Proving Reachability Properties by Coinduction [1]

Dorel Lucanu[1]
(Joint work with Ștefan Ciobâcă)

[1]Department of Computer Science
Alexandru Ioan Cuza University of Iași

SYNASC, September 21, 2018

[1]This work was supported by a grant of the Romanian National Authority for Scientific Research and Innovation, CNCS/CCCDI - UEFISCDI, project number PN-III-P2-2.1-BG-2016-0394, within PNCDI III.

Plan

A Specification of a Transition System

$$\langle n \rangle \twoheadrightarrow \langle n, a \rangle \ \texttt{if} \ \exists y \,.y = a \wedge 2 \leq y \wedge y < n$$
$$\langle n, a \rangle \twoheadrightarrow \langle \text{composite} \rangle \ \texttt{if} \ \text{isEullerWitness}(a, n)$$
$$\langle n, a \rangle \twoheadrightarrow \langle n \rangle \ \texttt{if} \ \neg\text{isEullerWitness}(a, n)$$

where

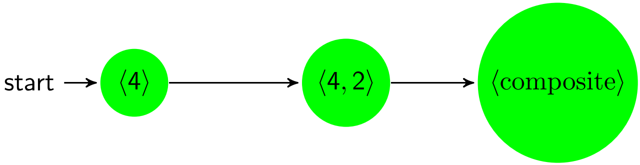
$$\text{isEullerWitness}(a, n) \equiv ((a \mid n) = 0 \vee (a^{\frac{n-1}{2}} \neq a \mid n \pmod n)))$$

$a \mid n$ is the Jacobi symbol

We want to show that
"if $\langle n \rangle$ goes to $\langle \text{composite} \rangle$ then
$\exists n_1, n_2.\, n = n_1 \cdot n_2 \wedge n_1 > 1 \wedge n_2 > 1$".

The First Issue

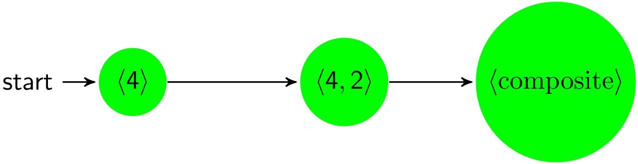
The computations can be finite:



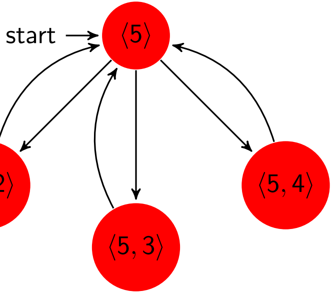
or infinite:

The First Issue

The computations can be finite:



or infinite:



The Second Issue

The conditions

$$\exists y\, .y = a \wedge 2 \leq y \wedge y < n$$

$$((a \mid n) = 0 \vee (a^{\frac{n-1}{2}} \not\equiv a \mid n \pmod n))$$

$$((a \mid n) = 0 \vee (a^{\frac{n-1}{2}} \not\equiv a \mid n \pmod n)) \to \exists n_1, n_2 .\, n = n_1 \cdot n_2 \wedge n_1 > 1 \wedge n_2 > 1$$

are very complex first order formulas including functions and predicates whose definitions are orthogonal with that of the transition system.

Our Proposal

- we use coinduction in order to handle both finite and infinite computations
- we introduce LCTRSs (Logical Constrained Term Rewriting Systems) for specifying transition systems
- we propose an effective proof system that, given a LCTRS, proves valid reachability formulas, assuming an oracle (e.g., an SMT solver) that solves logical constraints

Our Propossal

- we use coinduction in order to handle both finite and infinite computations
- we introduce LCTRSs (Logical Constrained Term Rewriting Systems) for specifying transition systems
- we propose an effective proof system that, given a LCTRS, proves valid reachability formulas, assuming an oracle (e.g., an SMT solver) that solves logical constraints

Our Proposal

- we use coinduction in order to handle both finite and infinite computations
- we introduce LCTRSs (Logical Constrained Term Rewriting Systems) for specifying transition systems
- we propose an effective proof system that, given a LCTRS, proves valid reachability formulas, assuming an oracle (e.g., an SMT solver) that solves logical constraints

Plan

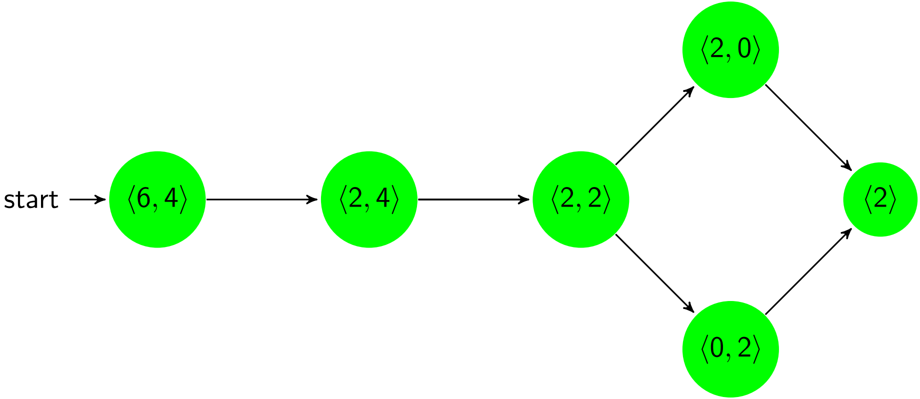
Outline

A Simpler Transition System Specification

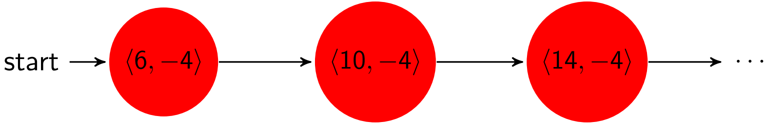
$$
\begin{aligned}
\langle a, b\rangle &\twoheadrightarrow \langle a-b, b\rangle \ \texttt{if}\ a \geq b\\
\langle a, b\rangle &\twoheadrightarrow \langle a, b-a\rangle \ \texttt{if}\ b \geq a\\
\langle a, b\rangle &\twoheadrightarrow \langle a+b\rangle \quad\ \ \texttt{if}\ a = 0 \vee b = 0
\end{aligned}
$$

Two Computations

– finite computations



– infinite computations



A Possible Specification of Computations

- using BNF notation:
  $C ::= \langle a \rangle \mid \langle a, b \rangle \rightsquigarrow C$
- equivalently, using inference rules

$$\frac{}{\langle a \rangle} \qquad \frac{C}{\langle a, b \rangle \rightsquigarrow C}$$

Question

- Are these specifications appropriate?
- I.e., do they uniquely define the computations?

Answer

Yes, if

- we consider the smallest fixed-point satisfying the rules (finite computations, inductively defined), or
- we consider the greatest fixed-point satisfying the rules (finite computations + infinite computations, coinductively defined)

A Possible Specification of Computations

- using BNF notation:
  $C ::= \langle a \rangle \mid \langle a, b \rangle \rightsquigarrow C$
- equivalently, using inference rules

$$\frac{}{\langle a \rangle} \qquad \frac{C}{\langle a, b \rangle \rightsquigarrow C}$$

Question

- Are these specifications appropriate?
- I.e., do they uniquely define the computations?

Answer

Yes, if

- we consider the smallest fixed-point satisfying the rules (finite computations, inductively defined), or
- we consider the greatest fixed-point satisfying the rules (finite computations + infinite computations, coinductively defined)

A Possible Specification of Computations

- using BNF notation:
  $C ::= \langle a \rangle \mid \langle a, b \rangle \rightsquigarrow C$
- equivalently, using inference rules

$$\frac{}{\langle a \rangle} \qquad \frac{C}{\langle a, b \rangle \rightsquigarrow C}$$

Question

- Are these specifications appropriate?
- I.e., do they uniquely define the computations?

Answer

Yes, if

- we consider the smallest fixed-point satisfying the rules (finite computations, inductively defined), or
- we consider the greatest fixed-point satisfying the rules (finite computations + infinite computations, coinductively defined)

A Possible Specification of Computations

- using BNF notation:
  $C ::= \langle a \rangle \mid \langle a, b \rangle \rightsquigarrow C$

- equivalently, using inference rules

$$\frac{}{\langle a \rangle} \qquad \frac{C}{\langle a, b \rangle \rightsquigarrow C}$$

Question

- Are these specifications appropriate?
- I.e., do they uniquely define the computations?

Answer

Yes, if

- we consider the smallest fixed-point satisfying the rules (finite computations, inductively defined), or
- we consider the greatest fixed-point satisfying the rules (finite computations + infinite computations, coinductively defined)

Outline

Complete Lattices

- partial ordered set (poset): set L together with a binary relation $\sqsubseteq \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\bot = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Complete Lattices

- partial ordered set (poset): set L together with a binary relation $\sqsubseteq \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\bot = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Complete Lattices

- partial ordered set (poset): set L together with a binary relation $\sqsubseteq \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\bot = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Complete Lattices

- partial ordered set (poset): set L together with a binary relation $\sqsubseteq\ \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\bot = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Complete Lattices

- partial ordered set (poset): set L together with a binary relation $\sqsubseteq \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\bot = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Complete Lattices

- partial ordered set (poset): set L together with a binary relation $\sqsubseteq \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\bot = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Complete Lattices

- partial ordered set (poset): set L together with a binary relation $\sqsubseteq \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\bot = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Complete Lattices

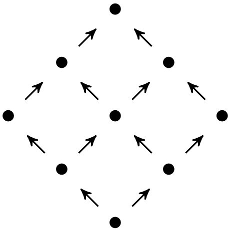
- partial ordered set (poset): set L together with a binary relation $\sqsubseteq \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\perp = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Complete Lattices

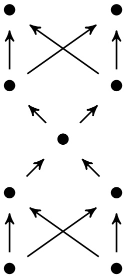
- partial ordered set (poset): set L together with a binary relation $\sqsubseteq \subseteq L \times L$ that is
  - reflexive
  - transitive
  - antisymmetric
- complete lattice = a poset with all lubs (least upper bounds, joins), and hence also all glbs (greatest lower bounds, meets)
- notations:
  - lub of x and y: $x \sqcup y$
  - lub of a set A: $\sqcup A$
  - glb of x and y: $x \sqcap y$
  - glb of a set A: $\sqcap A$
  - $\bot = \sqcap L$
  - $\top = \sqcup L$
- the most known (and used) example: $(\mathcal{P}(X), \subseteq)$, where X is a set

Examples of Lattices

$x \sqsubset y$



complete lattice



poset that is not
a complete lattice

Fixed Points

Let $(L, \sqsubseteq)$ be a complete lattice and $f : L \to L$.

- $x \in L$ pre-fixed point of f if $f(x) \sqsubseteq x$
- $x \in L$ post-fixed point of f if $x \sqsubseteq f(x)$
- $x \in L$ fixed point of f if $f(x) = x$

Terminology:

- pre-fixed point, f-forward-closed, f-closed
- post-fixed point, f-backward-closed, f-stable, f-consistent

Knaster-Tarski Theorem 1/2

Let $(L, \sqsubseteq)$ be a complete lattice.
$f : L \to L$ is monotone if $f(x) \sqsubseteq f(y)$ whenever $x \sqsubseteq y$.

Theorem (Knaster-Tarski)

Any $f : L \to L$ monotone has

- *a least fixed point $\mu\, y.\, f(y)$ (on short $\mu\, f$), and*
- *a greatest fixed point $\nu\, y.\, f(y)$ (on short $\nu\, f$).*

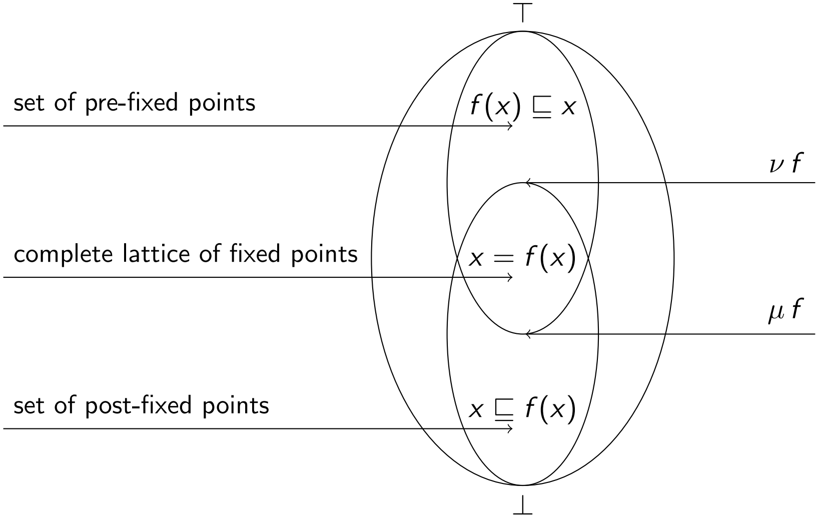
Moreover,

- $\mu\, f = \bigsqcap\{x \mid f(x) \sqsubseteq X\}$ *and*
- $\nu\, f = \bigsqcup\{x \mid x \sqsubseteq f(x)\}$

I.e.,

- $\mu\, f$ is the meet of pre-fixed points
- $\nu\, f$ is the join of post-fixed point

Knaster-Tarski Theorem 2/2



(Co)Induction Proof Principle

$f : L \to L$ monotone

- induction proof principle:

$$\frac{f(x) \sqsubseteq x}{\mu f \sqsubseteq x}\ \mu\text{-rule}$$

- coinduction proof principle:

$$\frac{x \sqsubseteq f(x)}{x \sqsubseteq \nu f}\ \nu\text{-rule}$$

(Co)Continuous Functions and Kleene Theorem

$f : L \to L$ is continuous if $f(\bigsqcup_{n\geq 0} x_n) = \bigsqcup_{n\geq 0} f(x_n)$ for any increasing chain $x_0 \sqsubseteq x_1 \sqsubseteq \cdots$.

$f : L \to L$ is cocontinuous if $f(\bigsqcap_{n\geq 0} x_n) = \bigsqcap_{n\geq 0} f(x_n)$ for any decreasing chain $x_0 \sqsupseteq x_1 \sqsupseteq \cdots$.

Theorem (Kleene)

If $f : L \to L$ is continuous then $\mu f = \bigsqcup_{n\geq 0} f^n(\bot)$.

If $f : L \to L$ is cocontinuous then $\nu f = \bigsqcap_{n\geq 0} f^n(\top)$.

The theorem supplies a practical way to compute the least/greatest fixed points, or their approximations.

(Co)Continuous Functions and Kleene Theorem

$f : L \to L$ is continuous if $f(\bigsqcup_{n\geq 0} x_n) = \bigsqcup_{n\geq 0} f(x_n)$ for any increasing chain $x_0 \sqsubseteq x_1 \sqsubseteq \cdots$.

$f : L \to L$ is cocontinuous if $f(\bigsqcap_{n\geq 0} x_n) = \bigsqcap_{n\geq 0} f(x_n)$ for any decreasing chain $x_0 \sqsupseteq x_1 \sqsupseteq \cdots$.

Theorem (Kleene)

If $f : L \to L$ is continuous then $\mu f = \bigsqcup_{n\geq 0} f^n(\bot)$.

If $f : L \to L$ is cocontinuous then $\nu f = \bigsqcap_{n\geq 0} f^n(\top)$.

The theorem supplies a practical way to compute the least/greatest fixed points, or their approximations.

Inductive and Coinductive Set Definitions

Context:

- U an universe set
- $(L, \sqsubseteq) = (\mathcal{P}(U), \subseteq)$
- $\bot = \emptyset$, $\top = U$
- $\bigsqcup \mathcal{X} = \bigcup \langle X \mid X \in \mathcal{X} \rangle$,
- $\bigsqcap \mathcal{X} = \bigcap \langle X \mid X \in \mathcal{X} \rangle$, where $\mathcal{X} \subseteq \mathcal{P}(U)$

Definition

A set $X \subseteq U$ is inductively defined if there is f monotone s.t. $X = \mu f$.
A set $X \subseteq U$ is coinductively defined if there is f monotone s.t. $X = \nu f$.

Inductive and Coinductive Set Definitions

Context:

- U an universe set
- $(L, \sqsubseteq) = (\mathcal{P}(U), \subseteq)$
- $\bot = \emptyset$, $\top = U$
- $\bigsqcup \mathcal{X} = \bigcup \langle X \mid X \in \mathcal{X} \rangle$,
- $\bigsqcap \mathcal{X} = \bigcap \langle X \mid X \in \mathcal{X} \rangle$, where $\mathcal{X} \subseteq \mathcal{P}(U)$

Definition

A set $X \subseteq U$ is inductively defined if there is f monotone s.t. $X = \mu f$.
A set $X \subseteq U$ is coinductively defined if there is f monotone s.t. $X = \nu f$.

Inductive and Coinductive Set Definitions

Context:

- U an universe set
- $(L, \sqsubseteq) = (\mathcal{P}(U), \subseteq)$
- $\bot = \emptyset$, $\top = U$
- $\bigsqcup \mathcal{X} = \bigcup \langle X \mid X \in \mathcal{X} \rangle$,
- $\bigsqcap \mathcal{X} = \bigcap \langle X \mid X \in \mathcal{X} \rangle$, where $\mathcal{X} \subseteq \mathcal{P}(U)$

Definition

A set $X \subseteq U$ is inductively defined if there is f monotone s.t. $X = \mu f$.
A set $X \subseteq U$ is coinductively defined if there is f monotone s.t. $X = \nu f$.

Inductive and Coinductive Set Definitions

Context:

- U an universe set
- $(L, \sqsubseteq) = (\mathcal{P}(U), \subseteq)$
- $\bot = \emptyset$, $\top = U$
- $\bigsqcup \mathcal{X} = \bigcup \langle X \mid X \in \mathcal{X} \rangle$,
- $\bigsqcap \mathcal{X} = \bigcap \langle X \mid X \in \mathcal{X} \rangle$, where $\mathcal{X} \subseteq \mathcal{P}(U)$

Definition

A set $X \subseteq U$ is inductively defined if there is f monotone s.t. $X = \mu f$.
A set $X \subseteq U$ is coinductively defined if there is f monotone s.t. $X = \nu f$.

Inductive and Coinductive Set Definitions

Context:

- U an universe set
- $(L, \sqsubseteq) = (\mathcal{P}(U), \subseteq)$
- $\bot = \emptyset$, $\top = U$
- $\bigsqcup \mathcal{X} = \bigcup \langle X \mid X \in \mathcal{X} \rangle$,
- $\bigsqcap \mathcal{X} = \bigcap \langle X \mid X \in \mathcal{X} \rangle$, where $\mathcal{X} \subseteq \mathcal{P}(U)$

Definition

A set $X \subseteq U$ is inductively defined if there is f monotone s.t. $X = \mu f$.
A set $X \subseteq U$ is coinductively defined if there is f monotone s.t. $X = \nu f$.

Inductive and Coinductive Set Definitions

Context:

- U an universe set
- $(L, \sqsubseteq) = (\mathcal{P}(U), \subseteq)$
- $\bot = \emptyset$, $\top = U$
- $\bigsqcup \mathcal{X} = \bigcup \langle X \mid X \in \mathcal{X} \rangle$,
- $\bigsqcap \mathcal{X} = \bigcap \langle X \mid X \in \mathcal{X} \rangle$, where $\mathcal{X} \subseteq \mathcal{P}(U)$

Definition

A set $X \subseteq U$ is inductively defined if there is f monotone s.t. $X = \mu f$.
A set $X \subseteq U$ is coinductively defined if there is f monotone s.t. $X = \nu f$.

Outline

Ground (Inference) Systems

[source: David Sangiorgi, 2008 (Chap. 2 in the book Introduction to Bisimulation and Coinduction, 2012)]

Definition

Let U be a set. A ground (inference) rule on U is a pair (S, x), where $S \subseteq U$, $x \in U$.
S is called the premise of the rule and x the conclusion of the rule.

If $S = \{x_1, x_2, \ldots\}$, then a rule (S, x) is written as

$$\frac{x_1, x_2, \ldots}{x}$$

If $S = \emptyset$ then the rule is called axiom.

Functional of a Ground (Inference) System

Definition

A set $\mathcal{R}$ of ground rules yields a function $\widehat{\mathcal{R}} : \mathcal{P}(U) \to \mathcal{P}(U)$ given by

$$\widehat{\mathcal{R}}(X) = \{x \mid (\exists S' \subseteq X)(S', x) \in \mathcal{R}\}.$$

Proposition

If $\mathcal{R}$ is a set of ground rules, then $\widehat{\mathcal{R}}$ is monotone.

It follows that each set of ground rules $\mathcal{R}$ inductively defines a set $\mu\widehat{\mathcal{R}}$ and coinductively defines a set $\nu\widehat{\mathcal{R}}$.

Functional of a Ground (Inference) System at Work

$U = (\mathbb{Z} \cup \{\langle, \rangle, "," , \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a\rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b\rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$

$$X = \left\{\begin{array}{l}\langle 2,5\rangle \rightsquigarrow \langle 5,3\rangle, \\ \rightsquigarrow\rangle 7,2,6\rangle\langle, \\ \langle 1\rangle \rightsquigarrow \langle 1\rangle \rightsquigarrow \cdots\end{array}\right\}$$

$$\widehat{\mathcal{R}}(X) = \{\langle a\rangle \mid a \in \mathbb{Z}\} \cup \left\{\begin{array}{l}\langle a,b\rangle \rightsquigarrow \langle 2,5\rangle \rightsquigarrow \langle 5,3\rangle, \\ \langle a,b\rangle \rightsquigarrow\rightsquigarrow\rangle 7,2,6\rangle\langle, \\ \langle a,b\rangle \rightsquigarrow \langle 1\rangle \rightsquigarrow \langle 1\rangle \rightsquigarrow \cdots\end{array}\middle|\, a, b \in \mathbb{Z}\right\}$$

Functional of a Ground (Inference) System at Work

$$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b \rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$$\mathcal{R} = \{[A], [B]\}$$

$$X = \left\{\begin{array}{l} \langle 2, 5 \rangle \rightsquigarrow \langle 5, 3 \rangle, \\ \rightsquigarrow \rangle 7, 2, 6 \rangle \langle, \\ \langle 1 \rangle \rightsquigarrow \langle 1 \rangle \rightsquigarrow \cdots \end{array}\right\}$$

$$\widehat{\mathcal{R}}(X) = \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \left\{\begin{array}{l} \langle a, b \rangle \rightsquigarrow \langle 2, 5 \rangle \rightsquigarrow \langle 5, 3 \rangle, \\ \langle a, b \rangle \rightsquigarrow \rightsquigarrow \rangle 7, 2, 6 \rangle \langle, \\ \langle a, b \rangle \rightsquigarrow \langle 1 \rangle \rightsquigarrow \langle 1 \rangle \rightsquigarrow \cdots \end{array} \middle|\ a, b \in \mathbb{Z} \right\}$$

Functional of a Ground (Inference) System at Work

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b\rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$

$$X = \left\{\begin{array}{l} \langle 2, 5\rangle \rightsquigarrow \langle 5, 3\rangle, \\ \rightsquigarrow\rangle 7, 2, 6\rangle\langle, \\ \langle 1\rangle \rightsquigarrow \langle 1\rangle \rightsquigarrow \cdots \end{array}\right\}$$

$$\widehat{\mathcal{R}}(X) = \{\langle a\rangle \mid a \in \mathbb{Z}\} \cup \left\{\begin{array}{l|l} \langle a, b\rangle \rightsquigarrow \langle 2, 5\rangle \rightsquigarrow \langle 5, 3\rangle, & \\ \langle a, b\rangle \rightsquigarrow\rightsquigarrow\rangle 7, 2, 6\rangle\langle, & a, b \in \mathbb{Z} \\ \langle a, b\rangle \rightsquigarrow \langle 1\rangle \rightsquigarrow \langle 1\rangle \rightsquigarrow \cdots & \end{array}\right\}$$

Construction of the Least Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b \rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$

fortunately $\widehat{\mathcal{R}}$ is continuous

$\widehat{\mathcal{R}}^0(\emptyset) = \emptyset$

$\widehat{\mathcal{R}}^1(\emptyset) = \{\langle a \rangle \mid a \in \mathbb{Z}\}$

$$\begin{aligned}\widehat{\mathcal{R}}^2(\emptyset) = &\{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ &\{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \mid a, b, c \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}\widehat{\mathcal{R}}^3(\emptyset) = &\{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ &\{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \cup \\ &\{\langle d, e \rangle \rightsquigarrow \langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c, d, e \in \mathbb{Z}\}\end{aligned}$$

...

Construction of the Least Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b \rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$

fortunately $\widehat{\mathcal{R}}$ is continuous

$\widehat{\mathcal{R}}^0(\emptyset) = \emptyset$

$\widehat{\mathcal{R}}^1(\emptyset) = \{\langle a \rangle \mid a \in \mathbb{Z}\}$

$$\begin{aligned}\widehat{\mathcal{R}}^2(\emptyset) = &\{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ &\{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \mid a, b, c \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}\widehat{\mathcal{R}}^3(\emptyset) = &\{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ &\{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \cup \\ &\{\langle d, e \rangle \rightsquigarrow \langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c, d, e \in \mathbb{Z}\}\end{aligned}$$

...

Construction of the Least Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b\rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$

fortunately $\widehat{\mathcal{R}}$ is continuous

$\widehat{\mathcal{R}}^0(\emptyset) = \emptyset$

$\widehat{\mathcal{R}}^1(\emptyset) = \{\langle a \rangle \mid a \in \mathbb{Z}\}$

$$\widehat{\mathcal{R}}^2(\emptyset) = \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \{\langle b, c\rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \mid a, b, c \in \mathbb{Z}\}$$

$$\widehat{\mathcal{R}}^3(\emptyset) = \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \{\langle b, c\rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \cup \{\langle d, e\rangle \rightsquigarrow \langle b, c\rangle \rightsquigarrow \langle a \rangle \mid a, b, c, d, e \in \mathbb{Z}\}$$

...

Construction of the Least Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b \rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$

fortunately $\widehat{\mathcal{R}}$ is continuous

$\widehat{\mathcal{R}}^0(\emptyset) = \emptyset$

$\widehat{\mathcal{R}}^1(\emptyset) = \{\langle a \rangle \mid a \in \mathbb{Z}\}$

$$\begin{aligned}\widehat{\mathcal{R}}^2(\emptyset) =& \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ & \{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \mid a, b, c \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}\widehat{\mathcal{R}}^3(\emptyset) =& \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ & \{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \cup \\ & \{\langle d, e \rangle \rightsquigarrow \langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c, d, e \in \mathbb{Z}\}\end{aligned}$$

...

Construction of the Least Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b \rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$
fortunately $\widehat{\mathcal{R}}$ is continuous

$\widehat{\mathcal{R}}^0(\emptyset) = \emptyset$

$\widehat{\mathcal{R}}^1(\emptyset) = \{\langle a \rangle \mid a \in \mathbb{Z}\}$

$$\begin{aligned}\widehat{\mathcal{R}}^2(\emptyset) =& \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ & \{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \mid a, b, c \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}\widehat{\mathcal{R}}^3(\emptyset) =& \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ & \{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \cup \\ & \{\langle d, e \rangle \rightsquigarrow \langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c, d, e \in \mathbb{Z}\}\end{aligned}$$

...

Construction of the Greatest Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b \rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$
fortunately $\widehat{\mathcal{R}}$ is cocontinuous

$\widehat{\mathcal{R}}^0(U) = U$

$\widehat{\mathcal{R}}^1(U) = \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \{\langle a, b \rangle \rightsquigarrow \tau \mid \tau \in U\}$

$$\begin{aligned}\widehat{\mathcal{R}}^2(U) = & \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ & \{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \cup \\ & \{\langle c, d \rangle \rightsquigarrow \langle a, b \rangle \rightsquigarrow \tau \mid a, b, c, d \in \mathbb{Z}, \tau \in U\}\end{aligned}$$

...

Construction of the Greatest Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b \rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$
fortunately $\widehat{\mathcal{R}}$ is cocontinuous

$\widehat{\mathcal{R}}^0(U) = U$

$\widehat{\mathcal{R}}^1(U) = \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \{\langle a, b \rangle \rightsquigarrow \tau \mid \tau \in U\}$

$$\begin{aligned}\widehat{\mathcal{R}}^2(U) = &\{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ &\{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \cup \\ &\{\langle c, d \rangle \rightsquigarrow \langle a, b \rangle \rightsquigarrow \tau \mid a, b, c, d \in \mathbb{Z}, \tau \in U\}\end{aligned}$$

...

Construction of the Greatest Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^{\infty}$

$$[A]\ \frac{}{\langle a\rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b\rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$
fortunately $\widehat{\mathcal{R}}$ is cocontinuous

$\widehat{\mathcal{R}}^0(U) = U$

$\widehat{\mathcal{R}}^1(U) = \{\langle a\rangle \mid a \in \mathbb{Z}\} \cup \{\langle a, b\rangle \rightsquigarrow \tau \mid \tau \in U\}$

$$\begin{aligned}\widehat{\mathcal{R}}^2(U) = &\{\langle a\rangle \mid a \in \mathbb{Z}\} \cup \\ &\{\langle b, c\rangle \rightsquigarrow \langle a\rangle \mid a, b, c \in \mathbb{Z}\} \cup \\ &\{\langle c, d\rangle \rightsquigarrow \langle a, b\rangle \rightsquigarrow \tau \mid a, b, c, d \in \mathbb{Z}, \tau \in U\}\end{aligned}$$

...

Construction of the Greatest Fixed Point

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$$[A]\ \frac{}{\langle a \rangle}\ a \in \mathbb{Z} \qquad [B]\ \frac{\tau}{\langle a, b \rangle \rightsquigarrow \tau}\ a, b \in \mathbb{Z}$$

$\mathcal{R} = \{[A], [B]\}$

fortunately $\widehat{\mathcal{R}}$ is cocontinuous

$\widehat{\mathcal{R}}^0(U) = U$

$\widehat{\mathcal{R}}^1(U) = \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \{\langle a, b \rangle \rightsquigarrow \tau \mid \tau \in U\}$

$$\begin{aligned}\widehat{\mathcal{R}}^2(U) = & \{\langle a \rangle \mid a \in \mathbb{Z}\} \cup \\ & \{\langle b, c \rangle \rightsquigarrow \langle a \rangle \mid a, b, c \in \mathbb{Z}\} \cup \\ & \{\langle c, d \rangle \rightsquigarrow \langle a, b \rangle \rightsquigarrow \tau \mid a, b, c, d \in \mathbb{Z}, \tau \in U\}\end{aligned}$$

...

Induction Principle on Rules

if $\widehat{\mathcal{R}}(X) \subseteq X$ then $\mu(\widehat{\mathcal{R}}) \subseteq X$

that means that

for a given X,
if for all rules $(S, x) \in R$, if $S \subseteq X$, then also $x \in X$
then $\mu(\widehat{\mathcal{R}}) \subseteq X$

Coinduction Principles on Rules

if $X \subseteq \widehat{\mathcal{R}}(X)$ then $X \subseteq \nu(\widehat{\mathcal{R}})$

that means that

for a given X,
if for all $x \in X$ there is a rule $(S, x) \in R$ with $S \subseteq X$
then $X \subseteq \nu(\widehat{\mathcal{R}})$

Example

$$\langle a, b\rangle \twoheadrightarrow \langle a-b, b\rangle \texttt{ if } a \geq b$$
$$\langle a, b\rangle \twoheadrightarrow \langle a, b-a\rangle \texttt{ if } b \geq a$$
$$\langle a, b\rangle \twoheadrightarrow \langle a+b\rangle \quad \texttt{ if } a = 0 \vee b = 0$$

$U = (\mathbb{Z} \cup \{\langle, \rangle, ",", \rightsquigarrow\})^\infty$

$[A]\ \dfrac{}{\langle a\rangle}\ a \in \mathbb{Z} \qquad [B]\ \dfrac{\tau}{\langle a, b\rangle \rightsquigarrow \tau}$ $\exists$ transition from $\langle a, b\rangle$ to $hd(\tau)$

The set of finite executions: $C^+ = \mu\,\widehat{[A, B]}$

The set of infinite and finite executions: $C^\infty = \nu\,\widehat{[A, B]}$

The set of infinite executions: $C^\omega = \nu\,\widehat{[B]}$

Proof Trees

$$[\mathrm{B}]\ \dfrac{[\mathrm{B}]\ \dfrac{[\mathrm{B}]\ \dfrac{[\mathrm{B}]\ \dfrac{[\mathrm{A}]\ \dfrac{}{\langle 2\rangle}}{\langle 2,0\rangle \leadsto \langle 2\rangle}}{\langle 2,2\rangle \leadsto \langle 2,0\rangle \leadsto \langle 2\rangle}}{\langle 2,4\rangle \leadsto \langle 2,2\rangle \leadsto \langle 2,0\rangle \leadsto \langle 2\rangle}}{\langle 6,4\rangle \leadsto \langle 2,4\rangle \leadsto \langle 2,2\rangle \leadsto \langle 2,0\rangle \leadsto \langle 2\rangle}$$

finite proof tree

$$[\mathrm{B}]\ \dfrac{[\mathrm{B}]\ \dfrac{[\mathrm{B}]\ \dfrac{\cdots}{\langle 14,-4\rangle \leadsto \langle 18,-4\rangle \leadsto \langle 22,-4\rangle \leadsto \cdots}}{\langle 10,-4\rangle \leadsto \langle 14,-4\rangle \leadsto \langle 18,-4\rangle \leadsto \cdots}}{\langle 6,-4\rangle \leadsto \langle 10,-4\rangle \leadsto \langle 14,-4\rangle \leadsto \cdots}$$

infinite proof tree

Proof Trees Supply Proofs

A tree is well-founded if the relation on the nodes, which contains a pair of nodes (n, p) if p is the parent of n, is well-founded.

Remark

Finite proof trees are well-founded.

Proposition

Let $\mathcal{R}$ be a set of a set of ground rules over U such that $\mathcal{R}$ is cocontinuous.

Then $x \in \mu\widehat{\mathcal{R}}$ iff there is a well-founded proof tree of x under $\mathcal{R}$.

Then $x \in \nu\widehat{\mathcal{R}}$ iff there is a proof tree of x under $\mathcal{R}$.

Plan

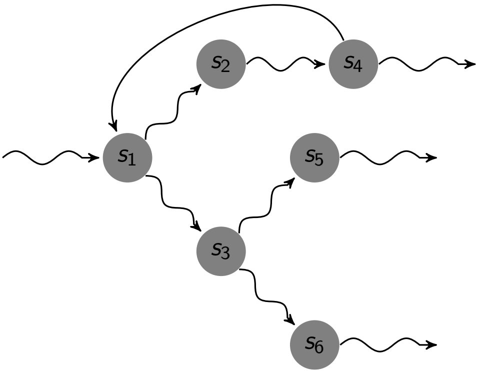
Overview

Semantics First! (J. Goguen)

- transition systems
- state predicate
- derivative (semantically)
- reachability predicate as pairs of state predicates

Transition Systems

$(M, \rightsquigarrow)$, with $\rightsquigarrow \subseteq M \times M$

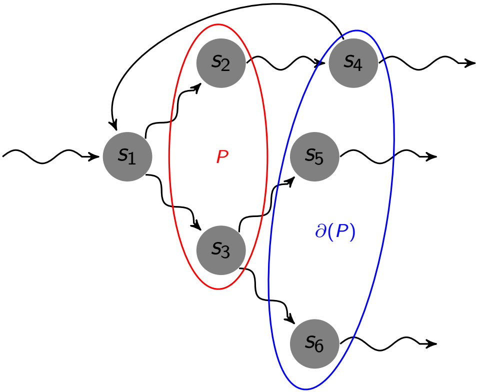


execution paths:

$$\frac{}{\gamma}\ \gamma \in M, \gamma \text{ irreducible} \qquad \frac{\tau}{\gamma_0 \circ \tau}\ \gamma_0 \rightsquigarrow hd(\tau)$$

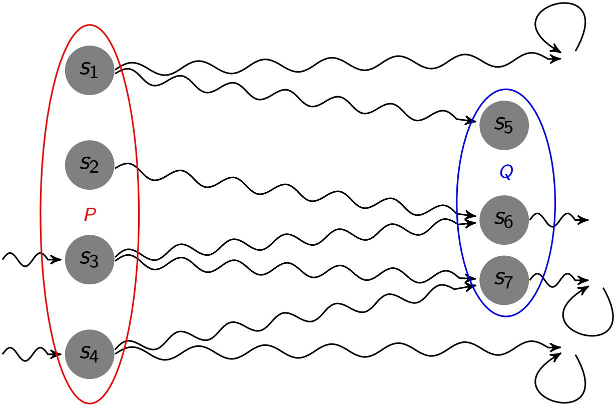
State Predicates and their Derivatives

- state predicate: $P \subseteq M$
- derivative of a state predicate P:
  $\partial(P) = \{\gamma' \mid \gamma \rightsquigarrow \gamma' \text{ for some } \gamma \in P\}$



Reachability Predicates

- a reachability predicate is a pair of state predicates: $P \Rightarrow Q$
- models: transition systems
- satisfiability: $(M, \rightsquigarrow) \models^{\forall} P \Rightarrow Q$ iff any execution path τ *starting from* P ($hd(\tau) \in P$) is infinite or eventually reaches Q



Satisfiability Coinductively

$$(M, \rightsquigarrow) \vDash^{\forall} P \Rightarrow Q$$

iff

$$P \Rightarrow Q \in \nu\, \widehat{\mathrm{DVP}}$$

where DVP consists of the following rules:

$$[\![\mathrm{Subs}]\!]\ \frac{}{P \Rightarrow Q}\ P \subseteq Q \qquad [\![\mathrm{Step}]\!]\ \frac{\partial(P \setminus Q) \Rightarrow Q}{P \Rightarrow Q}\ P \setminus Q \text{ runnable}$$

P is runnable if $P \neq \emptyset$ and for all $\gamma \in P$ there is $\gamma' \in M$ s.t. $\gamma \rightsquigarrow \gamma'$.

Plan

Overview

(based on IJCAR 2018 paper)

- builtin models (local computations, constraints over builtin model solvable by SMT)
- state predicates as constrained terms = $\langle \text{term} \mid \text{constraint-formulas} \rangle$
- reachability predicates as reachability formulas = pair of constrained terms
- transition systems represented as set of rewriting rules logically constrained (LCTRSs)

Overview

(based on IJCAR 2018 paper)

- builtin models (local computations, constraints over builtin model solvable by SMT)
- state predicates as constrained terms $= \langle \mathrm{term} \,|\, \mathrm{constraint\text{-}formulas} \rangle$
- reachability predicates as reachability formulas = pair of constrained terms
- transition systems represented as set of rewriting rules logically constrained (LCTRSs)

Overview

(based on IJCAR 2018 paper)

- builtin models (local computations, constraints over builtin model solvable by SMT)
- state predicates as constrained terms = $\langle \mathrm{term} \mid \mathrm{constraint\text{-}formulas} \rangle$
- reachability predicates as reachability formulas = pair of constrained terms
- transition systems represented as set of rewriting rules logically constrained (LCTRSs)

Overview

(based on IJCAR 2018 paper)

- builtin models (local computations, constraints over builtin model solvable by SMT)
- state predicates as constrained terms $= \langle \mathrm{term} \mid \mathrm{constraint\text{-}formulas} \rangle$
- reachability predicates as reachability formulas $=$ pair of constrained terms
- transition systems represented as set of rewriting rules logically constrained (LCTRSs)

Signatures Modulo a Builtin Model

- a builtin model M^{b} for a many-sorted builtin signature $\Sigma^{\mathrm{b}} = (S^{\mathrm{b}}, F^{\mathrm{b}})$.
  Example: $S^{\mathrm{b}} = \{Int, Bool\}$, $F^{\mathrm{b}} = \{+, \times, \wedge, \vee, \ldots\}$.
- an order-sorted signature $(S, \leq, \Sigma)$ including Σ^{b}
- M^{b} is freely extended to a Σ-model M^{Σ} s. t.:
  - each $f \in \Sigma \setminus \Sigma^{\mathrm{b}}$ is interpreted as a term constructor
  - the Σ^{b}-terms reduced to their values in M^{b}

Signatures Modulo a Builtin Model

- a builtin model M^{b} for a many-sorted builtin signature $\Sigma^{\mathrm{b}} = (S^{\mathrm{b}}, F^{\mathrm{b}})$. Example: $S^{\mathrm{b}} = \{Int, Bool\}$, $F^{\mathrm{b}} = \{+, \times, \wedge, \vee, \ldots\}$.
- an order-sorted signature $(S, \leq, \Sigma)$ including Σ^{b}
- M^{b} is freely extended to a Σ-model M^{Σ} s. t.:
  - each $f \in \Sigma \setminus \Sigma^{\mathrm{b}}$ is interpreted as a term constructor
  - the Σ^{b}-terms reduced to their values in M^{b}

Signatures Modulo a Builtin Model

- a builtin model M^{b} for a many-sorted builtin signature $\Sigma^{\mathsf{b}} = (S^{\mathsf{b}}, F^{\mathsf{b}})$. Example: $S^{\mathsf{b}} = \{Int, Bool\}$, $F^{\mathsf{b}} = \{+, \times, \wedge, \vee, \ldots\}$.
- an order-sorted signature $(S, \leq, \Sigma)$ including Σ^{b}
- M^{b} is freely extended to a Σ-model M^{Σ} s. t.:
  - each $f \in \Sigma \setminus \Sigma^{\mathsf{b}}$ is interpreted as a term constructor
  - the Σ^{b}-terms reduced to their values in M^{b}

Constrained Terms

- constrained terms $\langle t \mid \phi \rangle$
  - t is a Σ-term
  - ϕ is a first-order (with equality) formula
- Example:
  $\langle \mathit{init}(n) \mid \exists u . 1 < u < n \wedge n \ \mathit{mod} \ u = 0 \rangle$
  $\mathit{init} \in \Sigma_{\mathit{Int},\mathit{Cfg}}$, n and u variables of sort Int
- semantically, a constrained term defines a state predicate
  $[\![\langle t \mid \phi \rangle]\!] \triangleq \{\alpha(t) \mid \alpha : X \to M^{\Sigma} \text{ s.t. } M^{\Sigma}, \alpha \vDash \phi\}$.

Constrained Terms

- constrained terms $\langle t \mid \phi \rangle$
  - t is a Σ-term
  - ϕ is a first-order (with equality) formula
- Example:
  $\langle init(n) \mid \exists u . 1 < u < n \wedge n \; mod \; u = 0 \rangle$
  $init \in \Sigma_{Int,Cfg}$, n and u variables of sort Int
- semantically, a constrained term defines a state predicate
  $[\![\langle t \mid \phi \rangle]\!] \triangleq \{\alpha(t) \mid \alpha : X \to M^{\Sigma} \text{ s.t. } M^{\Sigma}, \alpha \models \phi\}$.

Constrained Terms

- constrained terms $\langle t \mid \phi \rangle$
  - t is a Σ-term
  - ϕ is a first-order (with equality) formula
- Example:
  $\langle init(n) \mid \exists u.1 < u < n \wedge n \bmod u = 0 \rangle$
  $init \in \Sigma_{Int,Cfg}$, n and u variables of sort Int
- semantically, a constrained term defines a state predicate
  $[\![\langle t \mid \phi \rangle]\!] \triangleq \{\alpha(t) \mid \alpha : X \to M^{\Sigma} \text{ s.t. } M^{\Sigma}, \alpha \models \phi\}$.

Specification of Transition Systems as LCTRS

- LCTRS = Logical Constrained Term Rewriting System
- example:

$$\begin{array}{l} init(n) \twoheadrightarrow loop(n,2) \texttt{ if } \top, \\ loop(i \times k, i) \twoheadrightarrow comp \texttt{ if } k > 1, \\ loop(n,i) \twoheadrightarrow loop(n, i+1) \texttt{ if } \neg(\exists k. k > 1 \wedge n = i \times k). \end{array}$$

- the general form of a rule: $l \twoheadrightarrow r \texttt{ if } \phi$
- we may think that $\langle l \mid \phi \rangle$ and $\langle r \mid \phi \rangle$ are two constrained terms, but this is not entirely true (see the next slide)
- a LCTRS $\mathcal{R}$ defines a transition relation $\rightsquigarrow_{\mathcal{R}}$ between the corresponding instances of l and r satisfying ϕ
  example: $loop(5,2) \rightsquigarrow_{\mathcal{R}} loop(5,3)$, $loop(8,2) \rightsquigarrow_{\mathcal{R}} comp$

Specification of Transition Systems as LCTRS

- LCTRS = Logical Constrained Term Rewriting System
- example:

$$\begin{array}{l} init(n) \twoheadrightarrow loop(n, 2) \texttt{ if } \top, \\ loop(i \times k, i) \twoheadrightarrow comp \texttt{ if } k > 1, \\ loop(n, i) \twoheadrightarrow loop(n, i + 1) \texttt{ if } \neg(\exists k. k > 1 \wedge n = i \times k). \end{array}$$

- the general form of a rule: $l \twoheadrightarrow r \texttt{ if } \phi$
- we may think that $\langle l \mid \phi \rangle$ and $\langle r \mid \phi \rangle$ are two constrained terms, but this is not entirely true (see the next slide)
- a LCTRS $\mathcal{R}$ defines a transition relation $\rightsquigarrow_{\mathcal{R}}$ between the corresponding instances of l and r satisfying ϕ
  example: $loop(5, 2) \rightsquigarrow_{\mathcal{R}} loop(5, 3)$, $loop(8, 2) \rightsquigarrow_{\mathcal{R}} comp$

Specification of Transition Systems as LCTRS

- LCTRS = Logical Constrained Term Rewriting System
- example:

$$\begin{array}{l} init(n) \twoheadrightarrow loop(n,2) \ \texttt{if}\ \top, \\ loop(i \times k, i) \twoheadrightarrow comp \ \texttt{if}\ k > 1, \\ loop(n,i) \twoheadrightarrow loop(n, i+1) \ \texttt{if}\ \neg(\exists k.k > 1 \wedge n = i \times k). \end{array}$$

- the general form of a rule: $l \twoheadrightarrow r \ \texttt{if}\ \phi$
- we may think that $\langle l \mid \phi \rangle$ and $\langle r \mid \phi \rangle$ are two constrained terms, but this is not entirely true (see the next slide)
- a LCTRS $\mathcal{R}$ defines a transition relation $\rightsquigarrow_{\mathcal{R}}$ between the corresponding instances of l and r satisfying ϕ
  example: $loop(5,2) \rightsquigarrow_{\mathcal{R}} loop(5,3)$, $loop(8,2) \rightsquigarrow_{\mathcal{R}} comp$

Reachability Properties of LCTRSs

- a reachability formula is a pair of constrained terms $\varphi \Rightarrow \varphi'$
- semantics:

$$\mathcal{R} \models^{\forall} \varphi \Rightarrow \varphi'$$

iff

$$(M^{\Sigma}, \rightsquigarrow_{\mathcal{R}}) \models^{\forall} [\![\sigma(\varphi)]\!] \Rightarrow [\![\sigma(\varphi')]\!]$$

for each $\sigma : var(\varphi) \cap var(\varphi') \to M^{\Sigma}$

- the shared variable must have the same values

Derivatives of Constrained Terms

- the derivatives of state predicates are extended to constrained terms
- the set of derivatives of a constrained term $\varphi \triangleq \langle t \mid \phi \rangle$ w.r.t. a rule $l \twoheadrightarrow r$ `if` ϕ_{lr} is

$$\Delta_{l,r,\phi_{lr}}(\varphi) \triangleq \{\langle c[r] \mid \phi' \rangle \mid \phi' \triangleq \phi \wedge t = c[l] \wedge \phi_{lr}, \\ c[\cdot] \text{ an appropriate context} \\ \phi' \text{ is satisfiable}\}.$$

- example:

$$\Delta_{\mathcal{R}}(\langle init(n) \mid \exists u.1 < u < n \wedge n \ mod \ u = 0 \rangle) = \\ \{\langle loop(n,2) \mid \exists u.1 < u < n \wedge n \ mod \ u = 0 \rangle\}.$$

Symbolic Derivatives and the Concrete Ones Agree

Theorem

Let $\varphi \triangleq \langle t \mid \phi\rangle$ be a constrained term, $\mathcal{R}$ a constrained rule system, and $(M^{\Sigma}, \rightsquigarrow_{\mathcal{R}})$ the transition system defined by $\mathcal{R}$. Then $[\![\Delta_{\mathcal{R}}(\varphi)]\!] = \partial([\![\varphi]\!])$.

Plan

Overview

- lift up the inference system to reachability formulas
- add a circular inference rule to infinite proof trees into finite ones

Overview

- lift up the inference system to reachability formulas
- add a circular inference rule to infinite proof trees into finite ones

Proof System (DSTEP($\mathcal{R}$))

it corresponds to the semantic coinductive definition

$$[\text{axiom}]\ \frac{}{\langle t_l \mid \bot \rangle \Rightarrow \langle t_r \mid \phi_r \rangle}$$

$$[\text{subs}]\ \frac{\langle t_l \mid \phi_l \wedge \neg(\exists \tilde{x}. t_l = t_r \wedge \phi_r) \rangle \Rightarrow \langle t_r \mid \phi_r \rangle}{\langle t_l \mid \phi_l \rangle \Rightarrow \langle t_r \mid \phi_r \rangle}\ \ \mathrm{cond}_{\mathsf{s}}$$

$$[\text{der}^{\forall}]\ \frac{\left\langle t^j \mid \phi^j \right\rangle \Rightarrow \langle t_r \mid \phi_r \rangle, j \in \{1, \ldots, n\}}{\langle t_l \mid \phi_l \rangle \Rightarrow \langle t_r \mid \phi_r \rangle}\ \ \mathrm{cond}_{\mathsf{d}}$$

$$\text{where } \Delta_{\mathcal{R}}(\langle t_l \mid \phi_l \rangle) = \{\left\langle t^1 \mid \phi^1 \right\rangle, \ldots, \langle t^n \mid \phi^n \rangle\}$$

The conditions ensure the sound application of the rules.

Example

The infinite proof tree for the reachability formula $\langle init(n) \,|\, \psi \rangle \Rightarrow \varphi_r$, where $\psi \triangleq \exists u.1 < u < n \wedge n \; mod \; u = 0$ and $\varphi_r \triangleq \langle comp \,|\, \top \rangle$:

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\langle comp \,|\, \bot \rangle \Rightarrow \varphi_r}\,[\text{axiom}]}{\langle comp \,|\, \psi \wedge \phi_a \rangle \Rightarrow \varphi_r}\,[\text{subs}] \qquad \dfrac{\dfrac{\dfrac{}{\langle comp \,|\, \bot \rangle \Rightarrow \varphi_r}\,[\text{axiom}]}{\langle comp \,|\, \psi \wedge \phi_2 \wedge \phi_b \rangle \Rightarrow \varphi_r}\,[\text{subs}] \qquad \vdots}{\langle loop(n,3) \,|\, \psi \wedge \phi_2 \rangle \Rightarrow \varphi_r}\,[\text{der}^\forall]}{\langle loop(n,2) \,|\, \psi \rangle \Rightarrow \varphi_r}\,[\text{der}^\forall]}{\langle init(n) \,|\, \psi \rangle \Rightarrow \varphi_r}\,[\text{der}^\forall]
$$

Infinite proof trees cannot be handled in practice, therefore we look for finite representations of them.

Extending the Proof System to the Unbounded Case

Let G be a finite set reachability formulas (goals that we intend to prove). Then the set of rules $\mathsf{DCC}(\mathcal{R}, G)$ consists of $\mathsf{DSTEP}(\mathcal{R})$, together with

$$[\mathrm{circ}]\ \frac{\begin{array}{c}\langle t_r^c \mid \phi_l \wedge \phi \wedge \phi_r^c\rangle \Rightarrow \varphi_r, \\ \langle t_l \mid \phi_l \wedge \neg\phi\rangle \Rightarrow \varphi_r\end{array}}{\langle t_l \mid \phi_l\rangle \Rightarrow \varphi_r} \quad \begin{array}{l}\phi \text{ is } \exists var(t_l^c, \phi_l^c).t_l = t_l^c \wedge \phi_l^c, \\ \langle t_l^c \mid \phi_l^c\rangle \Rightarrow \langle t_r^c \mid \phi_r^c\rangle \in G.\end{array}$$

Theorem (Circularity Principle)

Let $\mathcal{R}$ be a constrained rule system and G a set of goals. If $(\mathcal{R}, G) \vdash^{\forall} G$ then $\mathcal{R} \models^{\forall} G$.

Example

In order to prove $\langle init(n) \mid \psi \rangle \Rightarrow \langle comp \mid \top \rangle$, we choose the following set of circularities

$$G = \left\{ \begin{array}{l} \langle init(n) \mid \psi \rangle \Rightarrow \langle comp \mid \top \rangle, \\ \langle loop(n,i) \mid 2 \leq i \wedge \exists u. i \leq u < n \wedge n \ mod \ u = 0 \rangle \Rightarrow \langle comp \mid \top \rangle \end{array} \right\}.$$

The finite proof tree for the first circularity:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\langle comp \mid \bot \rangle \Rightarrow \varphi_r}\,[\text{axiom}]}{\langle comp \mid \psi \wedge \phi \wedge \top \rangle \Rightarrow \varphi_r}\,[\text{subs}] \qquad \dfrac{}{\langle loop(n,2) \mid \psi \wedge \neg\phi \rangle \Rightarrow \varphi_r}\,[\text{axiom}]}{\langle loop(n,2) \mid \psi \rangle \Rightarrow \varphi_r}\,[\text{circ}]}{\langle init(n) \mid \psi \rangle \Rightarrow \varphi_r}\,[\text{der}^{\forall}]$$

Example

In order to prove $\langle init(n) \mid \psi\rangle \Rightarrow \langle comp \mid \top\rangle$, we choose the following set of circularities

$$G = \left\{ \begin{array}{l} \langle init(n) \mid \psi\rangle \Rightarrow \langle comp \mid \top\rangle, \\ \langle loop(n,i) \mid 2 \le i \wedge \exists u.i \le u < n \wedge n \bmod u = 0\rangle \Rightarrow \langle comp \mid \top\rangle \end{array} \right\}.$$

The finite proof tree for the first circularity:

$$\dfrac{\dfrac{\dfrac{}{\langle comp \mid \bot\rangle \Rightarrow \varphi_r}\,[\text{axiom}]}{\langle comp \mid \psi \wedge \phi \wedge \top\rangle \Rightarrow \varphi_r}\,[\text{subs}] \qquad \dfrac{}{\langle loop(n,2) \mid \psi \wedge \neg\phi\rangle \Rightarrow \varphi_r}\,[\text{axiom}]}{\dfrac{\langle loop(n,2) \mid \psi\rangle \Rightarrow \varphi_r}{\langle init(n) \mid \psi\rangle \Rightarrow \varphi_r}\,[\text{der}^{\forall}]}\,[\text{circ}]$$

Example Proof Tree for the Second Circularity

$$
\dfrac{
\dfrac{\dfrac{}{\langle c \,|\, \bot \rangle \Rightarrow \varphi_r}}{\langle c \,|\, \psi_i \wedge \psi_a \rangle \Rightarrow \varphi_r}
\qquad
\dfrac{
\dfrac{\dfrac{}{\langle c \,|\, \bot \rangle \Rightarrow \varphi_r}}{\langle c \,|\, \psi_i \wedge \psi_b \wedge \psi_c \rangle \Rightarrow \varphi_r}
\qquad
\dfrac{}{\langle l(n, i+1) \,|\, \psi_i \wedge \psi_b \wedge \neg\psi_c \rangle \Rightarrow \varphi_r}
}{\langle l(n, i+1) \,|\, \psi_i \wedge \psi_b \rangle \Rightarrow \varphi_r,}
}{\langle l(n, i) \,|\, \psi_i \rangle \Rightarrow \langle c \,|\, \top \rangle}\ [\mathsf{der}^{\forall}]
$$

Plan

Conclusion

- we defined a framework for proving reachability properties consisting of
  - logical constrained rewriting systems, for specifying transition systems (LCTRS)
  - a coinductive proof system consisting of four rules
- LCTRSs are expressive enough to describe semantics of programming languages (K Framework, G. Roșu)
- there is a prototype that implements the proof system (Ciobâcă, Buruiană)
- further work includes
  - unification modulo builtins (a first step in WOLLIC 2018)
  - extension of the proof systems to program equivalence (a first step in FAoC 2015)