

Concurrency Theory

Lecture 5: Fixed-Point Theory

Joost-Pieter Katoen Thomas Noll

Lehrstuhl für Informatik 2
(Software Modeling and Verification)



{katoen,noll}@cs.rwth-aachen.de

<http://www-i2.informatik.rwth-aachen.de/i2/ct13/>

Winter Semester 2013/14

- 1 Recap: Hennessy-Milner Logic with Recursion
- 2 Complete Lattices
- 3 The Fixed-Point Theorem

Introducing Recursion

Solution: employ **recursion**!

- $Inv(\langle a \rangle tt) \equiv \langle a \rangle tt \wedge [a] \text{Inv}(\langle a \rangle tt)$
- $Pos([a] ff) \equiv [a] ff \vee \langle a \rangle Pos([a] ff)$

Interpretation: the sets of states $X, Y \subseteq S$ satisfying the respective formula should solve the corresponding equation, i.e.,

- $X = \langle \cdot a \cdot \rangle(S) \cap [\cdot a \cdot](X)$
- $Y = [\cdot a \cdot](\emptyset) \cup \langle \cdot a \cdot \rangle(Y)$

Open questions

- Do such recursive equations (always) have solutions?
- If so, are they unique?
- How can we compute whether a process satisfies a recursive formula?

Syntax of HML with One Recursive Variable

Initially: only one variable

Later: mutual recursion

Definition (Syntax of HML with one variable)

The set HMF_X of Hennessy-Milner formulae with one variable X over a set of actions Act is defined by the following syntax:

$F ::= X$	(variable)
tt	(true)
ff	(false)
$F_1 \wedge F_2$	(conjunction)
$F_1 \vee F_2$	(disjunction)
$\langle \alpha \rangle F$	(diamond)
$[\alpha] F$	(box)

where $\alpha \in Act$.

Semantics of HML with One Recursive Variable I

So far: $\llbracket F \rrbracket \subseteq S$ for $F \in HMF$ and LTS $(S, Act, \longrightarrow)$

Now: semantics of formula depends on states that (are assumed to) satisfy X

Definition (Semantics of HML)

Let $(S, Act, \longrightarrow)$ be an LTS and $F \in HMF_X$. The semantics of F ,

$$\llbracket F \rrbracket : 2^S \rightarrow 2^S,$$

is defined by

$$\begin{aligned}\llbracket X \rrbracket(T) &:= T \\ \llbracket tt \rrbracket(T) &:= S \\ \llbracket ff \rrbracket(T) &:= \emptyset \\ \llbracket F_1 \wedge F_2 \rrbracket(T) &:= \llbracket F_1 \rrbracket(T) \cap \llbracket F_2 \rrbracket(T) \\ \llbracket F_1 \vee F_2 \rrbracket(T) &:= \llbracket F_1 \rrbracket(T) \cup \llbracket F_2 \rrbracket(T) \\ \llbracket \langle \alpha \rangle F \rrbracket(T) &:= \langle \cdot \alpha \cdot \rangle(\llbracket F \rrbracket(T)) \\ \llbracket [\alpha] F \rrbracket(T) &:= [\cdot \alpha \cdot](\llbracket F \rrbracket(T))\end{aligned}$$

Semantics of HML with One Recursive Variable III

- Idea underlying the definition of

$$\llbracket . \rrbracket : HMF_X \rightarrow (2^S \rightarrow 2^S) :$$

if $T \subseteq S$ gives the set of states that satisfy X , then $\llbracket F \rrbracket(T)$ will be the set of states that satisfy F

- How to determine this T ?
- According to previous discussion: as solution of **recursive equation** of the form $X = F_X$ where $F_X \in HMF_X$
- But: solution **not unique**; therefore write:

$$X \stackrel{\min}{=} F_X \quad \text{or} \quad X \stackrel{\max}{=} F_X$$

- In the following we will see:
 - Equation $X = F_X$ always **solvable**
 - Least and greatest solutions are **unique** and can be obtained by **fixed-point iteration**

- 1 Recap: Hennessy-Milner Logic with Recursion
- 2 Complete Lattices
- 3 The Fixed-Point Theorem

Definition 5.1 (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 5.2

- 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 ($u \sqsubseteq v \iff \exists w \in \Sigma^* : uw = v$)

Upper and Lower Bounds

Definition 5.3 ((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 5.4

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

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

Definition 5.5 (Complete lattice)

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

$$\perp := \bigsqcap D \quad \text{and} \quad \top := \bigsqcup D$$

respectively denote the **least and greatest element** of D .

Example 5.6

- 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

Lemma 5.7

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 $\mathcal{T} \subseteq 2^S$
- $\perp = \bigsqcap 2^S = \emptyset$
- $\top = \bigsqcup 2^S = S$

Proof.

omitted □

- 1 Recap: Hennessy-Milner Logic with Recursion
- 2 Complete Lattices
- 3 The Fixed-Point Theorem

Definition 5.8 (Fixed point)

Let D be some domain, $d \in D$, and $f : D \rightarrow D$. If

$$f(d) = d$$

then d is called a **fixed point** of f .

Example 5.9

- ① The (only) fixed points of $f_1 : \mathbb{N} \rightarrow \mathbb{N} : n \mapsto n^2$ are 0 and 1
- ② A subset $T \subseteq \mathbb{N}$ is a fixed point of $f_2 : 2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}} : T \mapsto T \cup \{1, 2\}$ iff $\{1, 2\} \subseteq T$

Definition 5.10 (Monotonicity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders. A function $f : D \rightarrow D'$ 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 5.11

- ① $f_1 : \mathbb{N} \rightarrow \mathbb{N} : n \mapsto n^2$ is monotonic w.r.t. $(\mathbb{N}, \leq)$
- ② $f_2 : 2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}} : T \mapsto T \cup \{1, 2\}$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$
- ③ Let $\mathcal{T} := \{T \subseteq \mathbb{N} \mid T \text{ finite}\}$. Then $f_3 : \mathcal{T} \rightarrow \mathbb{N} : T \mapsto \sum_{n \in T} n$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ and $(\mathbb{N}, \leq)$.
- ④ $f_4 : 2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}} : T \mapsto \mathbb{N} \setminus T$ 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 I



Alfred Tarski (1901–1983)

Theorem 5.12 (Tarski's fixed-point theorem)

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

$$\begin{aligned}\text{fix}(f) &= \bigcap \{d \in D \mid f(d) \sqsubseteq d\} && \text{(GLB of all pre-fixed points of } f\text{)} \\ \text{FIX}(f) &= \bigcup \{d \in D \mid d \sqsubseteq f(d)\} && \text{(LUB of all post-fixed points of } f\text{)}\end{aligned}$$

Proof.

on the board



Example 5.13 (cf. Example 5.9)

- Let $f : 2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}} : T \mapsto T \cup \{1, 2\}$
- As seen before: $f(T) = T$ iff $\{1, 2\} \subseteq T$
- Theorem 5.12 for fix :

$$\begin{aligned}\text{fix}(f) &= \bigcap \{d \in D \mid f(d) \sqsubseteq d\} \\ &= \bigcap \{T \subseteq \mathbb{N} \mid f(T) \subseteq T\} \\ &= \bigcap \{T \subseteq \mathbb{N} \mid T \cup \{1, 2\} \subseteq T\} \\ &= \bigcap \{T \subseteq \mathbb{N} \mid \{1, 2\} \subseteq T\} \\ &= \{1, 2\}\end{aligned}$$

- Theorem 5.12 for FIX :

$$\begin{aligned}\text{FIX}(f) &= \bigcup \{d \in D \mid d \sqsubseteq f(d)\} \\ &= \bigcup \{T \subseteq \mathbb{N} \mid T \subseteq f(T)\} \\ &= \bigcup \{T \subseteq \mathbb{N} \mid T \subseteq T \cup \{1, 2\}\} \\ &= \bigcup 2^{\mathbb{N}} \\ &= \mathbb{N}\end{aligned}$$