Equations and logic on words

Sam van Gool

IRIF, Université de Paris

University of York

22 October 2019

Overview

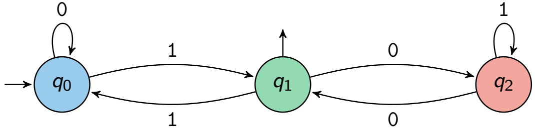
Overview

Regular languages: example

- A programming problem: given a natural number in binary, $w \in \{0,1\}^*$, determine if w is congruent 1 modulo 3.

Regular languages: example

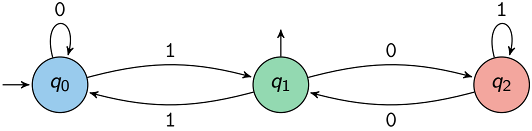
- A programming problem: given a natural number in binary, $w \in \{0, 1\}^*$, determine if w is congruent 1 modulo 3.
- Solution 1: a (deterministic) automaton A:



Answer yes iff A accepts w.

Regular languages: example

- A programming problem: given a natural number in binary, $w \in \{0,1\}^*$, determine if w is congruent 1 modulo 3.
- Solution 1: a (deterministic) automaton A:



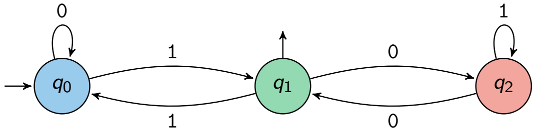
  Answer yes iff A accepts w.
- Solution 2: a homomorphism $\varphi\colon \{0,1\}^* \to S_3$ defined by

$$0 \mapsto (1\,2), \quad 1 \mapsto (0\,1).$$

  Answer yes iff the permutation $\varphi(w)$ sends 0 to 1.

Regular languages: example

- A programming problem: given a natural number in binary, $w \in \{0,1\}^*$, determine if w is congruent 1 modulo 3.
- Solution 1: a (deterministic) automaton A:



Answer yes iff A accepts w.

- Solution 3: an MSO sentence φ:

$\exists Q_0 \exists Q_1 \exists Q_2 (Q_0(\texttt{first}) \wedge Q_1(\texttt{last}) \wedge$

$\forall x [\texttt{0}(x) \wedge Q_0(x) \rightarrow Q_0(\texttt{S}x)] \wedge [\texttt{1}(x) \wedge Q_0(x) \rightarrow Q_1(\texttt{S}x)] \wedge \ldots).$

Answer yes iff w satisfies the formula φ.

Regular languages

Regular languages are subsets $L \subseteq \Sigma^*$ which are ...

- recognizable by a finite automaton;
- invariant under a finite index monoid congruence;
- definable by a monadic second order sentence.

Myhill-Nerode 1958; Büchi 1960

Monoids and finite index congruences

- A monoid is a set M equipped with an associative binary operation and a unit.
- The set Σ^* of finite words is a free monoid.
  - multiplication is concatenation;
  - unit is the empty word ϵ;
- A congruence on M is an equivalence relation θ which respects multiplication.
  - The quotient M/θ is again a monoid;
  - A congruence θ has finite index if M/θ is finite.

Monoids and finite index congruences

- A monoid is a set M equipped with an associative binary operation and a unit.
- The set Σ^* of finite words is a free monoid.
  - multiplication is concatenation;
  - unit is the empty word ϵ;
- A congruence on M is an equivalence relation θ which respects multiplication.
  - The quotient M/θ is again a monoid;
  - A congruence θ has finite index if M/θ is finite.
- Any language $L \subseteq \Sigma^*$ has an associated syntactic congruence, θ_L, i.e., the finest congruence under which L is invariant:

$$w \in L \text{ and } w \theta_L w' \text{ implies } w' \in L.$$

- L is called regular iff θ_L has finite index.

Logic on words

- **Syntax.** Monadic Second Order (MSO) logic over $<$, Σ.
  - Basic propositional connectives: $\wedge$, $\neg$.
  - Quantification over first-order variables x, y, $\ldots$ and monadic second-order variables P, Q, $\ldots$.
  - Relational signature: $x < y$, $\mathtt{a}(x)$ for $a \in \Sigma$.

Logic on words

- **Syntax.** Monadic Second Order (MSO) logic over $<$, Σ.
  - Basic propositional connectives: $\wedge$, $\neg$.
  - Quantification over first-order variables x, y, ... and monadic second-order variables P, Q, ...
  - Relational signature: $x < y$, $\mathtt{a}(x)$ for $a \in \Sigma$.

- **Semantics.** A word $w = a_1 \dots a_n$ gives a structure W.
  - The underlying set of W is $\{1, \dots, n\}$.
  - The natural linear order $<^W$ interprets the binary predicate $<$.
  - For every letter $a \in \Sigma$, $\mathtt{a}^W := \{i \in \{1, \dots, n\} : a_i = a\}$.

Logic on words

- **Syntax.** Monadic Second Order (MSO) logic over $<$, Σ.
- **Semantics.** A word $w = a_1 \ldots a_n$ gives a structure W.

- For a sentence φ, $L_\varphi := \{w \in \Sigma^* \mid w \models \varphi\}$.
- A language L is regular iff $L = L_\varphi$ for some φ in MSO.

- Shortcuts such as $\mathtt{S}(x)$, `first`, `last`, $\subseteq$, ... are MSO-definable.

Logic on words: examples

$\varphi\colon \exists P\big[\ P(\texttt{first}) \land \neg P(\texttt{last}) \land \forall x(P(x) \leftrightarrow \neg P(\texttt{S}(x))\ \big].$

Logic on words: examples

φ: $\exists P \left[P(\texttt{first}) \wedge \neg P(\texttt{last}) \wedge \forall x (P(x) \leftrightarrow \neg P(\texttt{S}(x)) \right]$.

- *aaaa*

Logic on words: examples

$\varphi\colon \exists P\big[\ P(\texttt{first}) \land \neg P(\texttt{last}) \land \forall x(P(x) \leftrightarrow \neg P(\texttt{S}(x))\ \big].$

- $aaaa \models \varphi$,

Logic on words: examples

$$\varphi\colon \exists P\left[\ P(\mathtt{first}) \wedge \neg P(\mathtt{last}) \wedge \forall x(P(x) \leftrightarrow \neg P(\mathtt{S}(x))\ \right].$$

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

Logic on words: examples

$\varphi\colon \exists P\big[\ P(\texttt{first}) \wedge \neg P(\texttt{last}) \wedge \forall x(P(x) \leftrightarrow \neg P(\texttt{S}(x))\ \big].$

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

$\psi\colon \exists P\big[\ \exists x P(x)\ \wedge\ P \subseteq \texttt{a} \wedge \forall y\big(\ (\forall x[P(x) \to x < y])\ \to \texttt{b}(y))\ \big].$

Logic on words: examples

φ: $\exists P\big[\ P(\mathtt{first}) \wedge \neg P(\mathtt{last}) \wedge \forall x(P(x) \leftrightarrow \neg P(\mathtt{S}(x))\ \big]$.

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

ψ: $\exists P\big[\ \exists x P(x)\ \wedge\ P \subseteq \mathtt{a} \wedge \forall y\big(\ (\forall x[P(x) \rightarrow x < y])\ \rightarrow \mathtt{b}(y)\big)\ \big]$.

- *aacbaccaabbb*

Logic on words: examples

φ: $\exists P [\ P(\texttt{first}) \wedge \neg P(\texttt{last}) \wedge \forall x (P(x) \leftrightarrow \neg P(\texttt{S}(x)) \ ]$.

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

ψ: $\exists P [\ \exists x P(x) \ \wedge \ P \subseteq \texttt{a} \wedge \forall y (\ (\forall x [P(x) \rightarrow x < y]) \ \rightarrow \texttt{b}(y)) \ ]$.

- $aacbaccaabbb \models \varphi$,

Logic on words: examples

$\varphi\colon \exists P\big[\ P(\mathtt{first}) \land \neg P(\mathtt{last}) \land \forall x(P(x) \leftrightarrow \neg P(\mathtt{S}(x))\ \big].$

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

$\psi\colon \exists P\big[\ \exists x P(x)\ \land\ P \subseteq \mathtt{a} \land \forall y\big(\ (\forall x[P(x) \to x < y])\ \to \mathtt{b}(y))\ \big].$

- $aacbaccaabbb \models \varphi$, but $aacbaccaabbc \not\models \varphi$.
- $W \models \varphi$ iff W has a non-empty subset of a-positions after which there are only b-positions.

Logic on words: examples

φ: $\exists P\big[\ P(\texttt{first}) \wedge \neg P(\texttt{last}) \wedge \forall x(P(x) \leftrightarrow \neg P(\texttt{S}(x))\ \big]$.

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

ψ: $\exists P\big[\ \exists x P(x)\ \wedge\ P \subseteq \texttt{a} \wedge \forall y\big(\ (\forall x[P(x) \to x < y])\ \to \texttt{b}(y))\ \big]$.

- $aacbaccaabbb \models \varphi$, but $aacbaccaabbc \not\models \varphi$.
- $W \models \varphi$ iff W has a non-empty subset of a-positions after which there are only b-positions.

ψ': $\exists x\big[\ \texttt{a}(x)\ \wedge\ \forall y[x < y \to (\neg\texttt{a}(y) \wedge \texttt{b}(y))]\ \big]$.

Logic on words: examples

φ: $\exists P\big[\ P(\mathtt{first}) \wedge \neg P(\mathtt{last}) \wedge \forall x(P(x) \leftrightarrow \neg P(\mathtt{S}(x))\ \big].$

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

ψ: $\exists P\big[\ \exists x P(x)\ \wedge\ P \subseteq \mathtt{a} \wedge \forall y\big(\ (\forall x[P(x) \rightarrow x < y])\ \rightarrow \mathtt{b}(y)\big)\ \big].$

- $aacbaccaabbb \models \varphi$, but $aacbaccaabbc \not\models \varphi$.
- $W \models \varphi$ iff W has a non-empty subset of a-positions after which there are only b-positions.

ψ': $\exists x\big[\ \mathtt{a}(x)\ \wedge\ \forall y[x < y \rightarrow (\neg\mathtt{a}(y) \wedge \mathtt{b}(y))]\ \big].$

- "There is a last a-position, with only b-positions after that."

Logic on words: examples

φ: $\exists P[\ P(\mathtt{first}) \wedge \neg P(\mathtt{last}) \wedge \forall x(P(x) \leftrightarrow \neg P(\mathtt{S}(x))\ ]$.

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

ψ: $\exists P[\ \exists x P(x)\ \wedge\ P \subseteq \mathtt{a} \wedge \forall y(\ (\forall x[P(x) \rightarrow x < y])\ \rightarrow \mathtt{b}(y))\ ]$.

- $aacbaccaabbb \models \varphi$, but $aacbaccaabbc \not\models \varphi$.
- $W \models \varphi$ iff W has a non-empty subset of a-positions after which there are only b-positions.

ψ': $\exists x[\ \mathtt{a}(x)\ \wedge\ \forall y[x < y \rightarrow (\neg\mathtt{a}(y) \wedge \mathtt{b}(y))]\ ]$.

- "There is a last a-position, with only b-positions after that."

ψ and ψ' are equivalent, and ψ' is first order.

Logic on words: examples

φ: $\exists P\big[\ P(\mathtt{first}) \wedge \neg P(\mathtt{last}) \wedge \forall x (P(x) \leftrightarrow \neg P(\mathtt{S}(x))\ \big]$.

- $aaaa \models \varphi$, but $aaaaa \not\models \varphi$.
- $W \models \varphi$ iff W has even length.

ψ: $\exists P\big[\ \exists x P(x)\ \wedge\ P \subseteq \mathtt{a} \wedge \forall y\big(\ (\forall x[P(x) \rightarrow x < y])\ \rightarrow \mathtt{b}(y))\ \big]$.

- $aacbaccaabbb \models \varphi$, but $aacbaccaabbc \not\models \varphi$.
- $W \models \varphi$ iff W has a non-empty subset of a-positions after which there are only b-positions.

ψ': $\exists x\big[\ \mathtt{a}(x)\ \wedge\ \forall y[x < y \rightarrow (\neg\mathtt{a}(y) \wedge \mathtt{b}(y))]\ \big]$.

- "There is a last a-position, with only b-positions after that."

ψ and ψ' are equivalent, and ψ' is first order.

Question. Does such an equivalent first order formula exist for φ?

Regular languages

Regular languages are subsets $L \subseteq \Sigma^*$ which are ...

- recognizable by a finite automaton;
- invariant under a finite index monoid congruence;
- definable by a monadic second order sentence.

Myhill-Nerode 1958; Büchi 1960

Overview

Duality

Key insight. The connection between MSO logic on words and monoids is an instance of Stone-Jónsson-Tarski duality.

Algebra	**Space**
Lindenbaum algebra of a logic	Canonical model
Residuated Boolean algebra of regular languages	(Pro)finite monoid

Gehrke, Grigorieff, Pin 2008

Duality

Key insight. The connection between MSO logic on words and monoids is an instance of Stone-Jónsson-Tarski duality.

Algebra	Space
Lindenbaum algebra of a logic	Canonical model
Residuated Boolean algebra of regular languages	(Pro)finite monoid
Equations between languages	Equations between words

Gehrke, Grigorieff, Pin 2008

Profinite monoids and their clopens

- A profinite monoid is a monoid equipped with a Boolean topology in which multiplication is continuous.
- Also: a limit of finite monoids with the discrete topology.

Profinite monoids and their clopens

- A profinite monoid is a monoid equipped with a Boolean topology in which multiplication is continuous.
- Also: a limit of finite monoids with the discrete topology.

- A subset of a profinite monoid is clopen iff it is recognizable, i.e., invariant under a finite index *topological* congruence.

Duality and profinite monoids

- There are natural division operators on the Boolean algebra of clopen sets of a profinite monoid:

$$K \backslash L = \{m \mid mK \subseteq L\}, \quad L/K = \{m \mid Km \subseteq L\}.$$

- These 'multiplicative operators' are dual to the monoid's multiplication,

  more precisely, to two distinct ternary relations derived from it.

Duality and profinite monoids

- There are natural division operators on the Boolean algebra of clopen sets of a profinite monoid:

$$K \backslash L = \{m \mid mK \subseteq L\}, \quad L/K = \{m \mid Km \subseteq L\}.$$

- These 'multiplicative operators' are dual to the monoid's multiplication,

  more precisely, to two distinct ternary relations derived from it.

Under this duality...

- the free profinite monoid is dual to the residuated Boolean algebra of all regular languages;
- quotients of the free profinite monoid correspond to subalgebras of regular languages that are ideals for division.

Duality

Key insight. The connection between MSO logic on words and monoids is an instance of Stone-Jónsson-Tarski duality.

Algebra	**Space**
Lindenbaum algebra of a logic	Canonical model
Residuated Boolean algebra of regular languages	(Pro)finite monoid
Equations between languages	Equations between words

Gehrke, Grigorieff, Pin 2008

Overview

Logic on words

Duality

Equations between words

Equations between languages

Logic and monoids

A language $L \subseteq \Sigma^*$ is MSO-definable

if, and only if,

L is invariant under a finite index monoid congruence.

Logic and monoids

A language $L \subseteq \Sigma^*$ is FO-definable

if, and only if,

L is invariant under a finite index aperiodic monoid congruence.

Logic and monoids

A language $L \subseteq \Sigma^*$ is FO-definable

if, and only if,

L is invariant under a finite index aperiodic monoid congruence.

A congruence θ on Σ^* is called aperiodic if Σ^*/θ does not have non-trivial subgroups.

Schützenberger 1965; McNaughton, Papert 1971

ω

In a finite monoid, any element x has a unique idempotent, x^ω, in its orbit $\{x, x^2, x^3, \ldots\}$.

Fact. A finite monoid is aperiodic iff it validates the equation

$$x^\omega = x^\omega x.$$

ω

In a profinite monoid, any element x has a unique idempotent, x^ω, in its orbit-closure $\overline{\{x, x^2, x^3, \dots\}}$.

Fact. A profinite monoid is aperiodic iff it validates the equation

$$x^\omega = x^\omega x.$$

ω

In a profinite monoid, any element x has a unique idempotent, x^ω, in its orbit-closure $\overline{\{x, x^2, x^3, \dots\}}$.

Fact. A profinite monoid is aperiodic iff it validates the equation

$$x^\omega = x^\omega x.$$

The quotient of the free profinite monoid obtained by enforcing $x^\omega = x^\omega x$ is the free pro-aperiodic monoid.
This is the dual space of the residuated algebra of FO-definable languages (instance of Eilenberg-Reiterman).

Logic on words: example revisited

$\varphi\colon \exists P\big[\ P(\mathtt{first}) \wedge \neg P(\mathtt{last}) \wedge \forall x(P(x) \leftrightarrow \neg P(\mathtt{S}(x))\ \big].$

- $L_\varphi = \{w\colon w \text{ has even length}\}.$

Question. Does an equivalent first order formula exist for φ?

Logic on words: example revisited

$\varphi\colon \exists P\big[\, P(\texttt{first}) \wedge \neg P(\texttt{last}) \wedge \forall x(P(x) \leftrightarrow \neg P(\texttt{S}(x))\,\big].$

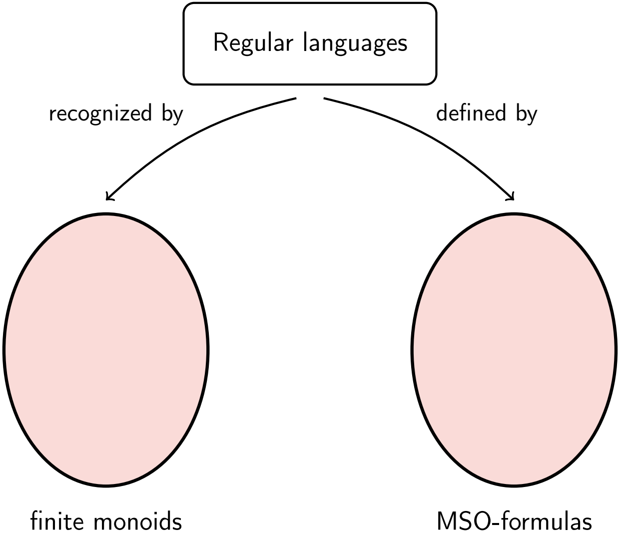
- $L_\varphi = \{w : w \text{ has even length}\}$.

Question. Does an equivalent first order formula exist for φ?

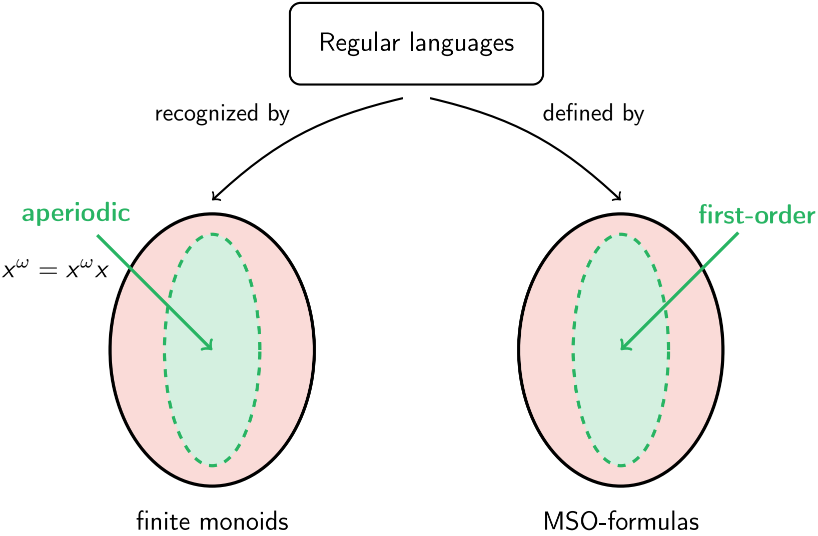
No, because:

- any quotient under which L_φ is invariant must contain a subgroup $\mathbb{Z}_2$; or:
- for any generator a of the free profinite monoid, we have $a^\omega \in \widehat{L_\varphi}$ and $a^\omega a \notin \widehat{L_\varphi}$, so L_φ 'falsifies' the equation $x^\omega = x^\omega x$.

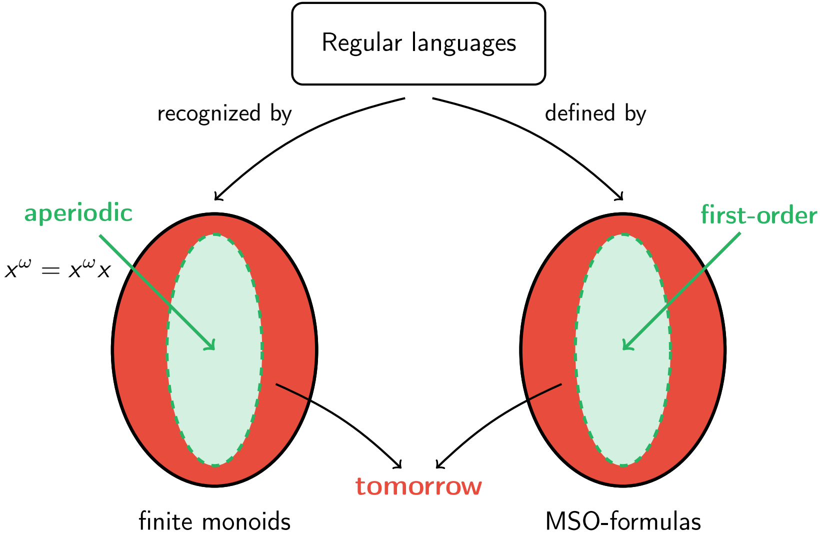
Monoids and logic



Monoids and logic



Monoids and logic



The free profinite aperiodic monoid

Theorem.

The free profinite aperiodic monoid

$=$

The topological monoid of ultrafilters of FO-definable languages

$=$

The topological monoid of $\equiv_{FO}$-classes of pseudo-finite words.

G. & Steinberg STACS 2017

Pseudo-finite words

- By a pseudo-finite word we mean a first-order structure $(W, <, (a^W)_{a \in \Sigma})$ that is a model of the theory of finite words.
- A pseudo-finite word is a discrete linear order with endpoints which is partitioned by the sets a^W

Pseudo-finite words

- By a pseudo-finite word we mean a first-order structure $(W, <, (a^W)_{a \in \Sigma})$ that is a model of the theory of finite words.
- A pseudo-finite word is a discrete linear order with endpoints which is partitioned by the sets a^W

- For example:
  - any finite word is pseudo-finite;
  - the word $a^{\mathbb{N}} + a^{\mathbb{N}^{\mathrm{op}}} = aaaa \ldots \ldots aaaa$ is pseudo-finite.

Pseudo-finite words

- By a pseudo-finite word we mean a first-order structure $(W, <, (a^W)_{a \in \Sigma})$ that is a model of the theory of finite words.
- A pseudo-finite word is a discrete linear order with endpoints which is partitioned by the sets a^W
- For example:
  - any finite word is pseudo-finite;
  - the word $a^{\mathbb{N}} + a^{\mathbb{N}^{\mathrm{op}}} = aaaa \ldots\ldots aaaa$ is pseudo-finite.
  - the word $a^{\mathbb{N}} + b^{\mathbb{N}^{\mathrm{op}}} = aaaa \ldots\ldots bbbb$

Pseudo-finite words

- By a pseudo-finite word we mean a first-order structure $(W, <, (a^W)_{a \in \Sigma})$ that is a model of the theory of finite words.
- A pseudo-finite word is a discrete linear order with endpoints which is partitioned by the sets a^W
- For example:
  - any finite word is pseudo-finite;
  - the word $a^{\mathbb{N}} + a^{\mathbb{N}^{\mathrm{op}}} = aaaa \ldots\ldots aaaa$ is pseudo-finite.
  - the word $a^{\mathbb{N}} + b^{\mathbb{N}^{\mathrm{op}}} = aaaa \ldots\ldots bbbb$ is **not**!

Pseudo-finite words

- By a pseudo-finite word we mean a first-order structure $(W, <, (a^W)_{a \in \Sigma})$ that is a model of the theory of finite words.
- A pseudo-finite word is a discrete linear order with endpoints which is partitioned by the sets a^W
- For example:
  - any finite word is pseudo-finite;
  - the word $a^{\mathbb{N}} + a^{\mathbb{N}^{\mathrm{op}}} = aaaa\ldots\ldots aaaa$ is pseudo-finite.
  - the word $a^{\mathbb{N}} + b^{\mathbb{N}^{\mathrm{op}}} = aaaa\ldots\ldots bbbb$ is **not**!
- The first-order sentence

$$\exists x \mathsf{a}(x) \to (\exists x_0 \mathsf{a}(x_0) \wedge \forall y > x_0 \neg \mathsf{a}(y))$$

is true in every finite word, but not in $a^{\mathbb{N}} + b^{\mathbb{N}^{\mathrm{op}}}$.

Pseudo-finite words

- By a pseudo-finite word we mean a first-order structure $(W, <, (a^W)_{a \in \Sigma})$ that is a model of the theory of finite words.
- A pseudo-finite word is a discrete linear order with endpoints which is partitioned by the sets a^W and every occurring first-order property has a last occurrence.
- For example:
  - any finite word is pseudo-finite;
  - the word $a^{\mathbb{N}} + a^{\mathbb{N}^{\mathrm{op}}} = aaaa\ldots\ldots aaaa$ is pseudo-finite.
  - the word $a^{\mathbb{N}} + b^{\mathbb{N}^{\mathrm{op}}} = aaaa\ldots\ldots bbbb$ is **not**!
- The first-order sentence

$$\exists x \mathrm{a}(x) \rightarrow (\exists x_0 \mathrm{a}(x_0) \wedge \forall y > x_0 \neg \mathrm{a}(y))$$

is true in every finite word, but not in $a^{\mathbb{N}} + b^{\mathbb{N}^{\mathrm{op}}}$.

Ultrafilters and pseudo-finite words

- An ultrafilter $\mathcal{U}$ of FO-definable languages uniquely determines an $\equiv_{FO}$-class $[W]$ of pseudo-finite words.
- This is a homeomorphism between the ultrafilter space and the space of types.
- There is a natural topological monoid multiplication on types:

$$\text{if } W \equiv W' \text{ then } VW \equiv VW' \text{ and } WV \equiv W'V.$$

The free profinite aperiodic monoid

Theorem.

The free profinite aperiodic monoid

=

The topological monoid of ultrafilters of FO-definable languages

=

The topological monoid of $\equiv_{FO}$-classes of pseudo-finite words.

G. & Steinberg STACS 2017

An application: the aperiodic ω-word problem

Decision problem. Given two terms in $\cdot$ and $()^\omega$, are they equal in every finite aperiodic monoid?

An application: the aperiodic ω-word problem

Decision problem. Given two terms in $\cdot$ and $()^\omega$, are they equal in the free profinite aperiodic monoid?

Realizing ω-words as ω-saturated models

- A countable model is ω-saturated if it realizes all the complete types over a finite parameter set.
- The following pseudo-finite words are ω-saturated:
  - finite words;
  - the constant word on $\mathbb{N} + \mathbb{Q} \times \mathbb{Z} + \mathbb{N}^{\mathrm{op}}$.

Realizing ω-words as ω-saturated models

- A countable model is ω-saturated if it realizes all the complete types over a finite parameter set.
- The following pseudo-finite words are ω-saturated:
  - finite words;
  - the constant word on $\mathbb{N} + \mathbb{Q} \times \mathbb{Z} + \mathbb{N}^{\mathrm{op}}$.
- Crucially, substitutions of ω-saturated words into ω-saturated words are again ω-saturated.
- Thus, any ω-term can be realized as an ω-saturated word.
- Using the uniqueness of countable ω-saturated models, equality of ω-terms reduces to isomorphism of these words, which we know is decidable.

Hüschenbett & Kufleitner STACS 2013;

G. & Steinberg STACS 2017

Overview

Solving equations

- Solve for $x \in \mathbb{R}$: $x^2 + 1 = 0$.

Solving equations

- Solve for $x \in \mathbb{C}$: $x^2 + 1 = 0$.

Solving equations

- Solve for $x \in \mathbb{C}$: $x^2 + 1 = 0$.
- A field F is existentially closed if any existential sentence that becomes true in some field extension of F already holds in F.

Solving equations

- Solve for $x \in \mathbb{C}$: $x^2 + 1 = 0$.
- A field F is existentially closed if any existential sentence that becomes true in some field extension of F already holds in F.
- This is first order definable: F is existentially closed iff

  for every non-constant polynomial p, $F \models \exists \overline{x} p(\overline{x}) = 0$.

Solving equations

- Solve for $x \in \mathbb{C}$: $x^2 + 1 = 0$.
- A field F is existentially closed if any existential sentence that becomes true in some field extension of F already holds in F.
- This is first order definable: F is existentially closed iff

  for every non-constant polynomial p, $F \models \exists \overline{x} p(\overline{x}) = 0$.
- A T-structure A is existentially closed* if any existential sentence that becomes true in some T-structure extending A already holds in A.

* If the class of T-structures does not have amalgamation, a more complicated definition is needed.

Solving equations

- Solve for $x \in \mathbb{C}$: $x^2 + 1 = 0$.
- A field F is existentially closed if any existential sentence that becomes true in some field extension of F already holds in F.
- This is first order definable: F is existentially closed iff

  for every non-constant polynomial p, $F \models \exists \overline{x} p(\overline{x}) = 0$.
- A T-structure A is existentially closed* if any existential sentence that becomes true in some T-structure extending A already holds in A.
- This property is often first order definable:
  - Linear orders without endpoints: density;
  - Boolean algebras: atomless;
  - Heyting algebras: mimick fields, use uniform interpolation.

* If the class of T-structures does not have amalgamation, a more complicated definition is needed.

Model companion

A first order theory T^* which captures the existentially closed models for a universal theory T is called a model companion of T.

Theorem.
The theory T^*, if it exists, is the unique theory such that:

1. T and T^* believe the same universal sentences;

2. T^* believes any sentence to be equivalent to an existential sentence.

Robinson, 1963

Model companion

A first order theory T^* which captures the existentially closed models for a universal theory T is called a model companion of T.

Theorem.
The theory T^*, if it exists, is the unique theory such that:

1. T and T^* believe the same universal sentences;

   T and T^* are co-theories

2. T^* believes any sentence to be equivalent to an existential sentence.

   T^* is model complete

Robinson, 1963

Model companions and languages

Theorem.

The first order theory T^* of an algebra for word languages, $\mathcal{P}(\omega)$,

is the model companion of

a theory T of algebras for a linear temporal logic.

Ghilardi & G. JSL 2017

Proof idea: set-up

Skip

- Enrich the Boolean algebra $\mathcal{P}(\omega)$ with temporal operators:
  - $\mathbf{X}a := \{t \in \omega \mid t+1 \in a\}$,
  - $\mathbf{F}a := \{t \in \omega \mid \exists t' \geq t \colon t' \in a\}$,
  - $\mathbf{I} := \{0\}$.

Proof idea: set-up

Skip

- Enrich the Boolean algebra $\mathcal{P}(\omega)$ with temporal operators:
  - $\mathbf{X}a := \{t \in \omega \mid t + 1 \in a\}$,
  - $\mathbf{F}a := \{t \in \omega \mid \exists t' \geq t \colon t' \in a\}$,
  - $\mathbf{I} := \{0\}$.

- Axioms for temporal logic $\to$ a first order theory T.

Proof idea: set-up

Skip

- Enrich the Boolean algebra $\mathcal{P}(\omega)$ with temporal operators:
  - $\mathbf{X}a := \{t \in \omega \mid t+1 \in a\}$,
  - $\mathbf{F}a := \{t \in \omega \mid \exists t' \geq t \colon t' \in a\}$,
  - $\mathbf{I} := \{0\}$.

- Axioms for temporal logic $\rightarrow$ a first order theory T.

Theorem. The theory T^* of $\mathcal{P}(\omega)$ is the model companion of T.

i.e., T^* is model complete and T^* is a co-theory of T.

Proof idea: co-theories

- Need to show: any equation of the form $t(\overline{p}) = \top$ that is valid in $\mathcal{P}(\omega)$ is valid in all T-structures.
- The theory T axiomatizes linear temporal logic on $\mathbf{X}$, $\mathbf{F}$, $\mathbf{I}$:
  - Boolean algebra axioms, $\mathbf{X}$ is a homomorphism, $\mathbf{F}a$ is the least fix point of the function $x \mapsto a \vee \mathbf{X}x$.
  - $\mathbf{I}$ is an atom and $\mathbf{I} \leq \mathbf{F}a$ whenever $a \neq \bot$.

Proof idea: co-theories

- Need to show: any equation of the form $t(\overline{p}) = \top$ that is valid in $\mathcal{P}(\omega)$ is valid in all T-structures.
- The theory T axiomatizes linear temporal logic on **X**, **F**, **I**:
  - Boolean algebra axioms, **X** is a homomorphism, **F**a is the least fix point of the function $x \mapsto a \vee \mathbf{X}x$.
  - **I** is an atom and $\mathbf{I} \leq \mathbf{F}a$ whenever $a \neq \bot$.
- If $t(\overline{p}) \neq \top$ in some T-structure A, consider its dual space X.
- By carefully using filtration-type techniques, we may read off from X a valuation $\overline{p} \to \mathcal{P}(\omega)$ which invalidates $t(\overline{p}) = \top$.

Proof idea: co-theories

- Need to show: any equation of the form $t(\overline{p}) = \top$ that is valid in $\mathcal{P}(\omega)$ is valid in all T-structures.
- The theory T axiomatizes linear temporal logic on **X**, **F**, **I**:
  - Boolean algebra axioms, **X** is a homomorphism, $\mathbf{F}a$ is the least fix point of the function $x \mapsto a \vee \mathbf{X}x$.
  - **I** is an atom and $\mathbf{I} \leq \mathbf{F}a$ whenever $a \neq \bot$.
- If $t(\overline{p}) \neq \top$ in some T-structure A, consider its dual space X.
- By carefully using filtration-type techniques, we may read off from X a valuation $\overline{p} \to \mathcal{P}(\omega)$ which invalidates $t(\overline{p}) = \top$.

Proof idea: model completeness

- Any first order formula $\varphi(\overline{p})$ in the temporal algebra $\mathcal{P}(\omega)$ translates to an MSO formula $\Phi(\overline{P})$ in logic on words.

Proof idea: model completeness

- Any first order formula $\varphi(\overline{p})$ in the temporal algebra $\mathcal{P}(\omega)$ translates to an MSO formula $\Phi(\overline{P})$ in logic on words.
- This MSO formula Φ defines a regular language L_Φ.

Proof idea: model completeness

- Any first order formula $\varphi(\overline{p})$ in the temporal algebra $\mathcal{P}(\omega)$ translates to an MSO formula $\Phi(\overline{P})$ in logic on words.
- This MSO formula Φ defines a regular language L_Φ.
- Build an automaton A for Φ.

Proof idea: model completeness

- Any first order formula $\varphi(\overline{p})$ in the temporal algebra $\mathcal{P}(\omega)$ translates to an MSO formula $\Phi(\overline{P})$ in logic on words.
- This MSO formula Φ defines a regular language L_{Φ}.
- Build an automaton A for Φ.
- Describe the automaton A with an existential first order formula φ' in the temporal algebra $\mathcal{P}(\omega)$.

Proof idea: model completeness

- Any first order formula $\varphi(\overline{p})$ in the temporal algebra $\mathcal{P}(\omega)$ translates to an MSO formula $\Phi(\overline{P})$ in logic on words.
- This MSO formula Φ defines a regular language L_{Φ}.
- Build an automaton A for Φ.
- Describe the automaton A with an existential first order formula φ' in the temporal algebra $\mathcal{P}(\omega)$.
- **Conclusion.** $\mathcal{P}(\omega)$ believes that any first order formula φ is equivalent to an existential formula φ'.

Model companions and languages

Theorem.

The first order theory T^* of an algebra for word languages, $\mathcal{P}(\omega)$,

is the model companion of

a theory T of algebras for a linear temporal logic.

Ghilardi & G. JSL 2017

Model companions and languages

Theorem.

The first order theory T^* of an algebra for tree languages, $\mathcal{P}(2^*)$,

is the model companion of

a theory T of algebras for a fair computation tree logic.

Ghilardi & G. LICS 2016

The future

- From FO to MSO
- Model companions for more logics
- Using ordered spaces