Concurrency Theory

Lecture 6: Application to Hennessy-Milner Logic

Joost-Pieter Katoen Thomas Noll

Lehrstuhl für Informatik 2
(Software Modeling and Verification)

RWTH AACHEN UNIVERSITY

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

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

Winter Semester 2013/14

Outline

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

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 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:

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

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,

$$\bot := \bigsqcap D \qquad \text{and} \qquad \top := \bigsqcup D$$

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

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 $\mathsf{fix}(f)$ and a greatest fixed point $\mathsf{FIX}(f)$ given by

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

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

Proof.

on the board □

Outline

The Fixed-Point Theorem for Finite Lattices

Theorem 6.1 (Fixed-point theorem for finite lattices)

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

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

for some $m, M \in \mathbb{N}$ *where*

$$f^0(d) := d \quad \text{and} \quad f^{k+1}(d) := f(f^k(d)).$$

The Fixed-Point Theorem for Finite Lattices

Theorem 6.1 (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*

$$f^0(d) := d \quad \textit{and} \quad f^{k+1}(d) := f(f^k(d)).$$

Proof.

on the board □

The Fixed-Point Theorem for Finite Lattices

Theorem 6.1 (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*

$$f^0(d) := d \quad \textit{and} \quad f^{k+1}(d) := f(f^k(d)).$$

Proof.

on the board □

Example 6.2

- Let $f : 2^{\{0,1\}} \to 2^{\{0,1\}} : T \mapsto T \cup \{0\}$

The Fixed-Point Theorem for Finite Lattices

Theorem 6.1 (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*

$$f^0(d) := d \quad \textit{and} \quad f^{k+1}(d) := f(f^k(d)).$$

Proof.

on the board □

Example 6.2

- 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 $m = 2$

The Fixed-Point Theorem for Finite Lattices

Theorem 6.1 (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*

$$f^0(d) := d \quad \textit{and} \quad f^{k+1}(d) := f(f^k(d)).$$

Proof.

on the board □

Example 6.2

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

Application to HML with Recursion I

Lemma 6.3

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.* $(2^S, \subseteq)$

Lemma 6.3

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. $\mathrm{FIX}([\![F]\!]) = \bigcup\{T \subseteq S \mid T \subseteq [\![F]\!](T)\}$

Application to HML with Recursion I

Lemma 6.3

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* $M \in \mathbb{N}$

Application to HML with Recursion I

Lemma 6.3

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. $\text{fix}([\![F]\!]) = \bigcap\{T \subseteq S \mid [\![F]\!](T) \subseteq T\}$
3. $\text{FIX}([\![F]\!]) = \bigcup\{T \subseteq S \mid T \subseteq [\![F]\!](T)\}$

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

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

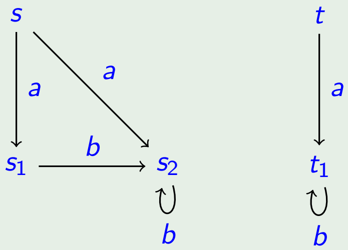
Proof.

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 6.1
5. by Lemma 5.7 and Theorem 6.1

□

Application to HML with Recursion II

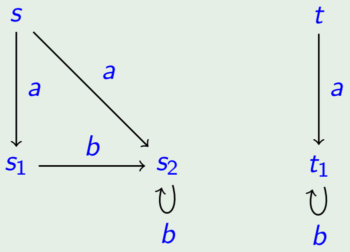
Example 6.4



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

Application to HML with Recursion II

Example 6.4

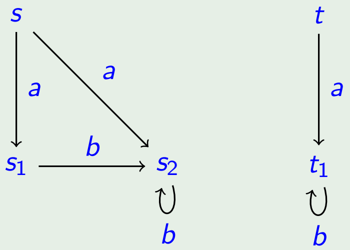


Let $S := \{s, s_1, s_2, t, t_1\}$.

1. Solution of $X \overset{max}{=} \langle b \rangle \mathrm{tt} \wedge [b]X$: on the board

Application to HML with Recursion II

Example 6.4



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

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

Outline

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

Largest Fixed Points and Invariants

- Remember (Example 4.7):
  - Invariant: $Inv(F) \equiv X$ for $F \in HMF$ and $X \overset{max}{=} F \wedge [Act]X$
  - $s \models Inv(F)$ if all states reachable from s satisfy F
- Now: formalize argument and prove its correctness

Largest Fixed Points and Invariants

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

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
- Let $inv : 2^S \to 2^S : T \mapsto [\![F]\!] \cap [\cdot Act \cdot]T$ be the corresponding semantic function
- By Theorem 5.12, $\text{FIX}(inv) = \bigcup\{T \subseteq S \mid T \subseteq inv(T)\}$
- Direct formulation of invariance property:

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

Largest Fixed Points and Invariants

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

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

Theorem 6.5

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

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
- 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:

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

Theorem 6.5

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

Proof.

on the board □