Automata in W-Toposes, and General Myhill-Nerode Theorems[1]

Victor Iwaniack

Laboratoire J. A. Dieudonné, Université Côte d'Azur

CMCS 2024, April 6

[1]This project has been partially funded by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No.670624).

A coalgebraic motivation

Given a (deterministic complete) automaton over Σ

$$(Q, \quad i \in Q, \quad F \subset Q, \quad \delta : Q \times \Sigma \to Q)$$

if we forget the initial state we can represent it as a coalgebra for the endofunctor $F(-) = \Omega \times (-)^{\Sigma}$

A coalgebraic motivation

Given a (deterministic complete) automaton over Σ

$$(Q, \quad i \in Q, \quad F \subset Q, \quad \delta : Q \times \Sigma \to Q)$$

if we forget the initial state we can represent it as a coalgebra for the endofunctor $F(-) = \Omega \times (-)^{\Sigma}$

$$Q \xrightarrow{(\delta^{\dashv}, \chi_F)} \Omega \times Q^{\Sigma}$$

by using the *exponential* Q^{Σ}, the *subset classifier* $\Omega := \{\bot, \top\}$ and the *characteristic function* $\chi_F : Q \to \Omega$ defined by $\chi_F(q) = \top$ if $q \in F$ and $\chi_F(q) = \bot$ otherwise.

Exponentials and subobjects classifiers are typical of toposes.

Toposes

Definition

An *(elementary) topos* is a category $\mathcal{E}$ with

- finite limits, in particular a terminal object $\mathbb{1}$
- *exponentials*: for all objects A and B, an object B^A such that

$$\mathcal{E}(A \times X, B) \cong \mathcal{E}(X, B^A) \text{ natural in } A, B, X$$

Toposes

Definition

An *(elementary) topos* is a category $\mathcal{E}$ with

- finite limits, in particular a terminal object $\mathbb{1}$
- *exponentials*: for all objects A and B, an object B^A such that

$$\mathcal{E}(A \times X, B) \cong \mathcal{E}(X, B^A) \text{ natural in } A,\ B,\ X$$

- a *subobject classifier* i.e. $\top : \mathbb{1} \to \Omega$ such that for each object A and subobject $S \hookrightarrow A$, there exists a unique morphism $\chi_S : A \to \Omega$, such that

$$\begin{array}{ccc} S & \xrightarrow{\ !\ } & \mathbb{1} \\ \big\downarrow & \lrcorner & \big\downarrow \top \\ A & \xrightarrow[\chi_S]{} & \Omega \end{array}$$

  i.e. $\mathrm{Sub}(A) \cong \mathcal{E}(A, \Omega)$ naturally in A

A theorem ensures that toposes also have finite colimits (in particular an initial object $\emptyset$).

G-sets toposes (another motivation)

Set is a topos with $B^A := \{\text{functions } A \to B\}$ and $\Omega := \{\bot, \top\}$

G-sets toposes (another motivation)

Set is a topos with $B^A := \{\text{functions } A \to B\}$ and $\Omega := \{\bot, \top\}$

Example

For a discrete group G, the category $G\,\text{Set}$ of G-sets and equivariant functions is a topos with

- exponential of $(B, \cdot)$ to the $(A, \cdot)$ the set B^A with the action, for all $f : A \to B, g \in G$

$$(f \cdot g)(x) = f(x \cdot g^{-1}) \cdot g$$

so that f is equivariant iff a fixed point of this action

G-sets toposes (another motivation)

Set is a topos with $B^A := \{\text{functions } A \to B\}$ and $\Omega := \{\bot, \top\}$

Example

For a discrete group G, the category $G\,\mathrm{Set}$ of G-sets and equivariant functions is a topos with

- exponential of $(B, \cdot)$ to the $(A, \cdot)$ the set B^A with the action, for all $f : A \to B, g \in G$
$$(f \cdot g)(x) = f(x \cdot g^{-1}) \cdot g$$
so that f is equivariant iff a fixed point of this action
- subobject classifier the set $\Omega := \{\bot, \top\}$ with trivial action

Connected objects

In any topos we have unions and intersections of subobjects, where $S \leq A$ means "S is a subobject of A":

Connected objects

In any topos we have unions and intersections of subobjects, where $S \leq A$ means "S is a subobject of A":

Definition

Let $\mathcal{E}$ be a topos and A any of its objects.

1. $S \leq A$ is *complemented* if there exists $C \leq A$ s.t. $S \cup C = A$ and $S \cap C = \emptyset$.

Connected objects

In any topos we have unions and intersections of subobjects, where $S \leq A$ means "S is a subobject of A":

Definition

Let $\mathcal{E}$ be a topos and A any of its objects.

1. $S \leq A$ is *complemented* if there exists $C \leq A$ s.t. $S \cup C = A$ and $S \cap C = \emptyset$.
2. A is *connected* if it admits exactly two complemented subobjects ($\emptyset$ and A)

Connected objects

In any topos we have unions and intersections of subobjects, where $S \leq A$ means "S is a subobject of A":

Definition

Let $\mathcal{E}$ be a topos and A any of its objects.

1. $S \leq A$ is *complemented* if there exists $C \leq A$ s.t. $S \cup C = A$ and $S \cap C = \emptyset$.
2. A is *connected* if it admits exactly two complemented subobjects ($\emptyset$ and A)

Example

A G-set A is connected iff non-empty transitive i.e. is an orbit.

Atomic toposes

Any G-set can be decomposed into a sum of its orbits i.e. every object of $G\,\mathrm{Set}$ is a coproduct of connected objects

Definition

A topos $\mathcal{E}$ is *atomic* if

- it is *locally connected* i.e. every object is a coproduct of connected objects;

Atomic toposes

Any G-set can be decomposed into a sum of its orbits i.e. every object of $G\,\mathrm{Set}$ is a coproduct of connected objects

Definition

A topos $\mathcal{E}$ is *atomic* if

- it is *locally connected* i.e. every object is a coproduct of connected objects;
- it is *Boolean* i.e. every subobject is complemented.

Atomic toposes

Any G-set can be decomposed into a sum of its orbits i.e. every object of $G\,\mathrm{Set}$ is a coproduct of connected objects

Definition

A topos $\mathcal{E}$ is *atomic* if

- it is *locally connected* i.e. every object is a coproduct of connected objects;
- it is *Boolean* i.e. every subobject is complemented.

In an atomic topos, connected objects are atoms i.e. they have no proper subobjects.

Example

$G\,\mathrm{Set}$ are atomic.

Internal monoids and W-toposes

An internal monoid in a topos $\mathcal{E}$ is an object M endowed with

- a multiplication morphism $m : M \times M \to M$;
- a unit *global element* i.e. a morphism $e : \mathbb{1} \to M$

satisfying associativity and unitality. We denote by $\mathrm{Mon}(\mathcal{E})$ the category of internal monoid and internal monoid morphisms.

Internal monoids and W-toposes

An internal monoid in a topos $\mathcal{E}$ is an object M endowed with

- a multiplication morphism $m : M \times M \to M$;
- a unit *global element* i.e. a morphism $e : \mathbb{1} \to M$

satisfying associativity and unitality. We denote by $\mathrm{Mon}(\mathcal{E})$ the category of internal monoid and internal monoid morphisms.

Proposition

For any object A of a topos $\mathcal{E}$, A^A is canonically endowed with an internal monoid structure.

Internal monoids and W-toposes

An internal monoid in a topos $\mathcal{E}$ is an object M endowed with

- a multiplication morphism $m : M \times M \to M$;
- a unit *global element* i.e. a morphism $e : \mathbb{1} \to M$

satisfying associativity and unitality. We denote by $\mathrm{Mon}(\mathcal{E})$ the category of internal monoid and internal monoid morphisms.

Proposition

For any object A of a topos $\mathcal{E}$, A^A is canonically endowed with an internal monoid structure.

Definition

A *W-topos* is a topos admitting free monoids $(\Sigma^*, m_\Sigma, \varepsilon_\Sigma)$ for all Σ i.e. for all object Σ and internal monoid M we have a natural isomorphism

$$\mathcal{E}(\Sigma, M) \cong \mathrm{Mon}(\mathcal{E})(\Sigma^*, M)$$

Internal monoids and W-toposes

An internal monoid in a topos $\mathcal{E}$ is an object M endowed with

- a multiplication morphism $m : M \times M \to M$;
- a unit *global element* i.e. a morphism $e : \mathbb{1} \to M$

satisfying associativity and unitality. We denote by $\mathrm{Mon}(\mathcal{E})$ the category of internal monoid and internal monoid morphisms.

Proposition

For any object A of a topos $\mathcal{E}$, A^A is canonically endowed with an internal monoid structure.

Definition

A *W-topos* is a topos admitting free monoids $(\Sigma^*, m_\Sigma, \varepsilon_\Sigma)$ for all Σ i.e. for all object Σ and internal monoid M we have a natural isomorphism

$$\mathcal{E}(\Sigma, M) \cong \mathrm{Mon}(\mathcal{E})(\Sigma^*, M)$$

Toposes $G\,\mathrm{Set}$ are W-toposes because they have countable coproducts: $\Sigma^* := \sum_{n \in \mathbb{N}} \Sigma^n$.

Languages and automata in a W-topos

We now work in a W-topos $\mathcal{E}$ and fix an alphabet Σ.

Languages and automata in a W-topos

We now work in a W-topos $\mathcal{E}$ and fix an alphabet Σ.

A language is any subobject $L \leq \Sigma^*$, and a Σ-automaton $\mathcal{A}$ is the data of

$$(Q, \quad \mathbb{1} \xrightarrow{i} Q, \quad Q \xrightarrow{\chi_F} \Omega, \quad Q \times \Sigma \xrightarrow{\delta} Q)$$

Languages and automata in a W-topos

We now work in a W-topos $\mathcal{E}$ and fix an alphabet Σ.

A language is any subobject $L \leq \Sigma^*$, and a Σ-automaton $\mathcal{A}$ is the data of

$$(Q, \quad \mathbb{1} \xrightarrow{i} Q, \quad Q \xrightarrow{\chi_F} \Omega, \quad Q \times \Sigma \xrightarrow{\delta} Q)$$

and to define the language recognised by $\mathcal{A}$ we use

$$\begin{array}{c} \mathcal{E}(Q \times \Sigma, Q) \xrightarrow{\text{currying}} \mathcal{E}(\Sigma, Q^Q) \xrightarrow{\text{free monoids}} \mathsf{Mon}(\mathcal{E})(\Sigma^*, Q^Q) \xrightarrow{\text{forget}} \mathcal{E}(\Sigma^*, Q^Q) \xrightarrow{\text{uncurrying}} \mathcal{E}(Q \times \Sigma^*, Q) \\ \delta \longmapsto \delta^* \end{array}$$

Languages and automata in a W-topos

We now work in a W-topos $\mathcal{E}$ and fix an alphabet Σ.

A language is any subobject $L \leq \Sigma^*$, and a Σ-automaton $\mathcal{A}$ is the data of

$$(Q, \quad \mathbb{1} \xrightarrow{i} Q, \quad Q \xrightarrow{\chi_F} \Omega, \quad Q \times \Sigma \xrightarrow{\delta} Q)$$

and to define the language recognised by $\mathcal{A}$ we use

$$\mathcal{E}(Q \times \Sigma, Q) \xrightarrow{\text{currying}} \mathcal{E}(\Sigma, Q^Q) \xrightarrow{\text{free monoids}} \mathrm{Mon}(\mathcal{E})(\Sigma^*, Q^Q) \xrightarrow{\text{forget}} \mathcal{E}(\Sigma^*, Q^Q) \xrightarrow{\text{uncurrying}} \mathcal{E}(Q \times \Sigma^*, Q)$$

$$\delta \longmapsto \delta^*$$

Definition

The language $L(\mathcal{A})$ recognised by $\mathcal{A} = (Q, i, F, \delta)$ is defined by its characteristic morphism

$$\Sigma^* \cong \mathbb{1} \times \Sigma^* \xrightarrow{i \times \Sigma^*} Q \times \Sigma^* \xrightarrow{\delta^*} Q \xrightarrow{\chi_F} \Omega$$

In Set it is really $w \in L(\mathcal{A})$ iff $\delta^*(i, w) \in F$.

Categories of Automata

Our goal now is to compute "the" "minimal" automaton of a given language L (c.f. Colcombet and Petrișan's 2020 "Automata minimization: a functorial approach").

Categories of Automata

Our goal now is to compute “the” “minimal” automaton of a given language L (c.f. Colcombet and Petrișan's 2020 “Automata minimization: a functorial approach”).

We define automaton morphisms $\alpha : \mathcal{A} \to \mathcal{A}' = (Q', i', \chi_{F'}, \delta')$ as morphisms $\alpha : Q \to Q'$ of $\mathcal{E}$ such that the following diagrams commute:

$$\begin{array}{ccc} Q \times \Sigma & \xrightarrow{\delta} & Q \\ {\scriptstyle \alpha\times\Sigma}\big\downarrow & & \big\downarrow{\scriptstyle \alpha} \\ Q' \times \Sigma & \xrightarrow[\delta']{} & Q' \end{array} \quad \text{and} \quad \begin{array}{ccccc} & \overset{i}{\nearrow} & Q & \overset{\chi_F}{\searrow} & \\ \mathbb{1} & & {\scriptstyle \alpha}\big\downarrow & & \Omega \\ & \underset{i'}{\searrow} & Q' & \underset{\chi_{F'}}{\nearrow} & \end{array}$$

Categories of Automata

Our goal now is to compute "the" "minimal" automaton of a given language L (c.f. Colcombet and Petrișan's 2020 "Automata minimization: a functorial approach").

We define automaton morphisms $\alpha : \mathcal{A} \to \mathcal{A}' = (Q', i', \chi_{F'}, \delta')$ as morphisms $\alpha : Q \to Q'$ of $\mathcal{E}$ such that the following diagrams commute:

$$
\begin{array}{ccc}
Q \times \Sigma & \xrightarrow{\delta} & Q \\
{\scriptstyle \alpha \times \Sigma}\downarrow & & \downarrow{\scriptstyle \alpha} \\
Q' \times \Sigma & \xrightarrow[\delta']{} & Q'
\end{array}
\quad \text{and} \quad
\begin{array}{ccccc}
 & \overset{i}{\nearrow} & Q & \overset{\chi_F}{\searrow} & \\
\mathbb{1} & & {\scriptstyle \alpha}\downarrow & & \Omega \\
 & \underset{i'}{\searrow} & Q' & \underset{\chi_{F'}}{\nearrow} &
\end{array}
$$

The existence of an automaton morphism $\alpha : \mathcal{A} \to \mathcal{A}'$ entails $L(\mathcal{A}) = L(\mathcal{A}')$.

Definition

We denote by $\text{Auto}(L)$ the category of L-automata (i.e. that recognise L) and automaton morphisms.

Minimal object of a category with a factorisation system

Definition

In a category $\mathscr{C}$ endowed with a factorisation system (E, M), we say an object X *divides* an object Y if there exists a span

$$X \xleftarrow{e \in E} Z \xrightarrow{m \in M} Y$$

in $\mathscr{C}$. An object is *minimal* if it divides any object of $\mathscr{C}$.

If $(E, M) = (\mathrm{epi}, \mathrm{mono})$, then "dividing" is "being a subquotient"

Minimal object of a category with a factorisation system

Definition

In a category $\mathscr{C}$ endowed with a factorisation system (E, M), we say an object X *divides* an object Y if there exists a span

$$X \overset{e \in E}{\twoheadleftarrow} Z \overset{m \in M}{\hookrightarrow} Y$$

in $\mathscr{C}$. An object is *minimal* if it divides any object of $\mathscr{C}$.

If $(E, M) = (\mathrm{epi}, \mathrm{mono})$, then "dividing" is "being a subquotient"

Proposition ([CP20, Lemma 2.3])

If moreover $\mathscr{C}$ admits initial $\emptyset$ and terminal $\mathbb{1}$ objects, then the factorisation of the unique $\emptyset \xrightarrow{!} \mathbb{1}$:

$$\emptyset \overset{e \in E}{\twoheadrightarrow} \mathrm{Min} \overset{m \in M}{\hookrightarrow} \mathbb{1}$$

provides a minimal object Min.

Minimal automaton

Lemma

The (epi, mono) factorisation system of $\mathcal{E}$ *lifts to* $\mathrm{Auto}(L)$.

Minimal automaton

Lemma

The (epi, mono) factorisation system of $\mathcal{E}$ lifts to $\mathrm{Auto}(L)$*.*

Lemma

$\mathrm{Auto}(L)$ *admits initial* $\mathrm{Init}(L) = (\Sigma^*, \dots)$ *and terminal* $\mathrm{Term}(L) = (\Omega^{\Sigma^*}, \dots)$ *automata, and the unique morphism* $\mathrm{Init}(L) \xrightarrow{!} \mathrm{Term}(L)$ *is given by*

$$(m_\Sigma \chi_L)^\dashv : \Sigma^* \to \Omega^{\Sigma^*} \text{ adjunct of } \Sigma^* \times \Sigma^* \xrightarrow{m_\Sigma} \Sigma^* \xrightarrow{\chi_L} \Omega$$

In Set, $(m_\Sigma \chi_L)^\dashv(u) = \{v \in \Sigma^* | uv \in L\} = u^{-1}L$.

Minimal automaton

Lemma

The (epi, mono) factorisation system of $\mathcal{E}$ lifts to Auto(L).

Lemma

Auto(L) *admits initial* $\mathrm{Init}(L) = (\Sigma^*, \dots)$ *and terminal* $\mathrm{Term}(L) = (\Omega^{\Sigma^*}, \dots)$ *automata, and the unique morphism* $\mathrm{Init}(L) \xrightarrow{!} \mathrm{Term}(L)$ *is given by*

$$(m_\Sigma \chi_L)^\dashv : \Sigma^* \to \Omega^{\Sigma^*} \text{ adjunct of } \Sigma^* \times \Sigma^* \xrightarrow{m_\Sigma} \Sigma^* \xrightarrow{\chi_L} \Omega$$

In Set, $(m_\Sigma \chi_L)^\dashv(u) = \{v \in \Sigma^* | uv \in L\} = u^{-1}L$.

Corollary

The factorisation of the unique $\mathrm{Init}(L) \xrightarrow{!} \mathrm{Term}(L)$*:*

$$\mathrm{Init}(L) \xrightarrow{e \text{ epic}} \mathrm{Min}(L) \xrightarrow{m \text{ monic}} \mathrm{Term}(L)$$

provides an automaton Min(L) *that is a subquotient of every other L-automaton.*

Internal Nerode Congruence

$$\mathsf{Init}(L) \xrightarrow{e \text{ epic}} \mathsf{Min}(L) \xhookrightarrow{m \text{ monic}} \mathsf{Term}(L)$$

is the factorisation of $\mathsf{Init}(L) \xrightarrow{!} \mathsf{Term}(L)$ and is done at the stage of the states objects so that the factorisation of $(m_\Sigma \chi_L)^\dashv$:

$$\Sigma^* \twoheadrightarrow \mathsf{Im}((m_\Sigma \chi_L)^\dashv) \hookrightarrow \Omega^{\Sigma^*}$$

provides the states object $\mathsf{Im}((m_\Sigma \chi_L)^\dashv)$ of $\mathsf{Min}(L)$:

Definition

The *Nerode quotient* $\Sigma^*_{/\equiv_L}$ *of* L is the states object of $\mathsf{Min}(L)$ and by definition

$$\Sigma^*_{/\equiv_L} := \mathsf{Im}((m_\Sigma \chi_L)^\dashv)$$

Internal Nerode Congruence

$$\mathsf{Init}(L) \xrightarrow{e \text{ epic}} \mathrel{\mkern-14mu}\rightarrow \mathsf{Min}(L) \xhookrightarrow{m \text{ monic}} \mathsf{Term}(L)$$

is the factorisation of $\mathsf{Init}(L) \xrightarrow{!} \mathsf{Term}(L)$ and is done at the stage of the states objects so that the factorisation of $(m_\Sigma \chi_L)^\dashv$:

$$\Sigma^* \twoheadrightarrow \mathsf{Im}((m_\Sigma \chi_L)^\dashv) \hookrightarrow \Omega^{\Sigma^*}$$

provides the states object $\mathsf{Im}((m_\Sigma \chi_L)^\dashv)$ of $\mathsf{Min}(L)$:

Definition

The *Nerode quotient* $\Sigma^*_{/\equiv_L}$ *of* L is the states object of $\mathsf{Min}(L)$ and by definition

$$\Sigma^*_{/\equiv_L} := \mathsf{Im}((m_\Sigma \chi_L)^\dashv)$$

Because $\mathsf{Min}(L)$ is a subquotient of any L-automaton $\mathcal{A} = (Q, \dots)$ then

Proposition

$\Sigma^*_{/\equiv_L}$ is a subquotient of the state object Q of any L-automaton $\mathcal{A}$.

Myhill-Nerode Theorem for Decomposition-Finiteness

We generalise orbit-finiteness:

Definition

An object of a topos is *decomposition-finite* if it is a **finite** sum of connected objects.

Myhill-Nerode Theorem for Decomposition-Finiteness

We generalise orbit-finiteness:

Definition

An object of a topos is *decomposition-finite* if it is a **finite** sum of connected objects.

Lemma

If the topos $\mathcal{E}$ is atomic, decomposition-finiteness is stable under taking subquotients.

Therefore if there exists an L-automaton $\mathcal{A} = (Q, \dots)$ with decomposition-finite Q, then because $\Sigma^*_{/\equiv_L}$ is a subquotient of Q, $\Sigma^*_{/\equiv_L}$ is decomposition-finite too:

Myhill-Nerode Theorem for Decomposition-Finiteness

We generalise orbit-finiteness:

Definition

An object of a topos is *decomposition-finite* if it is a **finite** sum of connected objects.

Lemma

If the topos $\mathcal{E}$ is atomic, decomposition-finiteness is stable under taking subquotients.

Therefore if there exists an L-automaton $\mathcal{A} = (Q, \dots)$ with decomposition-finite Q, then because $\Sigma^*_{/\equiv_L}$ is a subquotient of Q, $\Sigma^*_{/\equiv_L}$ is decomposition-finite too:

Theorem

In an atomic W-topos $\mathcal{E}$, a language L is recognised by a decomposition-finite automaton (is "decomposition-regular") iff $\Sigma^*_{/\equiv_L}$ is decomposition-finite.

Myhill-Nerode Theorem for Decomposition-Finiteness

We generalise orbit-finiteness:

Definition

An object of a topos is *decomposition-finite* if it is a **finite** sum of connected objects.

Lemma

If the topos $\mathcal{E}$ is atomic, decomposition-finiteness is stable under taking subquotients.

Therefore if there exists an L-automaton $\mathcal{A} = (Q, \dots)$ with decomposition-finite Q, then because $\Sigma^*_{/\equiv_L}$ is a subquotient of Q, $\Sigma^*_{/\equiv_L}$ is decomposition-finite too:

Theorem

In an atomic W-topos $\mathcal{E}$, a language L is recognised by a decomposition-finite automaton (is "decomposition-regular") iff $\Sigma^*_{/\equiv_L}$ is decomposition-finite.

We can change the finiteness conditions and get other Myhill-Nerode type theorems (e.g. Kuratowski-finiteness in Boolean W-toposes).