

New proofs of Shepherdson's theorem.

Olivier Gauwin and Géraud Sénizergues

LaBRI, Bordeaux.

Seminar GREYC, Caen, 30/01/2024

contents

- 1 INTRODUCTION
- 2 TWO-WAY finite automata
- 3 Proof by REWRITING
- 4 Proof by MSO over WORDS
- 5 WORDS of WORDS
- 6 Proof by GAMES over 2-pushdowns
- 7 Proof by MSO over WORDS-of-WORDS
- 8 Perspectives

INTRODUCTION

THE theorem

Theorem (Shepherdson 59, RabinScott 59)

*Every language recognized by a **two-way** automaton is **regular**.*

Previous proofs

[J.C. Shepherdson; IBM Journal of Research and Development, 1959]

consolidated by: [C. Doczkal and G. Smolka Journal of Automated Reasoning, 2018]

[M.O. Rabin and D. Scott; IBM Journal of Research and Development, 1959]

consolidated by: [E. Filiot and O. Gauwin and P-A Reynier and F. Servais LICS 2013]

[J.C. Birget; Theoret. Comput. Sci., 1989]

[M.Y. Vardi; Information Processing Letters, 1989]

[J. Sakarovitch; Elements of Automata Theory, 2009]

[M. Hulden; CIAA 2015]

Previous tools

The **old** tools we use in our **new** proofs.

[J. R. Büchi; Arch. Math. Logik Grundlag. 1964]

[J. R. Büchi and W. H. Hosken; Math. Syst. Theory, 1970]

[M.O. Rabin; Decidability of second-order theories and automata on infinite trees, TAMS 1969]

[M.Hague and C.H. Luke Ong; FOSSACS 2007]

[S. Fratani; Theoretical Computer Science 2012]

Our contribution

We **translate** 2 way finite automata into

- new **rewriting systems** over words
- new **rewriting systems** over words-of-words

The *new* proofs

Idea 1-2:

The language accepted by a 2-way f.a. is the set of consequences of a finite set of axioms, via a *right-linear deduction system* ([Büchi-Hosken])

Proof 1: based on [Büchi, 1964],[Büchi-Hosken, 1970]

Proof 2: based on [M.O. Rabin, 1969]

The new proofs

Idea 3-4:

Construct an embedding $\varphi : A^* \times A^* \hookrightarrow A^{[2]}$ such that the binary relation $\text{TRANS}(w, w')$:

$$\exists u, v \in A^*, \exists x \in A, w = \varphi(u, xv), w' = \varphi(ux, v)$$

is expressible as the **transition-relation** of some **order 2 pushdown-automaton**.

Proof 3: based on [Hague-Ong 2007] showing that the set of winning positions of an accessibility game over pushdown automaton of order 2, is Meyer-regular.

Proof 4: The relation $\text{TRANS}(w, w')$ is **MSO-definable** in the structure $A^{[2]}$.

Proof is based on [Fratani, 2012] that gives an automatic characterisation of the definable subsets of $A^{[2]}$.

TWO-WAY finite automata

Definitions

A finite *two-way automaton* is a tuple

$$\mathcal{A} = (Q, A, \ominus, \oslash, \Delta, I, F),$$

where Q is a finite set of states,

$I \subseteq Q$ is the set of initial states

$F \subseteq Q$ the set of final states,

A is an alphabet,

and \ominus and \oslash are special letters not in A .

We note $\hat{A} := A \cup \{\ominus, \oslash\}$.

A *configuration* of the two-way automaton \mathcal{A} is a tuple

$$(q, u, v) \in Q \times \hat{A}^* \times \hat{A}^*.$$

Definitions

Given $a, a' \in \hat{A}$, $u, v, u', v' \in \hat{A}^*$, and $q, q' \in Q$, we write:

$$\begin{aligned} (q, u, av) \vdash_{\mathcal{A}} (q', ua, v) & \text{ if } (q, a, q', \triangleright) \in \Delta \\ (q, ua, a'v) \vdash_{\mathcal{A}} (q', u, aa'v) & \text{ if } (q, a', q', \triangleleft) \in \Delta \end{aligned}$$

A word $u \in A^{[1]}$ is *accepted* by \mathcal{A} iff

$$(q_0, \epsilon, \odot u \odot) \vdash_{\mathcal{A}}^* (q_f, v, v')$$

with $q_0 \in I$ and $q_f \in F$, for some $v, v' \in \hat{A}^*$.

Proof by REWRITING

The rewriting rules

Alphabet: $A \cup \{[p, q] \mid p, q \in Q\}$ Set D of deduction rules:

$$\overline{u[p, p]}$$

for all $u \in \hat{A}^*, p \in Q$

$$\frac{ua[q, r]}{uab[p, s]}$$

if $(p, b, q, \triangleleft) \in \Delta, (r, a, s, \triangleright) \in \Delta$

$$\frac{u[p, q], u[q, r]}{u[p, r]}$$

if $p, q, r \in Q$.

The rewriting rules

For every $u \in A^*$, $p, q \in Q$, $a \in A$:

$$(p, u, a) \vdash^* (q, u, a)$$

iff

$$\frac{}{ua[p, q]} D$$

Hence the language L recognized by \mathcal{A} is equal to:

$$\{u \in A^* \mid \exists p \in I, \exists q \in F, \frac{}{\ominus u \ominus [p, q]} D\}$$

The proof

Theorem (Büchi-Hosken, 1970)

For every finite set D of right-linear deduction rules, the set of all provable words is a regular set.

By this theorem L is **regular**.

Proof by MSO logics over words

Proof by MSO over WORDS

The language P of provable words (modulo D) is the smallest subset $X \subseteq A^*$ such that:

$$\forall u \in \widehat{A}^*, p, q, r, s \in Q, (p, b, q, \triangleleft), (r, a, s, \triangleright) \in \Delta$$

$$u[p, p] \in X, \quad ua[q, r] \in X \rightarrow uab[p, s] \in X$$

$$(u[p, q] \in X \text{ and } u[q, r] \in X) \rightarrow u[p, r] \in X.$$

Hence there exists a **MSO formula** Φ , with only one free variable X , which is a set-variable, such that

$$A^*, v \models \Phi \text{ if and only if } v(X) = P.$$

Proof by MSO over WORDS

Theorem (Rabin 1969)

*The **regular** subsets of A^* are exactly the **MSO-definable** subsets of A^* .*

It follows that P is regular, which implies that

$$L = \{u \in X^* \mid \exists p \in I, q \in F, \otimes u \otimes [p, q] \in P\}$$

is regular too.

WORDS of WORDS

Words of words

A *word of words* over A is a word over the alphabet A^* , i.e. a finite sequence of finite words over A .

Notation:

$A^{[1]}$: the set A^* of words over A ,

$A^{[2]}$: the set of words of words over A .

Examples:

$A = \{a, b, c\}$

$abbcab, abba, \varepsilon$ are **words**

$[a, bbc, b], [abba, \varepsilon, bb, bbb bca], [\varepsilon], []$ are **words of words**.

Concatenations:

$aba \cdot_1 caaa = abacaaa$

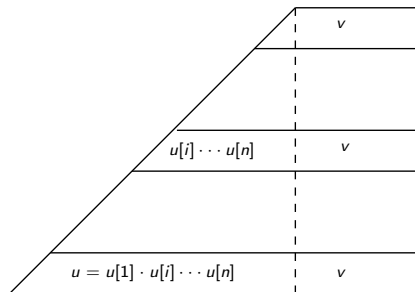
$[aba, c] \cdot_2 [c, ba] = [aba, c, c, ba]$.

Words of words

A language $L \subseteq A^{[2]}$ is said *Meyer-regular* iff, viewed as a language over $(A \cup \{ "[", " ", " ", "]" \})^*$ it is regular.

(i.e. the metasymbols, square brackets and commas , are treated as ordinary symbols)

Encoding pairs of words

Figure: The encoding of (u, v)

Encoding pairs of words

$$\varphi : A^{[1]} \hookrightarrow A^{[2]}$$

$$\varphi(u, v) = [v, u_n v, u_{n-1} u_n v, \dots, uv]$$

$$\varphi(cba, ba) = [ba, aba, baba, cbaba]$$

Encoding pairs of words

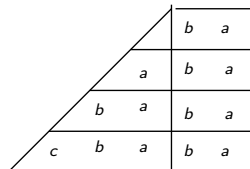


Figure: $\varphi(cba, ba)$

Encoding moves

For all $u, v \in A^{[1]}$ and $a \in A$,

$$\varphi(u, av) = [av, \dots, uav], \quad \varphi(ua, v) = [\textcolor{red}{v}, av, \dots, uav]$$

and

$$[av, \dots, uav] \xrightarrow{\text{push}_2} \xrightarrow{\text{pop}_1} [\textcolor{red}{v}, av, \dots, uav].$$

$$[\textcolor{red}{v}, av, \dots, uav] \xrightarrow{\text{pop}_2} [av, \dots, uav].$$

Proof by GAMES over 2-pushdowns

level 2 pushdowns

An level-2 pushdown automaton has:

- an input alphabet X
- a finite set of states Q
- a memory with contents in $A^{[2]}$
- a set of transitions

$$\Delta \subseteq Q \times X \times A \times Q \times \mathcal{O}$$

where

$$\mathcal{O} = \{\text{pop}_1, \text{pop}_2, \text{push}_2\} \cup \{\text{push}_1^a \mid a \in A\}.$$

level 2 pushdowns

For $a \in A$, $n \geq 1$ and $u, u_1, \dots, u_n \in A^{[1]}$,

$$\begin{array}{lll}
 \text{pop}_1([u_1, \dots, u_n]) & = & [\text{pop}_1(u_1), u_2, \dots, u_n] \quad \text{where } \text{pop}_1(au) = u \\
 \text{pop}_2([u_1, \dots, u_n]) & = & [u_2, \dots, u_n] \quad \text{when } n > 1 \\
 \text{push}_1^a([u_1, \dots, u_n]) & = & [\text{push}_1^a(u_1), u_2, \dots, u_n] \quad \text{where } \text{push}_1^a(u) = au \\
 \text{push}_2([u_1, \dots, u_n]) & = & [u_1, u_1, u_2, \dots, u_n]
 \end{array}$$

Games over level 2 pushdowns

Theorem (Hague-Ong2007)

Let \mathcal{A} be some order-2 pushdown automaton. Given a Meyer-regular set of configurations C , the set of configurations $\{c' \in Q \cdot A^{[2]} \mid \exists c \in C, c' \vdash_{\mathcal{A}}^ c\}$ is regular too.*

The proof

Let \mathcal{A} be a 2-way finite automaton with set of states Q , input-alphabet A . We construct a level-2 pushdown automaton, with set of states $Q \cup R$, stack-alphabet \hat{A} and transitions such that:

$$(p, u, v) \mapsto p \cdot \varphi(u, v)$$

embeds the set configurations of \mathcal{A} into the set of configurations of \mathcal{B} and

$$(p, u, v) \vdash_{\mathcal{A}}^* (q, u', v') \Leftrightarrow p \cdot \varphi(u, v) \vdash_{\mathcal{B}}^* q \cdot \varphi(u', v').$$

The proof

$$\begin{aligned}
 u \in L &\Leftrightarrow \\
 \exists u', v' \in \hat{A}^* \bigvee_{p \in I, q \in F} (p, \varepsilon, \odot u \odot) &\vdash_{\mathcal{A}}^* (q, u, v') \Leftrightarrow \\
 \exists u', v' \in \hat{A}^* \bigvee_{p \in I, q \in F} p \varphi(\varepsilon, \odot u \odot) &\vdash_{\mathcal{B}}^* q \cdot \varphi(u, v') \Leftrightarrow \\
 \exists w' \in \hat{A}^{[2]}, \bigvee_{p \in I, q \in F} p \cdot [\odot u \odot] &\vdash_{\mathcal{B}}^* q \cdot w'.
 \end{aligned}$$

Since $\hat{A}^{[2]}$ is Meyer-regular,
 by [Hague-ong 2007], for very $p \in I, q \in F$,
 the set $\{[\odot u \odot] \mid p \cdot [\odot u \odot] \vdash_{\mathcal{B}}^* q \cdot \hat{A}^{[2]}\}$ is Meyer-regular,
 hence L is regular.

Proof by MSO over WORDS-of-WORDS

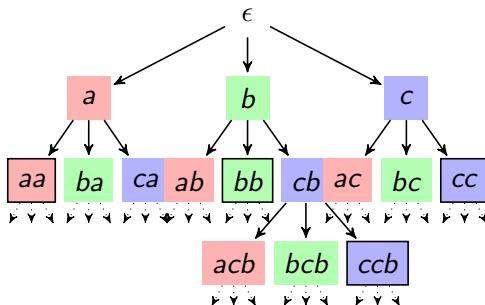
MSO over words-of-words

We consider the structure

$$\mathcal{S}_A^{**} = \langle A^{[2]}, (\text{letter}_a^{**})_{a \in A}, \text{son}_1^*, \text{clone}_1^*, \text{son}_2, \text{clone}_2 \rangle$$

- $\mathcal{S}_A^{**}, v \models \text{letter}_a^{**}(x)$ holds when $v(x) = [a \cdot_1 u] \cdot_2 v$ for some $u \in A^{[1]}, v \in A^{[2]}$,
- $\mathcal{S}_A^{**}, v \models \text{son}_1^*(x, y)$ holds when $v(x) = [u] \cdot_2 w$ and $v(y) = [au] \cdot_2 w$, for some $a \in A, u \in A^{[1]}$, and $w \in A^{[2]}$,
- $\mathcal{S}_A^{**}, v \models \text{clone}_1^*(x)$ holds when $v(x) = [aa u] \cdot_2 w$ for some $a \in A, w \in A^{[2]}$,
- $\mathcal{S}_A^{**}, v \models \text{son}_2(x, y)$ holds when $v(y) = [u] \cdot_2 v(x)$ for some $u \in A^{[1]}$,
- $\mathcal{S}_A^{**}, v \models \text{clone}_2(x)$ holds when $v(x) = [u, u] \cdot_2 w$ for some $u \in A^{[1]}$ and $w \in A^{[2]}$.

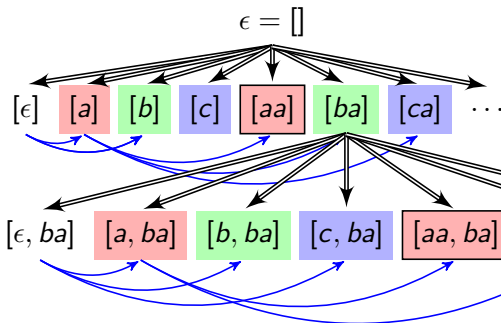
MSO over words-of-words

 \mathcal{S}_A^* :

relations:

 $\text{letter}_a^*(x)$ $\text{letter}_b^*(x)$ $\text{letter}_c^*(x)$ $\text{clone}_1(x)$
 $\text{son}_1(x, y)$
 $x \longrightarrow y$
Figure: Structure \mathcal{S}_A^* for $A = \{a, b, c\}$ (partial representations).

MSO over words-of-words

 \mathcal{S}_A^{**} :

relations:

 $\text{letter}_a^{**}(x)$ $\text{letter}_b^{**}(x)$ $\text{letter}_c^{**}(x)$ $\text{clone}_1^*(x)$ $\text{son}_1^*(x, y)$
 $x \xrightarrow{\quad} y$ $\text{clone}_2(x)$ $\text{son}_2(x, y)$
 $x \xrightarrow{\quad} y$ Figure: Structure \mathcal{S}_A^{**} for $A = \{a, b, c\}$ (partial representation).

definability within MSO

Lemma

Given a *two-way finite automaton* \mathcal{A} over a finite alphabet A , the set $[L(\mathcal{A})] = \{[u] \mid u \in L(\mathcal{A})\} \subseteq A^{[2]}$, is *definable* by an MSO formula $\Psi(x)$ over S_A^{**} .

definability within MSO

The key-idea is that one can express , within MSO over \mathcal{S}_A^{**} , the movement relation:

$$(u, av) \vdash (ua, v)$$

We construct a MSO formula $\text{Link}(*, *)$ such that, for all $y, z \in \text{Im}(\varphi)$,

$$\mathcal{S}_A^{**} \models \text{Link}(y, z)$$

iff there exist $u \in A^{[1]}$, $a \in A$, $v \in A^{[1]}$ such that

$$y = \varphi(u, av) \text{ and } z = \varphi(ua, v)$$

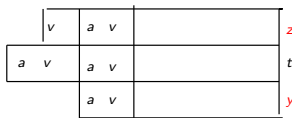


Figure: Formula $\text{Link}(y, z)$

definability within MSO

	v	a v		<i>z</i>
a v		a v		<i>t</i>
		a v		<i>y</i>

$$\text{Link}(\textcolor{red}{y}, \textcolor{red}{z}) := \exists t, \text{son}_2(\textcolor{red}{y}, t) \wedge \text{clone}_2(t) \wedge \text{son}_1^*(\textcolor{red}{z}, t)$$

lemma “a la Fatou”

Lemma (Fatou property)

Let $L \subseteq A^{[1]}$ such that $[L]$ is MSO-definable in $A^{[2]}$. Then L is MSO-definable in $A^{[1]}$.

This lemma can be deduced from the characterisation of definable subsets by oracle-automata over the “differential notation” of the words-of-words([Fratani 2012]).

End of the proof

Since $[L]$ is MSO-definable in $A^{[2]}$, L is MSO-definable in $A^{[1]}$ (by Fatou property) and by Rabin's theorem, L is regular.

Perspectives

- Extend Shepherdson's theorem to words of words ? to $A^{[n]}$ for $n \geq 2$?
- Find *logical proofs* for problems about *transductions* ?
- Find new *algebraic proofs* for Shepherdson's theorem. Can we use the links with the *free inverse monoid*?