Some recent advances in the monadic second-order theory of countable linear orderings

Thomas Colcombet

LLAMA Seminar, Mars 16 2022

Based on joint work with
Olivier Carton, Rémi Morvan, Sam van Gool,
Gabriele Puppis, Alexander Rabinovich, and Sreejith A. V.

Summary

- Part I: Monadic second-order logic over linear orderings/chains/words
- Part II: Algebras for countable words
- Part III: Answering questions

Part I
Monadic second-order logic and linear orderings

In which we present the objects we care about,
and start to ask questions about them.

Monadic Second-Order logic (MSO)
on linear orderings

First-order logic **(*FO*)** We consider *relational structures* (with no functional symbols).
First-order logic's syntax:

$$\begin{aligned} \Psi := &\quad \mathbf{T} \quad | \quad \mathbf{F} \\ | &\quad \Psi \wedge \Psi \\ | &\quad \Psi \vee \Psi \\ | &\quad \neg\Psi \\ | &\quad \exists x.\Psi \quad | \quad \forall x.\Psi \\ | &\quad R(x_1, \dots, x_k)\ . \end{aligned}$$

with the expected semantics.

Monadic second-order logic **(*MSO*)** extends FO Syntax:

$$\begin{aligned} \Psi := &\quad \text{FO syntax} \\ | &\quad \exists X.\Psi \quad | \quad \forall X.\Psi \\ | &\quad x \in X\ . \end{aligned}$$

Variables $X, Y, \dots$ are called *monadic* or *set variables*, and are interpreted over the powerset of the structure.

Example. On directed graphs, $\mathrm{Reach}(x, y)$ expresses the existence of a path from x to y.

$R(\_,\_)$

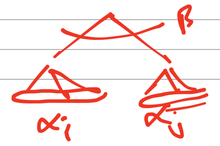
$\mathrm{Reach}(x_0, y_0)$: $\forall X. [(\forall x.\forall y.(x \in X \wedge R(x,y) \to y \in X)) \wedge x_0 \in X] \to y_0 \in X$

Linear order(ing)s

A *linear order* is a total order
(structure over signature = "$<$").
We are interested in countable linear orders.
We implicitly consider linear orders modulo isomorphisms (monotonic bijections)

—

Example.
- Finite linear orders.
- $\omega = (\mathbb{N}, <)$.
- $\omega^* = (\mathbb{N}, >)$.
- $\zeta = (\mathbb{Z}, <)$ — $\zeta = \omega^* + \omega$
- $\eta = (\mathbb{Q}, <)$ (rational line)
- sums of linear orders indexed by a linear order, as $\sum_{i \in \eta} \zeta$



$\sum_{i \in \beta} \alpha_i$

- etc...

—⁕—

Some notions over linear orders, and their logical expression

- Being empty/non-empty.

  $\forall x . \bot$

- Being *dense*:

  $\forall x . \forall y \ (x < y) \to \exists z . x < z < y .$

  $\wedge \ \exists x_1 \exists x_2 \ x_1 \neq x_2$

- Having a minimal/maximal element.

- Being isomorphic to $(\mathbb{Q}, <)$.

  $\alpha \approx (\mathbb{Q}, <)$ iff.
  0. α is countable
  1. α is dense
  2. α has no minimal elt
  3. ___ max .

- Being infinite.

  $\exists X . (X \neq \emptyset . \forall y \in X . \exists z \in X . z > y)$

- Being finite.

- Being well founded (ie isomorphic to an ordinal).

  $\forall X . X \neq \emptyset \to X$ ___

- A *(Dedekind) cut* is a downward closed subset.

  $\mathrm{Cut}(X) . \ \forall x \in X . \forall y < x . \ y \in X$

(Cuts + elements can be totally ordered

- A *gap* is a 'hole' in the linear ordering: a cut which it not minimal nor maximal, has no predecessor, and no successor.

  $\mathrm{Cut}(X) \wedge X$ has no max

  $\mathbb{Q} \wedge \bar{X}$ ___ min

- Being Dedekind complete.

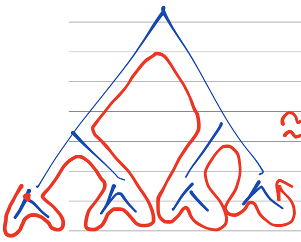
  No gap.

- Being *scattered* is being nowhere dense (no subset is dense).

  $\forall X . \neg \mathrm{dense}(X)$

  $\sum_{\mathbb{Q}} \mathbb{Z}$) not scattered.

Theorem(Rabin69) The MSO-theory of the rational line is decidable.



Theorem(Shelah75) The MSO-theory of the real line is undecidable.

$(\mathbb{R}, <)$

Chain and words

A *chain* is a linear order together with unary predicates.

A *word* is a chain such that all element belong to exactly one of the unary predicates (called letters). A word is *countable* if its universe (set of positions) is countable.

We set

$$A^{\mathrm{cw}} := \{\text{countable words over } A\}$$

Of course finite words coincide with words in the usual sense.

Construction for words
Given word u, v, uv is their concatenation.
One can perform products indexed by linear orderings:

$$\prod_{i\in\alpha} u_i := \dots$$

Exponentiation is a special case:

$$u^\alpha := \prod_{i\in\alpha} u\,.$$

Definition For X a (finite) set of letter,

$$\mathrm{shuffle}(X)$$

denotes a word over the alphabet X such that:

- It is countable.
- It has at least two elements.
- It has no minimal nor maximal element.
- All letters in X appear densely:

$$\bigwedge_{a\in X} \forall x\forall y\ \left(x<y\rightarrow \exists z.x<z<y\wedge a(z)\right).$$

Lemma Up to isomorphism shuffle(X) is uniquely defined.

Since:

- all countable linear orders are suborders of $(\mathbb{Q})$, and
- MSO can quantify over unary predicates,

we obtain:

Corollary of [Rabin69] The MSO-theory of countable linear orders/countable chains/countable words is decidable.

Plenty of “natural” questions

Do we need all quantifiers ?

Eg. MSO is known to collapse to one existential monadic quantifier over finite words.

Does the same thing occur over countable linear orders?

What is the expressiveness of MSO with cuts in the background?

Does it help when expressing a property over the rationals to use all cut in the logic?

What is the status of FO inside MSO?

Is FO equivalent to MSO?

If not, can we decide if a formula of MSO is equivalent to a formula of FO over countable words?

Are there other natural logics between FO and MSO?

Same questions...

And what about separation?

Can we decide if two MSO formulae can be separated by an FO one? Other logics?

Uniformization?

If there is a solution to $\Psi(X)$, is it possible to define uniquely such an X?

Recap of part I

We have seen:

- First-order and monadic second-order logics,
- Linear orders, chains and words, and many examples.
- In particular the word shuffle(X).
- The seminal results of Rabin (decidability of MSO over $(\mathbb{Q}, <)$) and Shelah (undecidability over $(\mathbb{R}, <)$).
- We also asked ourselves many questions on the expressiveness of FO and MSO over countable words.

II
Algebras for countable words

Where we present another, algebraic, way to describe sets of countable words, and see how to handle algorithmically these description.

Monoids for countable words

Note for languages of finite words that:

MSO-definable = recognizable by finite monoids

and,

monoid = algebra for the word monad

We want to extend this approach to countable words.

Definition 1: A *countable words monoids* (*cw monoid* for short) consists of a set

$$M$$

and a (family of) operation(s), called *product*,

$$\pi \colon M^{\mathrm{cw}} \longrightarrow M \ ,$$

that satisfy suitable generalized associativity identities.

Definition 2 [Bojanczyck15]: A cw monoid is an (Eilenberg-Moore) algebra for the monad:

$$T \colon \mathsf{Set} \longrightarrow \mathsf{Set}$$
$$M \longmapsto M^{\mathrm{cw}}$$

with a multiplication $\mu_M \colon [M^{\mathrm{cw}}]^{\mathrm{cw}} \to M^{\mathrm{cw}}$, and unit $\eta_M \colon M \to M^{\mathrm{cw}}$.

Example $M = \{1, a, 0\}$ with

$$\pi(u) = \begin{cases} 1 & \text{if } u_i = 1 \text{ for all } i \in \mathrm{dom}(u), \\ 0 & \text{if } u_i = 0 \text{ for some } i, \text{ or } u_i = a \text{ for infinitely many } i\text{'s, or} \\ a & \text{ortherwise.} \end{cases}$$

Definition: A language $L \subseteq A^{\mathrm{cw}}$ is *recognizable* if there is a cw monoid morphism $\rho \colon A^{\mathrm{cw}} \to M$ with M a finite cw monoid and $F \subseteq M$ such that:

$$u \in L \qquad \text{if and only if} \qquad \rho(u) \in F \ .$$

Example The language of words with finitely many a's is recognizable.

Finite presentations for cw monoids

Two operations are sufficient for describing a monoid:

$$1 := \pi(\varepsilon), \quad \text{and} \quad a \cdot b := \pi(ab)\ .$$

we search for sufficient operations for describing a cw monoid.

Given a cw monoid (M, π), we define its *derived operations*:

$$1 = \pi(\varepsilon), \qquad a \cdot b = \pi(ab)$$

$$a^\omega = \pi(\overbrace{aaa\ldots}^{\omega \text{ times}}) \qquad a^{\omega*} = \pi(\overbrace{\ldots aaa}^{\omega* \text{ times}})$$

$$\text{and} \quad X^\eta = \pi(\text{shuffle}(X))$$

Example $M = \{1, a, 0\}$ with

$$\pi(u) = \begin{cases} 1 & \text{if } u_i = 1 \text{ for all } i \in \text{dom}(u), \\ 0 & \text{if } u_i = 0 \text{ for some } i, \text{ or } u_i = a \text{ for infinitely many } i\text{'s, or} \\ a & \text{ortherwise.} \end{cases}$$

	1	a	0	ω	$\omega*$	η
1	1	a	0	1	1	1
a	a	a	0	0	0	0
0	0	0	0	0	0	0

Furthermore the derived operations $1, \cdot, ^\omega, ^{\omega*}, ^\eta$ satisfy identities I:

$(a^n)^\omega = a^\omega$

$(ab)^\omega = a(ba)^\omega$

$a^n \cdot a^n = a^n$

Theorem[Carton&C.&Puppis11] Given a finite set M and operations $1, \cdot, ^\omega, ^{\omega*}, ^\eta$ satisfying the identities I, there exists one and exactly one

$$\pi\colon M^{\text{cw}} \to M\ ,$$

that makes (M, π) a cw monoid of derived operations $1, \cdot, ^\omega, ^{\omega*}, ^\eta$.

From now, it is the same to give derived operations or the product.

Examples of cw monoids

Example The countable words that are well founded.

1 empty

a well founded word

0

	1	a	0	ω	ω*	η
1	1	a	0	1	1	1
a	a	a	0	a	0	0
0	0	0	0	0	0	0

Example The countable words that are Dedekind complete (have no gaps).

Example The countable words that have a domain isomorphic to the $(\mathbb{Q}, <)$.

Example The countable words that are scattered.

The composition method of Shelah

Definition: Call the *k-type* $\text{type}_k(u)$ of a word $u \in A^{cw}$ the set of formulae of MSO of quantifier rank at most k that it satisfies.
Types_k is the set of k-types.

Lemma The set of k-types is finite.
(Similar to Feferman-Vaught)

Lemma[implicitly in Shelah75] The set of k-types can be equipped of a product π turning (Types_k, π) into a cw monoid, and:

$$\text{type}_k : A^{cw} \longrightarrow \text{Types}_k$$

into a cw monoid morphism.

Corollary All MSO-definable languages of countable words are recognizable (even effectively).

Theorem[Carton&C.&Puppis11] A language of countable words is MSO-definable if and only if it is recognizable. And this is effective.

A (very small) idea about the proof.

Recap of part II

We have seen:

- Sets of countable words can be recognized by algebras extending monoids to the countable words.
- These cw monoids are, from the category perspective, algebras for the countable word monad.
- And being recognizable by finite cw monoids is equivalent to MSO-definable.
- Though with infinitely many operations, finite cw monoids can be finitely/algorithmically used using their finitely many finite-arity derived operations.

III
Answering questions

Where we can start to give answers...

Do we have a collapse of quantifiers?

EMSO is MSO restricted to formulae of the form:

$$\exists X_1 \ldots \exists X_k\ \Psi, \qquad \text{with } \Psi \text{ first-order.}$$

Let *UMSO* be its duall.

Folklore A language of finite words is MSO-definable if and only if it is EMSO-definable.

—⁂—

Recall that being scattered is expressed as:

For all sets X, the linear order induced by X is not dense.

This is a formula of UMSO.

Lemma Being scattered is not expressible in EMSO.

Recall:

Theorem[Carton&C.&Puppis11] A language of countable words is MSO-definable if and only if it is recognizable.

—

In fact, the proof provides more: MSO is effectively equivalent over countable words to its

$$\exists^{\text{sets}}\forall^{\text{sets}}\ \text{FO} \qquad \text{and} \qquad \forall^{\text{sets}}\exists^{\text{sets}}\ \text{FO}$$

fragments (one alternation of monadic quantifiers). But not less.

—

Can we use cuts in the background?

—⁕—

Question[Gurevitch&Rabinovich00] Given a formula $\Psi(X)$ of MSO, does there exists a formula $\Psi^*(X)$ of MSO such that for all $X \subseteq \mathbb{Q}$,

$$(\mathbb{R}, <) \models \Psi(X) \quad \text{if and only if} \quad (\mathbb{Q}, <) \models \Psi^*(X).$$

—

Or simply, ``is it equiexpressive to quantify over cuts for defining a property of a set of rationals?"

—

—⁕—

Theorem[C.13] Yes.

Proof The map which to all countable words u defines

$$\begin{aligned} \delta\colon A^{\mathrm{cw}} &\longrightarrow \mathrm{Types}_{\mathrm{k}} \\ u &\longmapsto \mathrm{type}_{\mathrm{k}}(\hat{u}), \end{aligned}$$

in which $\hat{u}$ is the completion of u in which a special letter $\circ$ is substituted to all gaps, is a cw monoid morphism.

—

The funny thing. The MSO-theory of $(\mathbb{R}, <)$ being undecidable, the theorem cannot be effective!

—⁕—

Comparing FO, MSO and others

Given a monoid M, it is *aperiodic* if for all $a \in M$,

$$a^{n+1} = a^n \qquad \text{for some } n.$$

In particular, the language ``the words of length i modulo k" are not recognizable by an aperiodic monoid.

It is classical in language theory:

Theorem[Schützenberger66] For a language of finite words, the following items are equivalent:

- being definable in first-order logic
- being recognizable by a finite aperiodic monoid
- having an aperiodic `syntactic' monoid
- ... and several other things ...

And this is effective.

Theorem[C.&Sreejith15] An MSO-definable language of countable words is definable in first-order logic if and only if it is recognized by a cw monoid satisfying ap, id→sc, sc→sh, sh→ss, and this is effective.

Where:

Ap is aperiodic.

Id→sc If $e = e \cdot e$ implies $e = e^{\omega} \cdot e^{\omega *}$.

Also called *gap insensitivity*.

Sc→sh If $e = e^{\omega} \cdot e^{\omega *}$ implies $e = e^{\eta}$.

Sh→ss If $e = e^{\eta} = e \cdot a \cdot e$ implies $e = \{e, a\}^{\eta}$.

(in real, for several a's simultaneously...)

and more... An MSO-definable language is definable in:

- WMSO=FO[finite] iff id→sc, sc→sh, sh→ss,
- FO[cut] iff ap, sc→sh, sh→ss,
- FO[finite,cut]=FO[ordinals] iff sc→sh, sh→ss,
- FO[scattered] iff sh→ss.

And these properties are decidable.

Separating languages

—⁂—

The problem: Fix a logic $\mathcal{L}$. Given two MSO-definable languages of countable words K, L, decide if there is a separating language S definable in $\mathcal{L}$.

S is *separating* if $K \subseteq S$, and $S \cap L = \emptyset$.

Remark Decidable $\mathcal{L}$-separation implies decidability of $\mathcal{L}$-characterization.

—

—⁂—

Theorem[C.&Movan&vanGool22] FO-separatbil is decidable over countable ordinal words.

—⁂—

We are currently studying the generalisations...

Uniformization

—⁎—

Definition. A formula $\Psi(X, \bar{Y})$ is *uniformizable* (in a given logic over some class of models) if there exists a formula (called the *uniformizer*) $\Psi^*(x, \bar{Y})$ such that for all models u and valuations $\bar{B}$, if

$$u \models \Psi(A, \bar{B})$$

for some set B, then

$$u \models \Psi(\{x \mid \Psi^*(x, \bar{B})\}, \bar{B}) .$$

—

Proposition[Shelah&Lifshes98] MSO is uniformizable in MSO over all words of domain at most ω^k (for some k).

Proposition[Shelah&Lifshes98] MSO is not uniformizable in MSO over ω^ω.

—

In particular the non uniformizable formula

$$\omega\text{−Cof}(X, Y)$$

expresses that X has order-type ω , and is cofinal in Y.

—⁎—

Theorem[C.&Rabinovich??] MSO is uniformizable in MSO+ω−CofU, in which ω−CofU(x, Y) new constructs that uniformizes ω−Cof(X, Y).

—

Theorem[C.&Rabinovich??] It is possible, given an MSO formula, to decide whether it that an MSO-definable uniformizer.

—⁎—

Conclusion

—

- MSO over countable linear orders/chains/words has a rich and well behaved theory.
- The algebraic approach, using suitable extensions of the notion of monoids exactly captures the expressiveness of MSO.
- This technology gives a common handle for solving many non trivial questions.

—

Thank you!