A Semantic Approach to the Analysis of Rewriting-Based Systems

Salvador Lucas

DSIC, Universitat Politècnica de València, Spain

27^{th} International Symposium on Logic-Based Program Synthesis and Transformation, LOPSTR 2017

Is the following *true*?

$$(\forall x) \qquad x + 0 \geq x \tag{1}$$

Yes!... provided that the *standard* (arithmetic) interpretation $\mathcal{A}$ is assumed for all symbols: $\mathcal{A} \models (1)$.

Is the following *true*?

$$(\forall x) \qquad x + 0 \geq x \tag{1}$$

Yes!... provided that the *standard* (arithmetic) interpretation $\mathcal{A}$ is assumed for all symbols: $\mathcal{A} \models (1)$.

What about this?

$$(\forall x_1) \qquad A_1^2(f_1^2(x_1, a_1), x_1) \tag{2}$$

(1) and (2) are 'syntactically equivalent' under *renaming of symbols*.

Viewed as *first-order logic* (FOL) formulas, *non-logic* symbols occurring in (1) (e.g., '0', '+', and '$\geq$') have no special meaning!

Many interpretations of a_1, f_1^2 and A_1^2 in (2) do *not* satisfy (2), i.e.,

$$\not\models (2) \quad \text{and even} \quad \not\models (1)!$$

How to use FOL in the analysis of computational properties of rewriting-based systems?

For instance, *confluence* can be expressed as follows:

$$(\forall x, y, z)\ (x \to^* y \wedge x \to^* z \Rightarrow (\exists u)(y \to^* u \wedge z \to^* u)) \tag{3}$$

Given a Term Rewriting System $\mathcal{R}$, how do we say "*$\mathcal{R}$ is confluent*" using FOL?

1. $\overline{\mathcal{R}} \vdash (3)$, i.e., (3) can be *proved* from some theory $\overline{\mathcal{R}}$ associated to $\mathcal{R}$?
2. $\overline{\mathcal{R}} \models (3)$, i.e., *every* model of $\overline{\mathcal{R}}$ satisfies (3)?
3. $\mathcal{A}_{\mathcal{R}} \models (3)$, i.e., (3) is satisfied by some *special* interpretation $\mathcal{A}_{\mathcal{R}}$ associated to $\mathcal{R}$?

Dauchet and Tison's *first-order theory of rewriting* uses 3 with the *standard interpretation* $\mathcal{H}_{\mathcal{R}}$ where predicate symbols $\to$ and $\to^*$ are interpreted as the *one-step* and *many-step* rewrite relations on *ground terms* $\to_{\mathcal{R}}$ and $\to^*_{\mathcal{R}}$, respectively.

Problems

- In general, $\mathcal{H}_{\mathcal{R}}$ is not computable, and $\mathcal{H}_{\mathcal{R}} \models (3)$ is *undecidable*!
- Can we use *other* (*computable*!) interpretations? How?

Summary

1. Preservation of first-order formulas
2. Application to Horn theories
3. Rewriting-based systems as Horn theories
4. Examples of use
5. Related work
6. Conclusions and future work

Our approach is based on two well-known facts :

[Hodges97, Theorem 1.5.2]

Every set $\mathcal{S}$ of *ground atoms* has an *initial (Herbrand) model* $\mathcal{I}_\mathcal{S}$, i.e.,

- $\mathcal{I}_\mathcal{S} \models \mathcal{S}$ and
- for all models $\mathcal{A}$ of $\mathcal{S}$, there is a homomorphism $h : \mathcal{I}_\mathcal{S} \to \mathcal{A}$.

A *positive boolean combination of atoms* is a formula

$$\bigvee_{i=1}^{m} \bigwedge_{j=1}^{n_i} A_{ij} \tag{4}$$

where the A_{ij} are *atoms*. Satisfiability of the *existential closure* of (4) is *preserved* under homomorphism

[Hodges97, Theorem 2.4.3(a)]

Given interpretations $\mathcal{A}$ and $\mathcal{A}'$ with an homomorphism $h : \mathcal{A} \to \mathcal{A}'$,

$$\mathcal{A} \models (\exists x_1) \cdots (\exists x_k) \bigvee_{i=1}^{m} \bigwedge_{j=1}^{n_i} A_{ij} \implies \mathcal{A}' \models (\exists x_1) \cdots (\exists x_k) \bigvee_{i=1}^{m} \bigwedge_{j=1}^{n_i} A_{ij} \tag{5}$$

According to these results, we have the following:

Corollary

Let $\mathcal{S}$ be a set of ground atoms, and A_{ij} be atoms with variables $x_1, \ldots, x_k$. Then,

$$\mathcal{I}_{\mathcal{S}} \models (\exists x_1) \cdots (\exists x_k) \bigvee_{i=1}^{m} \bigwedge_{j=1}^{n_i} A_{ij} \implies \mathcal{S} \models (\exists x_1) \cdots (\exists x_k) \bigvee_{i=1}^{m} \bigwedge_{j=1}^{n_i} A_{ij} \quad (6)$$

If the set of atoms $\mathcal{S}$ is generated by a set $\mathcal{S}_0$ of Horn sentences, then the interpretation of each predicate symbol P by $\mathcal{I}$ consists of the set of ground atoms $P(t_1, \ldots, t_n)$ such that $\mathcal{S}_0 \vdash P(t_1, \ldots, t_n)$.

Corollary (Semantic criterion)

Let $\mathcal{S}$ be a Horn theory, φ be the existential closure of a positive boolean combination of atoms, and $\mathcal{A}$ be a model of $\mathcal{S}$. If $\mathcal{A} \models \neg\varphi$, then $\mathcal{I}_{\mathcal{S}} \models \neg\varphi$.

Many-sorted theories

The previous corollaries easily generalize to many-sorted signatures: as usual, we just treat sorted variables $x_i : s_i$ by using atoms $S_i(x_i)$ which are added as a new conjunction $\bigwedge_{i=1}^{k} S_i(x_i)$ to the matrix formula (4).

In the following, we focus on *oriented* CTRSs $\mathcal{R}$, with rules

$$\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_n \to t_n$$

whose operational semantics is given by the following inference system:

(Rf) $$\frac{}{x \to^* x}$$

(C) $$\frac{x_i \to y_i}{f(x_1, \ldots, x_i, \ldots, x_k) \to f(x_1, \ldots, y_i, \ldots, x_k)}$$
for all $f \in \mathcal{F}$ and $1 \leq i \leq k = arity(f)$

(T) $$\frac{x \to z \qquad z \to^* y}{x \to^* y}$$

(Rp) $$\frac{s_1 \to^* t_1 \quad \ldots \quad s_n \to^* t_n}{\ell \to r}$$
for all $\ell \to r \Leftarrow s_1 \to t_1 \cdots s_n \to t_n \in \mathcal{R}$

The Horn theory $\overline{\mathcal{R}}$ for a CTRS $\mathcal{R}$ is obtained by *specializing* (C) and (Rp). Inference rules $\frac{B_1 \cdots B_n}{A}$ become universally quantified *implications* $(\forall \vec{x}) B_1 \wedge \cdots \wedge B_n \Rightarrow A$.

Example

For the CTRS $\mathcal{R}$ (from [Giesl & Arts, AAECC'01])

$$\begin{array}{rcl} \mathsf{a} & \to & \mathsf{b} \\ \mathsf{f}(\mathsf{a}) & \to & \mathsf{b} \end{array} \qquad \begin{array}{rcl} \mathsf{g}(x) & \to & \mathsf{g}(\mathsf{a}) \Leftarrow \mathsf{f}(x) \to x \end{array}$$

its associated theory $\overline{\mathcal{R}}$ is

$$\begin{array}{rl} (\forall x) & x \to^* x \\ (\forall x, y, z) & x \to y \wedge y \to^* z \Rightarrow x \to^* z \\ (\forall x, y) & x \to y \Rightarrow \mathsf{f}(x) \to \mathsf{f}(y) \\ (\forall x, y) & x \to y \Rightarrow \mathsf{g}(x) \to \mathsf{g}(y) \end{array} \qquad \begin{array}{rl} & \mathsf{a} \to \mathsf{b} \\ & \mathsf{f}(\mathsf{a}) \to \mathsf{b} \\ (\forall x) & \mathsf{f}(x) \to^* x \Rightarrow \mathsf{g}(x) \to \mathsf{g}(\mathsf{a}) \end{array}$$

Infeasibility of conditional rules

For infeasibity of $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_n \to t_n$ we use φ_{Feas} given by:

$$(\exists \vec{x}) s_1 \to^* t_1 \wedge \cdots \wedge s_n \to^* t_n$$

The following structure $\mathcal{A}$ over $\mathbb{N} - \{0\}$:

$$\mathsf{a}^{\mathcal{A}} = 1 \qquad \mathsf{b}^{\mathcal{A}} = 2 \qquad \mathsf{f}^{\mathcal{A}}(x) = x + 1 \qquad \mathsf{g}^{\mathcal{A}}(x) = 1$$
$$x \to^{\mathcal{A}} y \Leftrightarrow y \geq x \qquad x\,(\to^*)^{\mathcal{A}}\, y \Leftrightarrow y \geq x$$

is a model of $\overline{\mathcal{R}} \cup \{\neg(\exists x)\,\mathsf{f}(x) \to^* x\}$ for our running CTRS $\mathcal{R}$.

Automation

This model has been automatically generated by using the tool AGES:
`http://zenon.dsic.upv.es/ages/`

Thus, rule

$$\mathsf{g}(x) \to \mathsf{g}(\mathsf{a}) \Leftarrow \mathsf{f}(x) \to x$$

is proved $\mathcal{R}$-infeasible.

The following CTRS $\mathcal{R}$ (Example 23 in [Sternagel & Sternagel, FSCD'16])

$$\mathsf{g}(x) \;\to\; \mathsf{f}(x,x) \tag{7}$$
$$\mathsf{g}(x) \;\to\; \mathsf{g}(x) \Leftarrow \mathsf{g}(x) \to \mathsf{f}(\mathsf{a},\mathsf{b}) \tag{8}$$

has a conditional critical pair $\mathsf{f}(x,x) \downarrow \mathsf{g}(x) \Leftarrow \mathsf{g}(x) \to \mathsf{f}(\mathsf{a},\mathsf{b})$. The following structure $\mathcal{A}$ over the finite domain $\{0,1\}$:

$$\mathsf{a}^{\mathcal{A}} = 1 \qquad \mathsf{b}^{\mathcal{A}} = 0 \qquad \mathsf{f}^{\mathcal{A}}(x,y) = \begin{cases} x - y + 1 & \text{if } x \geq y \\ y - x + 1 & \text{otherwise} \end{cases}$$

$$\mathsf{g}^{\mathcal{A}}(x) = 1 \qquad x \to^{\mathcal{A}} y \Leftrightarrow x = y \qquad x\,(\to^*)^{\mathcal{A}}\,y \Leftrightarrow x \geq y$$

is a model $\overline{\mathcal{R}} \cup \{\neg(\exists x)\ \mathsf{g}(x) \to^* \mathsf{f}(\mathsf{a},\mathsf{b})\}$. The critical pair is infeasible.

In the FSCD'16 paper, this is proved by using unification tests together with a transformation. It is discussed that the alternative tree automata techniques investigated in the paper do *not* work for this example.

A term t *loops* if there is a rewrite sequence $t = t_1 \to_{\mathcal{R}} \cdots \to_{\mathcal{R}} t_n$ for some $n > 1$ such that t is a (non-necessarily strict) subterm of t_n, written $t_n \trianglerighteq t$. A CTRS is non-looping if no term loops.

We can check (non)loopingness of terms t or CTRSs $\mathcal{R}$ by using

$$\begin{array}{rcl} \varphi_{Loopt} & \Leftrightarrow & (\exists x, y)\ t \to x \wedge x \to^* y \wedge y \trianglerighteq t \\ \varphi_{Loop} & \Leftrightarrow & (\exists x, y, z)\ x \to y \wedge y \to^* z \wedge z \trianglerighteq x \end{array}$$

for $\overline{\mathcal{R}} \cup H_{\trianglerighteq}$ where $H_{\trianglerighteq}$ describe the subterm relation $\trianglerighteq$:

$$(\forall x)\ \ x \trianglerighteq x \tag{9}$$

$$(\forall x, y, z)\ \ x \trianglerighteq y \wedge y \trianglerighteq z \Rightarrow x \trianglerighteq z \tag{10}$$

$$(\forall x_1, \ldots, x_k)\ \ f(x_1, \ldots, x_k) \trianglerighteq x_i \tag{11}$$

for each k-ary function symbol $f \in \mathcal{F}$ and argument i, $1 \leq i \leq k$.

Example (A non-looping term)

For $\mathcal{R} = \{\mathsf{a} \to \mathsf{c}(\mathsf{b}), \mathsf{b} \to \mathsf{c}(\mathsf{b})\}$, $\overline{\mathcal{R}} \cup H_{\trianglerighteq}$ is:

$$(\forall x)\; x \to^* x \quad (12)$$
$$(\forall x, y, z)\; (x \to y \wedge y \to^* z \Rightarrow x \to^* z) \quad (13)$$
$$(\forall x, y)\; (x \to y \Rightarrow \mathsf{c}(x) \to \mathsf{c}(y)) \quad (14)$$
$$\mathsf{a} \to \mathsf{c}(\mathsf{b}) \quad (15)$$
$$\mathsf{b} \to \mathsf{c}(\mathsf{b}) \quad (16)$$
$$(\forall x)\; x \trianglerighteq x \quad (17)$$
$$(\forall x, y, z)\; x \trianglerighteq y \wedge y \trianglerighteq z \Rightarrow x \trianglerighteq z \quad (18)$$
$$(\forall x)\; \mathsf{c}(x) \trianglerighteq x \quad (19)$$

The following structure over $\mathbb{N} \cup \{-1\}$:

$$\mathsf{a}^{\mathcal{A}} = -1 \qquad \mathsf{b}^{\mathcal{A}} = 1 \qquad \mathsf{c}^{\mathcal{A}}(x) = x$$
$$x \to^{\mathcal{A}} y \Leftrightarrow x \leq 1 \wedge y \geq 1 \qquad x\,(\to^*)^{\mathcal{A}}\, y \Leftrightarrow x \leq y \qquad x \trianglerighteq^{\mathcal{A}} y \Leftrightarrow x \leq y$$

satisfies $\overline{\mathcal{R}} \cup H_{\trianglerighteq} \cup \{\neg\varphi_{Loopt}\}$ where

$$\varphi_{Loopt} \Leftrightarrow (\exists x, y)\; \mathsf{a} \to x \wedge x \to^* y \wedge y \trianglerighteq \mathsf{a}.$$

Therefore, a is non-looping.

Example (A non-cycling TRS)

Although b is a looping term (for $\mathcal{R} = \{\mathsf{a} \to \mathsf{c}(\mathsf{b}), \mathsf{b} \to \mathsf{c}(\mathsf{b})\}$), we can prove it non-cycling (i.e., it does not rewrite into itself in at least one step).

Actually, we can prove $\mathcal{R}$ non-cycling (i.e., no term rewrites into itself in at least one step) with the following structure over $\mathbb{N} \cup \{-1\}$

$$\begin{array}{ccc} \mathsf{a}^{\mathcal{A}} = -1 & \mathsf{b}^{\mathcal{A}} = -1 & \mathsf{c}^{\mathcal{A}}(x) = 2x + 2 \\ x \to^{\mathcal{A}} y \Leftrightarrow x < y & x\,(\to^*)^{\mathcal{A}}\,y \Leftrightarrow x \leq y & \end{array}$$

which is a model of $\overline{\mathcal{R}} \cup \{\neg\varphi_{Cycl}\}$ where

$$\varphi_{Cycl} \Leftrightarrow (\exists x, y)\ x \to y \wedge y \to^* x.$$

We have presented a semantic approach to disprove properties of Horn theories which can be expressed as the satisfability of the existential closure of a positive boolean combination of atoms.

We can apply this approach to rewriting-based systems with

- many-sorted signatures,
- alternative satisfiability notions for the conditions (e.g., joinability), or
- more general components there (e.g., memberships).

We could handle many examples coming from papers developing different specific techniques to deal with these problems.

We have presented a semantic approach to disprove properties of Horn theories which can be expressed as the satisfability of the existential closure of a positive boolean combination of atoms.

We can apply this approach to rewriting-based systems with

- many-sorted signatures,
- alternative satisfiability notions for the conditions (e.g., joinability), or
- more general components there (e.g., memberships).

We could handle many examples coming from papers developing different specific techniques to deal with these problems.

Future work

- Use other *preservation* results for FOL.
- Use these techniques in *tools* for proving computational properties of rewriting-based systems (e.g., confluence, termination, etc.)

Thanks!