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

<table>
<thead>
<tr>
<th>Strong logic</th>
<th>Weak Logic</th>
<th>Weaker Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{FO} [+, V_b]$</td>
<td>$\text{FO} [+]$</td>
<td>$\text{FO} [&lt;, \text{mod}]$</td>
</tr>
<tr>
<td>$</td>
<td></td>
<td>$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Automata</th>
</tr>
</thead>
</table>

### 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
\[
17_{10} = 2210_3, 18_{10} = 0020_3.
\]

Example

Arity $r = 2$
\[
\begin{pmatrix} 17 \\ 18 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 2 \\ 1 \\ 0 \end{pmatrix}
\]

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.
\[ |\overline{A}| = \{(x, y) \mid x + 1 = y \lor y + 1 = x\}. \]

**Theorem (Büchi 60)**

Let \( R \subseteq \mathbb{N}^r \), \( R \) is accepted by a deterministic automaton in base \( b \) iff it is definable in \( \text{FO}[+, V_b] \).

\( V_b(n) = b^k \) 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 $\text{FO}[<, \text{mod}]$.

Figure: $x = 3 \lor (x = 0 \mod 3 \land y = 0 \mod 2 \land y > x)$
Characterization

Theorem

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

Theorem

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

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

**Theorem**

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

**Theorem**

\( R \in \text{FO}[<, \mod k] \) iff

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

**Theorem (Cooper 72)**

Quantifier-free \( \text{FO}[+, =, \leq, <, \mod] \) 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 FO[+] set is decidable in polynomial time.*

Theorem (Marsault-Sakarovitch 13)

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

Theorem

*Deciding if a deterministic automaton accepts a FO[<, mod] set is decidable in time 3-EXP.*
First easy solutions, two 3-EXP algorithms

**Theorem**

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

- Obtaining a polynomial-size FO[+] formula by Leroux 06
- Checking if the formula could be stated in FO[<, mod] by Choffrut 08
- Stating $\phi$ in FO[+, $R$] "$R$ is regular" by Milchior 13
- Rewriting $\phi$ 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 $R \in \text{FO}[+, V_b]$. There exists an algorithm in polynomial time that accepts iff $R$ is in $\text{FO}[<, \mod]$.

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

Theorem (Computation of the formula)

There exists an algorithm that computes a $\text{FO}[<, \mod, +C, = C]$-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 \( \text{FO}[\text{mod}] \) and when \( C \subseteq \mathbb{N} \),
\( X \subseteq \{+C, = C, =, <\} \) it works for \( \Pi_0[X, \text{mod}] \).
Further research

Open question:
- If the alphabet is $[0, b - 1]^*$, is there a polynomial time algorithm?
- Is there a polynomial time algorithm for $\text{FO}[\prec]$ or $\text{FO}[\prec, \text{mod } k]$?
Further research

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

Conjecture
The algorithm works for $\text{FO}[^<, \text{mod}, \times b]$
Further research

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

Conjecture
The algorithm works for $\text{FO}[\prec, \text{mod}, \times b]$

Thank you