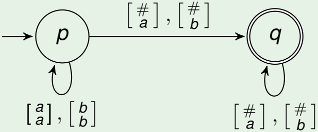
A relation $R \subseteq (\Sigma^*)^n$ is **automatic** if the language

$$L_R := \{w_1 \otimes w_2 \otimes \cdots \otimes w_n : (w_1, \ldots, w_n) \in R\}$$

is regular.

Example

$R = \{(u, v) \in (\Sigma^*)^2 : u \text{ is a prefix of } v\}$ with $\Sigma = \{a, b\}$ is automatic:



Automatic structures

Definition

A relational structure $\mathcal{A} = (U_{\mathcal{A}}, R_1, \ldots, R_m)$ is **automatic** if there are a finite alphabet Σ and regular languages $L, L_1, \ldots, L_m$ such that

- $L = U_{\mathcal{A}}$
- $L_i = L_{R_i}$ for all $1 \leq i \leq m$

Definition

A relational structure $\mathcal{A} = (U_{\mathcal{A}}, R_1, \ldots, R_m)$ is **automatic** if there are a finite alphabet Σ and regular languages $L, L_1, \ldots, L_m$ such that

- $L = U_{\mathcal{A}}$
- $L_i = L_{R_i}$ for all $1 \leq i \leq m$

A structure $\mathcal{A}$ has an **automatic presentation** if $\mathcal{A}$ is isomorphic to an automatic structure.

Presburger arithmetic has an automatic presentation

Suffices to show that a structure isomorphic to $(\mathbb{N}, +)$ is automatic:

- Set $N := (\{0,1\}^*1) \cup \{0\} \subseteq \{0,1\}^*$
- For $w = b_0 b_1 \cdots b_m \in N$, define $\mathrm{val}\colon N \to \mathbb{N}$ by

$$\mathrm{val}(w) := \sum_{i=0}^{m} 2^i \cdot b_i$$

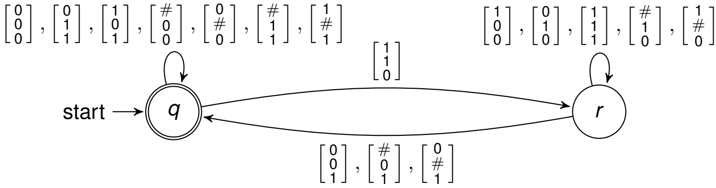
- Set $A := \big\{(a,b,c) \in N^3 : \mathrm{val}(a) + \mathrm{val}(b) = \mathrm{val}(c)\big\} \subseteq N^3$
- Then $(\mathbb{N}, +)$ is isomorphic to (N, A) by mapping $n \in \mathbb{N}$ to its unique minimal binary expansion $\mathrm{val}^{-1}(n)$

Proposition

The structure (N, A) is automatic.

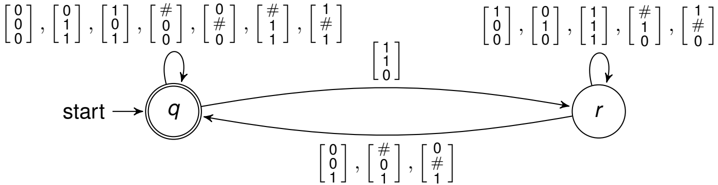
A is automatic

N is obviously regular, and L_A is contained in the language of the following DFA:



A is automatic

N is obviously regular, and L_A is contained in the language of the following DFA:



Intersect with $\{a \otimes b \otimes c : a, b, c \in N\}$ to obtain NFA for L_A

Unbounded dense linear orders have automatic presentations

Theorem

Any structure $\mathcal{A} = (Q, <)$ that is a model of the unbounded dense linear order axioms has an automatic presentation.

Unbounded dense linear orders have automatic presentations

Theorem

Any structure $\mathcal{A} = (Q, <)$ that is a model of the unbounded dense linear order axioms has an automatic presentation.

Proof strategy:

- Show that unbounded dense linear orders are isomorphic
- Show statement for suitable structure that is a unbounded dense linear order

Unbounded dense linear orders have automatic presentations

Theorem

Any structure $\mathcal{A} = (Q, <)$ that is a model of the unbounded dense linear order axioms has an automatic presentation.

Proof strategy:

- Show that unbounded dense linear orders are isomorphic
- Show statement for suitable structure that is a unbounded dense linear order

Theorem (Cantor)

Any two countable unbounded dense linear orders are isomorphic.

Proof.

Wait until tomorrow... □

An automatic unbounded dense linear order

Let $L = \{0,1\}^* \cdot 1$ and $<$ such that $x < y$ iff either

- $y = xu$ for some $u \in \{0,1\}^*$, or
- $x = z0u$ and $y = z1v$ for some $u, v, z \in \{0,1\}^*$

Clearly, $(L, <)$ is automatic. Remains to show that $(L, <)$ is UDLO:

- No smallest element: for $u1 \in L$, have $u01 < u1$
- No largest element: for $u1 \in L$, have $u1 < u11$
- Density: Let $x, y \in L$ such that $x < y$:
  Case $x = u1, y = u1v1$: then $x < u10^{|v|+1}1 < y$
  Case $x = u0v1, y = u1w$: then $x < u01^{|v|+2} < y$

Proposition

The structure $(L, <)$ is an automatic unbounded dense linear order.

Structures with automatic presentations are decidable

Theorem (Khoussainov, Nerode)

$\mathrm{Th}(\mathcal{A})$ *is decidable for every structure* $\mathcal{A}$ *with an automatic presentation.*

Structures with automatic presentations are decidable

Theorem (Khoussainov, Nerode)

$\mathrm{Th}(\mathcal{A})$ *is decidable for every structure* $\mathcal{A}$ *with an automatic presentation.*

Not every decidable theory is automatic, for instance:

- $(\mathbb{R}, +)$ (since $\mathbb{R}$ is uncountable)
- structures with undecidable theories such as $(\mathbb{N}, +, \cdot)$
- $(\mathbb{N}, \cdot)$, $(\mathbb{N}, |)$ and $(\mathbb{Q}, +)$

Structures with automatic presentations are decidable

Theorem (Khoussainov, Nerode)

$\mathrm{Th}(\mathcal{A})$ *is decidable for every structure* $\mathcal{A}$ *with an automatic presentation.*

Not every decidable theory is automatic, for instance:

- $(\mathbb{R}, +)$ (since $\mathbb{R}$ is uncountable)
- structures with undecidable theories such as $(\mathbb{N}, +, \cdot)$
- $(\mathbb{N}, \cdot)$, $(\mathbb{N}, |)$ and $(\mathbb{Q}, +)$

Proposition

Let $\mathcal{A} = (L, R_1, \ldots, R_m)$ be an automatic σ-structure and let F be a σ-formula with at most free variables $x_1, \ldots, x_n$. There is an effectively constructible regular language $L_F \subseteq (\Sigma_\#^*)^n$ such that

$$L_F = \left\{ w_1 \otimes \cdots \otimes w_n : \mathcal{A}_{[x_1 \mapsto w_1] \cdots [x_n \mapsto w_n]} \models F \right\} .$$

Proof of the proposition

Case $F = R_i(x_{i_1}, \ldots, x_{i_k})$ with $1 \leq i_1, \ldots, i_k \leq n$:

- Define homomorphism $h\colon (\Sigma_\#^n)^* \to (\Sigma_\#^k)^*$ such that for $a_1, \ldots, a_n \in \Sigma_\#$:

$$h(a_1, \ldots, a_n) = \begin{cases} \epsilon & \text{if } a_1 = \cdots = a_n = \# \\ (a_{i_1}, \ldots, a_{i_k}) & \text{otherwise} \end{cases}$$

- By assumption $L_{R_i} \subseteq (\Sigma_\#^k)^*$ regular, using closure under inverse homomorphisms, obtain

$$L_F = h^{-1}(L_{R_i}) \cap \{w_1 \otimes \cdots \otimes w_n : w_1, \ldots, w_n \in L\}$$

Proof of the proposition

Case $F = R_i(x_{i_1}, \ldots, x_{i_k})$ with $1 \leq i_1, \ldots, i_k \leq n$:

- Define homomorphism $h\colon (\Sigma_\#^n)^* \to (\Sigma_\#^k)^*$ such that for $a_1, \ldots, a_n \in \Sigma_\#$:

$$h(a_1, \ldots, a_n) = \begin{cases} \epsilon & \text{if } a_1 = \cdots = a_n = \# \\ (a_{i_1}, \ldots, a_{i_k}) & \text{otherwise} \end{cases}$$

- By assumption $L_{R_i} \subseteq (\Sigma_\#^k)^*$ regular, using closure under inverse homomorphisms, obtain

$$L_F = h^{-1}(L_{R_i}) \cap \{w_1 \otimes \cdots \otimes w_n : w_1, \ldots, w_n \in L\}$$

Case $F = G \wedge H$, $F = G \vee H$, or $F = \neg G$:

- Induction hypothesis yields regular languages $L_G, L_H \subseteq (\Sigma_\#^n)^*$
- Statement follows from closure of regular languages under intersection, union and complement
- Example: for $F = \neg G$ get

$$L_F = \{w_1 \otimes \cdots \otimes w_n : w_1, \ldots, w_n \in L\} \setminus L_G$$

Proof of the proposition

Case $F = \exists x_{n+1}\, G$ with $x_1, \ldots, x_n, x_{n+1}$ free in G:

- Induction hypothesis yields regular languages L_G for G
- Define homomorphism $h\colon (\Sigma_\#^{n+1})^* \to (\Sigma_\#^n)^*$ such that for $a_1, \ldots, a_n \in \Sigma_\#$

$$h(a_1, \ldots, a_n, a_{n+1}) = \begin{cases} \epsilon & \text{if } a_1 = \cdots = a_n = \# \\ (a_1, \ldots, a_n) & \text{otherwise} \end{cases}$$

- Get $L_F = h(L_G)$

Proof of the proposition

Case $F = \exists x_{n+1}\, G$ with $x_1, \ldots, x_n, x_{n+1}$ free in G:

- Induction hypothesis yields regular languages L_G for G
- Define homomorphism $h\colon (\Sigma_{\#}^{n+1})^* \to (\Sigma_{\#}^{n})^*$ such that for $a_1, \ldots, a_n \in \Sigma_{\#}$

$$h(a_1, \ldots, a_n, a_{n+1}) = \begin{cases} \epsilon & \text{if } a_1 = \cdots = a_n = \# \\ (a_1, \ldots, a_n) & \text{otherwise} \end{cases}$$

- Get $L_F = h(L_G)$

For sentences F, wlog. have $F = \exists x\, G$. Then

$$\mathcal{A} \models F \iff L_G \neq \emptyset$$

Intractability

Theorem

There exists an automatic structure $\mathcal{A}$ with non-elementary complexity, i.e., no algorithm decides $F \in \mathrm{Th}(\mathcal{A})$ in time $2^{2^{\cdot^{\cdot^{\cdot 2^n}}}}$.

Proof.

This can be shown for the structure $\mathcal{A} = (\{0,1\}^*, S_1, S_2, \leq)$, where

- $S_0 = \{(w, w0) : w \in \{0,1\}^*\}$
- $S_1 = \{(w, w1) : w \in \{0,1\}^*\}$
- $\leq \; = \{(w, u) : w, u \in \{0,1\}^*\}$. □

Proving Lagrange-style theorems automatically

Theorem (Lagrange, 1770)

Every natural number can be written as the sum of four integer squares.

Proving Lagrange-style theorems automatically

Theorem (Lagrange, 1770)

Every natural number can be written as the sum of four integer squares.

Call $n \in \mathbb{N}$ a binary palindrome if the string representing its binary presentation is a palindrome, e.g.,

$$27 = \mathrm{val}(11011)$$

Proving Lagrange-style theorems automatically

Theorem (Lagrange, 1770)

Every natural number can be written as the sum of four integer squares.

Call $n \in \mathbb{N}$ a binary palindrome if the string representing its binary presentation is a palindrome, e.g.,

$$27 = \mathrm{val}(11011)$$

Theorem (Rajasekaran, Shallit, Smith, 2017)

Every natural number can be written as the sum of four binary palindromes.

Proof idea.

Translate statement into a suitably constructed nested-word automaton accepting all numbers that are the sum of four binary palindromes, and check the automaton for universality. □