First-order logic with idempotent variables over free inverse monoids

Volker Diekert and Géraud Sénizergues

Stuttgart university, Bordeaux university

Tuesday March 8th 2016

INTRODUCTION

FO theory of a monoid

Structure :

$$\mathcal{M} := \langle M, \cdot, 1_M, a_M, b_M, \cdots, = \rangle$$

Formulas :
first-order formulas on the signature

$$(\cdot, 1, a, b, \cdots, =)$$

Decision problem :
Instance : a formula φ
Question : $\mathcal{M} \models \varphi$?

FO theory of a monoid

For the free monoid :

$$\langle \{a, b\}^*, \cdot, \varepsilon, a, b, =\rangle$$

the FO theory is undecidable.
For the free group :

$$\langle \mathrm{FG}(\{a, b\}), \cdot, \varepsilon, =\rangle$$

the FO theory is decidable.
[Kharlampovich-Myasnikov 2006]

Free inverse monoid

$\mathrm{FIM}(A) :=$ the Free Inverse Monoid over the finite set A.

$$(A \cup \bar{A})^* \twoheadrightarrow \mathrm{FIM}(A) \twoheadrightarrow \mathrm{FG}(A)$$

Main result

Theorem

Suppose $|A| \geq 6$. The FO-theory of $\mathrm{FIM}(A)$, with idempotent variables only, is undecidable or decidable.

contents

FREE inverse monoid

Inverse monoids

Let $(M, \cdot, 1)$ be a monoid, and let $u, u' \in M$.
u' is an inverse for u iff

$$u \cdot u' \cdot u = u \quad \wedge \quad u' \cdot u \cdot u' = u'$$

Inverse monoids

Let $(M, \cdot, 1)$ be a monoid, and let $e \in M$. The element e is idempotent iff

$$e \cdot e = e$$

Inverse monoids

Definition

A monoid $(M, \cdot, 1)$ is called an inverse monoid iff

$$\forall u \in M, \exists! u' \in M, \quad u \cdot u' \cdot u = u \quad \wedge \quad u' \cdot u \cdot u' = u'.$$

Fundamental example : monoid of partial injections from E to E.
Inverse of u : $u' = \{(x, y) \in E \times E \mid (y, x) \in u\}$
Idempotent : $e = \{(x, x) \mid x \in E'\}$ where $E' \subseteq E$.

free inverse monoids

Free inverse monoids exist : [Scheiblich 73,Munn 74 .]
The domain of $\mathrm{FIM}(A)$ is the set of pairs :

$$(T, g)$$

where
1- $g \in \mathrm{FG}(A)$ (the free group over A)
2- T is a subtree of the Cayley-graph of $\mathrm{FG}(A)$,
such that $g \in T$.
The operations are defined by :

$$(T, g) \times (U, h) = (T + g \cdot U, g \cdot h).$$

$$(T, g)' = (g^{-1} \cdot T, g^{-1})$$

free inverse monoids

Such pairs (T, g) are also called Munn trees, or bi-rooted trees.

Equations

Theorem (Rozenblat 1986)

The satisfiability problem for equations in the free inverse monoid is undecidable.

bad start for the FO theory.

Equations

BUT :

[Deis-Meakin-Sénizergues 2007] :
satisfiability is decidable for equations in the free inverse monoid with idempotent variables (reduction to [Rabin 71]).

[Diekert-Martin-S.-Silva CSR'15] :
the above problem is EXPTIME (reduction to [Baader-Narendran 91])

[D-M-S-S 2016] :
the above problem is EXPTIME-complete (red. from equations over finite sets, shown complete in [Baader-Narendran 91]).

Link with non-empty prefix-closed subsets of F(A)

$\mathrm{PC}_f(\mathrm{FG}(A)) :=$ The set of all non-empty p-closed subsets of $F(A)$.
Additive structure, with left-translations :

$$\langle \mathrm{PC}_f(\mathrm{FG}(A)), +, (S \mapsto aS + \varepsilon)_{a \in A \cup A^{-1}}, = \rangle$$

The FO theory of non-empty p-closed subsets of $\mathrm{FG}(A)$ reduces to the FO theory of $\mathrm{FIM}(A)$ with idempotent variables (and conversely).
method : given in [DS-D-M-S CSR'15].

First-order theories of TREES

Theories of trees

Trees :
Let F a graded alphabet. For $f \in F$:

$$\hat{f}(t_1, \ldots, f_k) := f(t_1, \ldots, f_k)$$

$$\langle T(F), (\hat{f})_{f \in F}, = \rangle$$

[Malcev <71] : FO of terms is decidable
[Comon 90] : FO of terms, with rational constraints, is decidable
[Comon 91],[Comon-Treinen 94], etc ... : many structures on trees have a decidable FO theory.

Theories of trees

Prefix-closed Sets :
$\mathrm{PC}_f(A^*)$: set of finite prefix-closed subsets of A^*.
Additive structure :

$$\langle \mathrm{PC}_f(A), +, = \rangle$$

[Rabin 71] : FO-theory of finite prefix-closed subsets of A^* is decidable

$$\langle \mathrm{PC}_f(\mathrm{FG}(A)), +, = \rangle$$

[Muller-Schupp 81] : FO-theory of finite prefix-closed subsets of $\mathrm{FG}(A)$ is decidable.

First-order theories of WORDS

Theories of words

The FO-theory of

$$\langle A^*, \cdot, = \rangle$$

for $|A| \geq 2$, is undecidable.
[folklore]
The FO-theory of

$$\langle A^*, \leq_f \rangle$$

for $|A| \geq 2$, where $\leq_f$ is the factor-ordering, is undecidable.
[(tiring) exercise]

FO theories of $\mathrm{FIM}(A)$

Decidable or undecidable ?

Positive hint : Munn-trees are trees

Negative hint : FO of words with factor ordering is undecidable. Prefix sets, combined with left-translations, might be enough to express the factor ordering.

Undecidable

FO of words with factor
reduces to
FO of non-empty, p-closed subsets of $\mathrm{FG}(A)$ (addition and left-translation)
reduces to
FO theory of $\mathrm{FIM}(A)$ with idempotent variables.

Finite sets of words

Starting alphabet A.
New alphabet $\Delta := A \cup \{q_0, q, \#, m\}$.
Equation E over finite subsets of Δ^* :

$$q \cdot X + \sum_{a \in A} q \cdot X_{q,a} + \sum_{a \in A} q_0 \cdot X_{q,a} = \sum_{\substack{a \in A \\ p \in \{q, q_0\}}} q \cdot \# \cdot a \cdot X_{p,a} + q_0 \cdot m$$

Finite sets of words

Lemma (Baader-Narendran 91)

$(X, (X_{q,a})_{a\in A}, (X_{q_0,a})_{a\in A})$ is a solution of E iff
1- $X = Zm$ for some non-empty $Z \subseteq (\#A)^+$
2- $X_{q,a}$ = set of suffixes of Z, starting after letter a, followed by some $\#a'$ ($a' \in A$)
3- $X_{q_0,a}$ = set of suffixes of Z, starting after letter a, followed by m.

N.B.1 : Every minimal solution is of the form

$$X = \{u \cdot m\} \text{ where } u \in (\#A)^+$$

finite p-closed sets of words

The equation E' over non-empty finite p-closed subsets of Δ^* :

$$\varepsilon + q \cdot X + \sum_{a \in A} q \cdot X_{q,a} + \sum_{a \in A} q_0 \cdot X_{q_0,a} = \varepsilon + q + q \cdot \# + \sum_{\substack{a \in A \\ p \in \{q, q_0\}}} q \cdot \# \cdot a \cdot X_{p,a} + q_0 + q$$

Same kind of description of the minimal solutions.
N.B.2 : Every minimal solution fulfills

$$X = \mathrm{Pref}(u \cdot m) \text{ for some } u \in (\# A)^+$$

$$X + \sum_{a \in A} q \cdot X_{q,a} = \mathrm{Fact}(u \cdot m) \cap ((\# A)^* (\varepsilon + \# + m))$$

finite p-closed subsets of $F(\Delta)$

The equations E'' over non-empty finite p-closed subsets of $F(\Delta)$:

$$\varepsilon + \#^{-1} \cdot (X + \sum_{a \in A} X_{q,a}) = \varepsilon + \#^{-1} + \sum_{\substack{a \in A \\ p \in \{q, q_0\}}} a \cdot X_{p,a}$$

$$\sum_{a \in A} q_0 \cdot X_{q_0,a} = \varepsilon + m.$$

N.B.3 : minimal solutions are of the form :

$$X = \mathrm{Pref}(u \cdot m)$$

$$X + \sum_{a \in A} q \cdot X_{q,a} = \mathrm{Fact}(u \cdot m) \cap ((\#A)^*(\varepsilon + \# + m))$$

for some $u \in (\#A)^+$

FO-interpretation

The interpretation :
$\varphi : A^+ \hookrightarrow \mathrm{PC}_f(F(\Delta))$

$$u \mapsto \mathrm{Pref}(\#u[0]\#u[1]\cdots\#u[\ell-1]m)$$

FO formula asserting that $S \in \mathrm{Im}(\varphi)$:

$$\exists (X_{q,a})_{a\in A}, \exists (X_{q_0,a})_{a\in A}), E''(S,(X_{q,a})_{a\in A},(X_{q_0,a})_{a\in A}) \wedge Minimal(S).$$

FO-interpretation

FO formula asserting that $\varphi^{-1}(X)$ is a factor of $\varphi^{-1}(Y)$:

$$\exists (X_{q,a})_{a\in A}, \exists (X_{q_0,a})_{a\in A}), \exists (Y_{q,a})_{a\in A}, \exists (Y_{q_0,a})_{a\in A}), \exists X'$$
$$E''(X, (X_{q,a})_{a\in A}, (X_{q_0,a})_{a\in A}) \wedge E''(Y, (Y_{q,a})_{a\in A}, (Y_{q_0,a})_{a\in A})$$
$$\wedge X' \text{ is a maximal strict subset of } X$$
$$\wedge X' \subseteq Y + \sum_{a\in A} Y_{q,a}.$$

Main result

Theorem

Suppose $|A| \geq 6$. The FO-theory of $\mathrm{FIM}(A)$, with idempotent variables only, is undecidable.

Open questions

- FO of $\mathrm{FIM}(A)$ for $1 \leq |A| \leq 5$
- existential theory of $\mathrm{FIM}(A)$?
- other fragments of the FO theory of $\mathrm{FIM}(A)$?