Automaton and FO[$\mathbb{N}^r, <, \mathrm{mod}$]

Arthur MILCHIOR

Liafa
Université Paris Diderot, France
LACL, UPEC, Créteil, France

September 2013

Problem

Strong logic	Weak Logic	Weaker Logic
$FO[+, V_b]$	$FO[+]$	$FO[<, \text{mod}]$
$\vert\vert$		$FO[<]$, $FO[\text{mod}]$
Automata		

Question

Decide in *polynomial time* if R definable in a strong logic is definable in a weak logic.

Automata reading r-tuple of integers

Example

Base $b = 3$, least digit first
$\overline{17}^{10} = \overline{2210}^{3}, \overline{18}^{10} = \overline{0020}^{3}$.

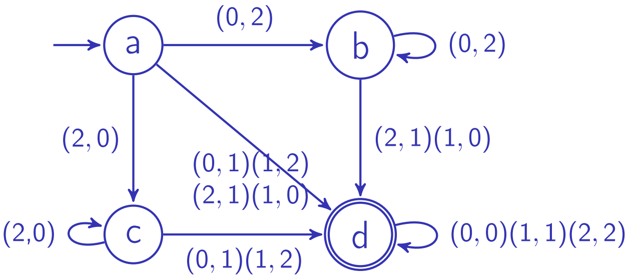
Example

Arity $r = 2$
$\binom{17}{18} = \binom{2}{0}\binom{2}{0}\binom{1}{2}\binom{0}{0}$

Definition

$A = (Q, [0, b-1]^r, \delta, q_0, F)$
A read an r-tuple of base b integer least digit first.

- $|A| = \{w \in [0, b-1]^{r*} \mid \delta(q_0, w) \in F\}$ its accepted set of tuples of words.
- $|\overline{A}| \subseteq \mathbb{N}^r$ its accepted set of integers.



$|\overline{A}| = \{(x, y) \mid x + 1 = y \vee y + 1 = x\}.$

Theorem (Büchi 60)

Let $R \subseteq \mathbb{N}^r$, R is accepted by a deterministic automaton in base b iff it is definable in $\mathrm{FO}[+, V_b]$.
$V_b(n) = b^k$ *when* $n = b^k c$ *and b does not divide c.*

Regular sets

Definition

$R \subseteq \mathbb{N}^r$ is regular if the set of r-tuples in R, written in base 1, is accepted by a synchronous automaton.

Theorem (Péladeau Straubing 94)

R is regular iff it is definable in FO$[<, \text{mod}]$.

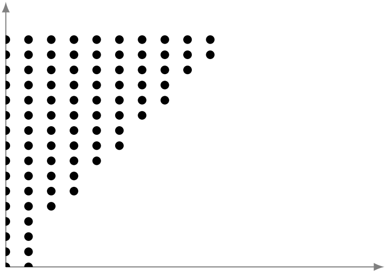


Figure: $x = 3 \vee (x = 0 \mod 3 \wedge y = 0 \mod 2 \wedge y > x)$

Characterization

Theorem

Let $R \subseteq \mathbb{N}^r$. $R \notin \mathrm{FO}[<, \mathrm{mod}]$ *iff there exists a unary function definable in* $\mathrm{FO}[<, R]$ *not in* $\mathrm{FO}[<, \mathrm{mod}]$.

Theorem

$R \in \mathrm{FO}[<, \mathrm{mod}\, k]$ *iff*

- *every sections and diagonal are in* $\mathrm{FO}[<, \mathrm{mod}\, k]$ *and*
- $\exists l.\forall x_1 > l, \ldots, x_r > l \Rightarrow (x_1, \ldots, x_r) \in R \Leftrightarrow (x_1 + k, \cdots, x_r + k) \in R]$

Characterization

Theorem

Let $R \subseteq \mathbb{N}^r$. $R \notin \mathrm{FO}[<, \mathrm{mod}]$ *iff there exists a unary function definable in* $\mathrm{FO}[<, R]$ *not in* $\mathrm{FO}[<, \mathrm{mod}]$.

Theorem

$R \in \mathrm{FO}[<, \mathrm{mod}\, k]$ *iff*

- *every sections and diagonal are in* $\mathrm{FO}[<, \mathrm{mod}\, k]$ *and*
- $\exists l. \forall x_1 > l, \dots, x_r > l \Rightarrow (x_1, \dots, x_r) \in R \Leftrightarrow (x_1 + k, \cdots, x_r + k) \in R]$

Theorem (Cooper 72)

Quantifier-free $\mathrm{FO}[+C, =C, =, <, \quad \mathrm{mod}\ ]$ *admits quantifier elimination.*

Sections and Diagonals

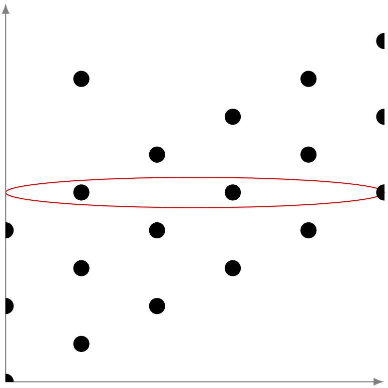


Figure: Section $y = 5$

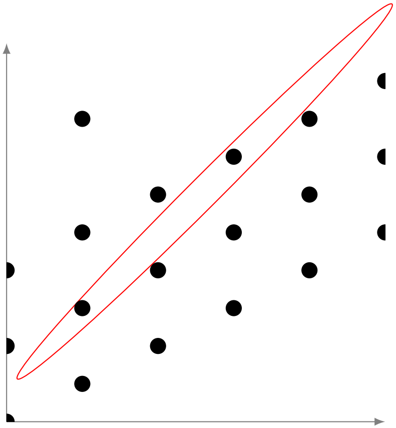


Figure: Diagonal $x = y - 1$

Known results

Theorem (Leroux 06)

Deciding if a deterministic automaton accepts a $\mathrm{FO}[+]$ *set is decidable in polynomial time.*

Theorem (Marsault-Sakarovitch 13)

Deciding if a deterministic automaton accepts a $\mathrm{FO}[\mathrm{mod}]$ *or* $\mathrm{FO}[\mathbb{N}, \mathrm{mod}]$ *set of integers is decidable in time* $n \log(n)$.

Theorem

Deciding if a deterministic automaton accepts a $\mathrm{FO}[<, \mathrm{mod}]$ *set is decidable in time 3-EXP.*

First easy solutions, two 3-EXP algorithms

Theorem

Deciding if a deterministic automaton accepts a $\mathrm{FO}[<, \mathrm{mod}]$ *set is decidable in time 3-EXP.*

- Obtaining a polynomial-size $\mathrm{FO}[+]$-formula by Leroux 06
- Checking if the formula could be stated in $\mathrm{FO}[<, \mathrm{mod}]$ by Choffrut 08

- Stating ϕ in $\mathrm{FO}[+, R]$ "R is regular" by Milchior 13
- Rewriting ϕ as a deterministic automaton as in Muchnik 03 of size 3-EXP
- Checking if the formula is true on the automaton.

Our polynomial time algorithm

Theorem (Decidability)

Let $R \in \mathrm{FO}[+, V_b]$. There exists an algorithm in polynomial time that accepts iff R is in $\mathrm{FO}[<, \mathrm{mod}]$.

Its complexity is $O(2^r|Q|^2(r^2b^r + 2^r\log(|Q|) + 8^r))$ when R is given as a deterministic automaton A.

Theorem (Computation of the formula)

There exists an algorithm that computes a $\mathrm{FO}[<, \mathrm{mod}, +C, = C]$-formula, if one exists, of polynomial size.

The size of the formula is $O(|Q|^2 r(b^r + |Q|^2 r\log(b)\log(|Q|)))$.

Remark

Everything still holds if $\mathbb{Z}$ replaces $\mathbb{N}$.
The computation time is multiplied by 2^r.

The existence algorithm also works for FO[mod] and when $C \subseteq \mathbb{N}$, $X \subseteq \{+C, = C, =, <\}$ it works for $\Pi_0[X, \mathrm{mod}]$.

Further research

Open question:

- If the alphabet is $[0, b-1]^*$, is there a polynomial time algorithm?
- Is there a polynomial time algorithm for $FO[<]$ or $FO[<, \mathrm{mod}\ k]$?

Further research

Open question:

- If the alphabet is $[0, b-1]^*$, is there a polynomial time algorithm?
- Is there a polynomial time algorithm for $\mathrm{FO}[<]$ or $\mathrm{FO}[<, \bmod k]$?

Conjecture

The algorithm works for $\mathrm{FO}[<, \bmod, \times b]$

Further research

Open question:

- If the alphabet is $[0, b-1]^*$, is there a polynomial time algorithm?
- Is there a polynomial time algorithm for $\mathrm{FO}[<]$ or $\mathrm{FO}[<, \bmod k]$?

Conjecture

The algorithm works for $\mathrm{FO}[<, \bmod, \times b]$

Thank you