Concurrency Theory

Winter Semester 2015/16

Lecture 6: Mutually Recursive Equational Systems

Joost-Pieter Katoen and Thomas Noll
Software Modeling and Verification Group
RWTH Aachen University

http://moves.rwth-aachen.de/teaching/ws-1516/ct/

Software Modeling and Verification Chair | RWTH AACHEN UNIVERSITY

Partial Orders

Definition (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example

1. $(\mathbb{N}, \leq)$ is a total partial order
2. $(\mathbb{N}, <)$ is not a partial order (since not reflexive)
3. $(2^{\mathbb{N}}, \subseteq)$ is a (non-total) partial order
4. $(\Sigma^*, \sqsubseteq)$ is a (non-total) partial order, where Σ is some alphabet and $\sqsubseteq$ denotes prefix ordering ($u \sqsubseteq v \iff \exists w \in \Sigma^* : uw = v$)

Recap: Fixed-Point Theory

Upper and Lower Bounds

Definition ((Least) upper bounds and (greatest) lower bounds)

Let $(D, \sqsubseteq)$ be a partial order and $T \subseteq D$.

1. An element $d \in D$ is called an upper bound of T if $t \sqsubseteq d$ for every $t \in T$ (notation: $T \sqsubseteq d$). It is called least upper bound (LUB) (or supremum) of T if additionally $d \sqsubseteq d'$ for every upper bound d' of T (notation: $d = \bigsqcup T$).
2. An element $d \in D$ is called an lower bound of T if $d \sqsubseteq t$ for every $t \in T$ (notation: $d \sqsubseteq T$). It is called greatest lower bound (GLB) (or infimum) of T if $d' \sqsubseteq d$ for every lower bound d' of T (notation: $d = \bigsqcap T$).

Example

1. $T \subseteq \mathbb{N}$ has a LUB/GLB in $(\mathbb{N}, \leq)$ iff it is finite/non-empty
2. In $(2^{\mathbb{N}}, \subseteq)$, every subset $T \subseteq 2^{\mathbb{N}}$ has an LUB and GLB:

$$\bigsqcup T = \bigcup T \quad \text{and} \quad \bigsqcap T = \bigcap T$$

Complete Lattices

Definition (Complete lattice)

A complete lattice is a partial order $(D, \sqsubseteq)$ such that all subsets of D have LUBs and GLBs. In this case,

$$\bot := \bigsqcup \emptyset \; (= \bigsqcap D) \qquad \text{and} \qquad \top := \bigsqcap \emptyset \; (= \bigsqcup D)$$

respectively denote the least and greatest element of D.

Example

1. $(\mathbb{N}, \leq)$ is not a complete lattice as, e.g., $\mathbb{N}$ does not have a LUB
2. $(\mathbb{N} \cup \{\infty\}, \leq)$ with $n \leq \infty$ for all $n \in \mathbb{N}$ is a complete lattice
3. $(2^{\mathbb{N}}, \subseteq)$ is a complete lattice

Application to HML with Recursion

Lemma

Let $(S, Act, \longrightarrow)$ *be an LTS. Then* $(2^S, \subseteq)$ *is a complete lattice with*

- $\bigsqcup \mathcal{T} = \bigcup \mathcal{T} = \bigcup_{T \in \mathcal{T}} T$ *for all* $\mathcal{T} \subseteq 2^S$
- $\bigsqcap \mathcal{T} = \bigcap \mathcal{T} = \bigcap_{T \in \mathcal{T}} T$ *for all* $\mathcal{T} \subseteq 2^S$
- $\bot = \bigsqcup \emptyset = \bigsqcap 2^S = \emptyset$
- $\top = \bigsqcap \emptyset = \bigsqcup 2^S = S$

Proof.

omitted □

Monotonicity of Functions

Definition (Monotonicity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders. A function $f : D \to D'$ is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \implies f(d_1) \sqsubseteq' f(d_2).$$

Example

1. $f_1 : \mathbb{N} \to \mathbb{N} : n \mapsto n^2$ is monotonic w.r.t. $(\mathbb{N}, \leq)$
2. $f_2 : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : T \mapsto T \cup \{1, 2\}$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$
3. Let $\mathcal{T} := \{T \subseteq \mathbb{N} \mid T \text{ finite}\}$. Then $f_3 : \mathcal{T} \to \mathbb{N} : T \mapsto \sum_{n \in T} n$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ and $(\mathbb{N}, \leq)$.
4. $f_4 : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : T \mapsto \mathbb{N} \setminus T$ is not monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ (since, e.g., $\emptyset \subseteq \mathbb{N}$ but $f_4(\emptyset) = \mathbb{N} \not\subseteq f_4(\mathbb{N}) = \emptyset$).

The Fixed-Point Theorem

Alfred Tarski (1901–1983)

Theorem (Tarski's fixed-point theorem)

Let $(D, \sqsubseteq)$ be a complete lattice and $f : D \to D$ monotonic. Then f has a least fixed point $\mathrm{fix}(f)$ and a greatest fixed point $\mathrm{FIX}(f)$ given by

$$\mathrm{fix}(f) = \bigsqcap\{d \in D \mid f(d) \sqsubseteq d\} \qquad \textit{(GLB of all pre-fixed points of } f\textit{)}$$

$$\mathrm{FIX}(f) = \bigsqcup\{d \in D \mid d \sqsubseteq f(d)\} \qquad \textit{(LUB of all post-fixed points of } f\textit{)}$$

Proof.

on the board □

The Fixed-Point Theorem for Finite Lattices

Theorem (Fixed-point theorem for finite lattices)

Let $(D, \sqsubseteq)$ *be a finite complete lattice and* $f : D \to D$ *monotonic. Then*

$$\mathrm{fix}(f) = f^m(\bot) \quad \textit{and} \quad \mathrm{FIX}(f) = f^M(\top)$$

for some $m, M \in \mathbb{N}$ *where* $f^0(d) := d$ *and* $f^{k+1}(d) := f(f^k(d))$.

Proof.

on the board □

Example

- Let $f : 2^{\{0,1\}} \to 2^{\{0,1\}} : T \mapsto T \cup \{0\}$
- $f^0(\bot) = \emptyset$, $f^1(\bot) = \{0\}$, $f^2(\bot) = \{0\} = f^1(\bot)$
  $\Longrightarrow$ $\mathrm{fix}(f) = \{0\}$ for $m = 2$
- $f^0(\top) = \{0, 1\}$, $f^1(\top) = \{0, 1\} = f^0(\top)$
  $\Longrightarrow$ $\mathrm{FIX}(f) = \{0, 1\}$ for $M = 1$

Application to HML with Recursion

Lemma

Let $(S, Act, \longrightarrow)$ *be an LTS and* $F \in HMF_X$*. Then*

1. $[\![F]\!] : 2^S \to 2^S$ *is monotonic w.r.t.* $(2^S, \subseteq)$
2. $\mathrm{fix}([\![F]\!]) = \bigcap\{T \subseteq S \mid [\![F]\!](T) \subseteq T\}$
3. $\mathrm{FIX}([\![F]\!]) = \bigcup\{T \subseteq S \mid T \subseteq [\![F]\!](T)\}$

If, in addition, S *is finite, then*

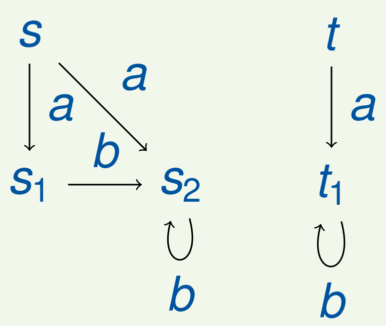
4. $\mathrm{fix}([\![F]\!]) = [\![F]\!]^m(\emptyset)$ *for some* $m \in \mathbb{N}$
5. $\mathrm{FIX}([\![F]\!]) = [\![F]\!]^M(S)$ *for some* $M \in \mathbb{N}$

Proof.

1. by induction on the structure of F (details omitted)
2. by Lemma 5.7 and Theorem 5.12
3. by Lemma 5.7 and Theorem 5.12
4. by Lemma 5.7 and Theorem 5.14
5. by Lemma 5.7 and Theorem 5.14 □

Applying the Fixed-Point Theorem for Finite Lattices

Example 6.1



Let $S := \{s, s_1, s_2, t, t_1\}$.

1. Solution of $X \stackrel{max}{=} \langle b \rangle \mathrm{tt} \wedge [b]X$: on the board
2. Solution of $Y \stackrel{min}{=} \langle b \rangle \mathrm{tt} \vee \langle \{a, b\} \rangle Y$: on the board

Largest Fixed Points and Invariants

- Remember (Example 4.7):
  - Invariant: $Inv(F) \equiv X$ for $F \in HMF$ and $X \stackrel{max}{=} F \wedge [Act]X$
  - $s \models Inv(F)$ if all states reachable from s satisfy F
- Now: formalize argument and prove its correctness (for arbitrary LTSs)
- Let $inv : 2^S \to 2^S : T \mapsto [\![F]\!] \cap [\cdot Act \cdot] T$ be the corresponding semantic function
- By Theorem 5.12, $\mathrm{FIX}(inv) = \bigcup \{T \subseteq S \mid T \subseteq inv(T)\}$
- Direct formulation of invariance property:

$$Inv = \{s \in S \mid \forall w \in Act^*, s' \in S : s \stackrel{w}{\longrightarrow} s' \implies s' \in [\![F]\!]\}$$

Theorem 6.2

For every LTS $(S, Act, \longrightarrow)$, $Inv = \mathrm{FIX}(inv)$ holds.

Proof.

on the board □

Introducing Several Variables

Sometimes useful: using more than one variable

Example 6.3

> *"It is always the case that a process can perform an a-labelled transition leading to a state where b-transitions can be executed forever."*

can be specified by

$$Inv(\langle a \rangle Forever(b))$$

where

$$Inv(F) \stackrel{max}{=} F \land [Act]F \qquad \text{(cf. Theorem 6.2)}$$
$$Forever(b) \stackrel{max}{=} \langle b \rangle Forever(b)$$

Syntax of Mutually Recursive Equational Systems

Definition 6.4 (Syntax of mutually recursive equational systems)

Let $\mathcal{X} = \{X_1, \ldots, X_n\}$ be a set of variables. The set $HMF_{\mathcal{X}}$ of Hennessy-Milner formulae over $\mathcal{X}$ is defined by the following syntax:

$$
\begin{array}{rll}
F ::= & X_i & \text{(variable)} \\
| & \mathrm{tt} & \text{(true)} \\
| & \mathrm{ff} & \text{(false)} \\
| & F_1 \wedge F_2 & \text{(conjunction)} \\
| & F_1 \vee F_2 & \text{(disjunction)} \\
| & \langle\alpha\rangle F & \text{(diamond)} \\
| & [\alpha]F & \text{(box)}
\end{array}
$$

where $1 \leq i \leq n$ and $\alpha \in Act$. A mutually recursive equational system has the form

$$(X_i = F_{X_i} \mid 1 \leq i \leq n)$$

where $F_{X_i} \in HMF_{\mathcal{X}}$ for every $1 \leq i \leq n$.

Semantics of Recursive Equational Systems I

As before: semantics of formula depends on states satisfying the variables

Definition 6.5 (Semantics of mutually recursive equational systems)

Let $(S, Act, \longrightarrow)$ be an LTS and $E = (X_i = F_{X_i} \mid 1 \leq i \leq n)$ a mutually recursive equational system. The semantics of E, $[\![E]\!] : (2^S)^n \to (2^S)^n$, is defined by

$$[\![E]\!](T_1, \ldots, T_n) := ([\![F_{X_1}]\!](T_1, \ldots, T_n), \ldots, [\![F_{X_n}]\!](T_1, \ldots, T_n))$$

where

$$\begin{aligned}
[\![X_i]\!](T_1, \ldots, T_n) &:= T_i \\
[\![\mathrm{tt}]\!](T_1, \ldots, T_n) &:= S \\
[\![\mathrm{ff}]\!](T_1, \ldots, T_n) &:= \emptyset \\
[\![F_1 \wedge F_2]\!](T_1, \ldots, T_n) &:= [\![F_1]\!](T_1, \ldots, T_n) \cap [\![F_2]\!](T_1, \ldots, T_n) \\
[\![F_1 \vee F_2]\!](T_1, \ldots, T_n) &:= [\![F_1]\!](T_1, \ldots, T_n) \cup [\![F_2]\!](T_1, \ldots, T_n) \\
[\![\langle\alpha\rangle F]\!](T_1, \ldots, T_n) &:= \langle\cdot\alpha\cdot\rangle([\![F]\!](T_1, \ldots, T_n)) \\
[\![[\alpha]F]\!](T_1, \ldots, T_n) &:= [\cdot\alpha\cdot]([\![F]\!](T_1, \ldots, T_n))
\end{aligned}$$

Semantics of Recursive Equational Systems II

Lemma 6.6

Let $(S, Act, \longrightarrow)$ *be a finite LTS and* $E = (X_i = F_{X_i} \mid 1 \leq i \leq n)$ *a mutually recursive equational system. Let* $(D, \sqsubseteq)$ *be given by* $D := (2^S)^n$ *and*

$$(T_1, \ldots, T_n) \sqsubseteq (T'_1, \ldots, T'_n)$$

iff $T_i \subseteq T'_i$ *for every* $1 \leq i \leq n$.

1. $(D, \sqsubseteq)$ *is a complete lattice with*
$$\bigsqcup\{(T^i_1, \ldots, T^i_n) \mid i \in I\} = \left(\bigcup\{T^i_1 \mid i \in I\}, \ldots, \bigcup\{T^i_n \mid i \in I\}\right)$$
$$\bigsqcap\{(T^i_1, \ldots, T^i_n) \mid i \in I\} = \left(\bigcap\{T^i_1 \mid i \in I\}, \ldots, \bigcap\{T^i_n \mid i \in I\}\right)$$
2. $[\![E]\!]$ *is monotonic w.r.t.* $(D, \sqsubseteq)$
3. $\mathrm{fix}([\![E]\!]) = [\![E]\!]^m(\emptyset, \ldots, \emptyset)$ *for some* $m \in \mathbb{N}$
4. $\mathrm{FIX}([\![E]\!]) = [\![E]\!]^M(S, \ldots, S)$ *for some* $M \in \mathbb{N}$

Proof.

omitted □