Semantics and Verification

Lecture 6

9 March 2010

Overview

Last lecture:

- Hennessy-Milner logic

This lecture:

- Hennessy-Milner logic with recursion (introduction)
- Tarski's fixed-point theorem

Next lecture:

- Hennessy-Milner logic with recursion

1. Last lecture
2. Hennessy-Milner logic with recursion
3. Lattice theory
4. Tarski's Fixed Point Theorem

Verifying Correctness of Reactive Systems

Equivalence Checking Approach

$$\textit{Impl} \equiv \textit{Spec}$$

- $\equiv$ is an abstract equivalence, e.g. $\sim$ or $\approx$
- *Spec* is often expressed in the same language as *Impl*
- *Spec* provides the full specification of the intended behaviour

Model Checking Approach

$$\textit{Impl} \models \textit{Property}$$

- $\models$ is the satisfaction relation
- *Property* is a particular feature, often expressed via a logic
- *Property* is a partial specification of the intended behaviour

Hennessy-Milner Logic: Syntax

Syntax of the Formulae ($a \in Act$)

$$F, G \; ::= \; tt \mid ff \mid F \wedge G \mid F \vee G \mid \langle a \rangle F \mid [a]F$$

Intuition:

- tt all processes satisfy this property
- ff no process satisfies this property
- $\wedge$, $\vee$ usual logical AND and OR
- $\langle a \rangle F$ there is at least one a-successor that satisfies F
- $[a]F$ all a-successors have to satisfy F

Hennessy-Milner Logic: Denotational Semantics

For a formula F let $[\![F]\!] \subseteq Proc$ contain all states that satisfy F.

Denotational Semantics: $[\![\_]\!] : Formulae \to 2^{Proc}$

- $[\![tt]\!] = Proc$
- $[\![ff]\!] = \emptyset$
- $[\![F \vee G]\!] = [\![F]\!] \cup [\![G]\!]$
- $[\![F \wedge G]\!] = [\![F]\!] \cap [\![G]\!]$
- $[\![\langle a \rangle F]\!] = \langle \cdot a \cdot \rangle [\![F]\!]$
- $[\![[a]F]\!] = [\cdot a \cdot][\![F]\!]$

where $\langle \cdot a \cdot \rangle, [\cdot a \cdot] : 2^{Proc} \to 2^{Proc}$ are defined by

$$\langle \cdot a \cdot \rangle S = \{p \in Proc \mid \exists p'.\ p \xrightarrow{a} p' \text{ and } p' \in S\}$$

$$[\cdot a \cdot] S = \{p \in Proc \mid \forall p'.\ p \xrightarrow{a} p' \implies p' \in S\}$$

Relationship between HML and Strong Bisimilarity

Hennessy-Milner Theorem

Let $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ be an image-finite LTS and $p, q \in Proc$. Then

$$p \sim q$$

if and only if

for every HML formula F: $(p \models F \iff q \models F)$.

- One says that HML is adequate with respect to strong bisimilarity for image-finite LTS.

Is Hennessy-Milner Logic Powerful Enough?

Modal depth (nesting degree) for Hennessy-Milner formulae:

- $md(tt) = md(ff) = 0$
- $md(F \wedge G) = md(F \vee G) = \max\{md(F), md(G)\}$
- $md([a]F) = md(\langle a \rangle F) = md(F) + 1$

Idea: a formula F can "see" only upto depth $md(F)$.

Is Hennessy-Milner Logic Powerful Enough?

Modal depth (nesting degree) for Hennessy-Milner formulae:

- $md(tt) = md(ff) = 0$
- $md(F \wedge G) = md(F \vee G) = \max\{md(F), md(G)\}$
- $md([a]F) = md(\langle a \rangle F) = md(F) + 1$

Idea: a formula F can “see” only upto depth $md(F)$.

Theorem (let F be a HM formula and $k = md(F)$)

If the defender has a winning strategy in the strong bisimulation game from s and t up to k rounds, then $s \models F \iff t \models F$.

Conclusion

There is no Hennessy-Milner formula F that can detect a deadlock in an arbitrary LTS.

Temporal Properties not Expressible in HM Logic

$s \models Inv(F)$ iff all states reachable from s satisfy F
$s \models Pos(F)$ iff there is a reachable state which satisfies F

Fact

Properties $Inv(F)$ and $Pos(F)$ are not expressible in HM logic.

Temporal Properties not Expressible in HM Logic

$s \models Inv(F)$ iff all states reachable from s satisfy F
$s \models Pos(F)$ iff there is a reachable state which satisfies F

Fact

Properties $Inv(F)$ and $Pos(F)$ are not expressible in HM logic.

Let $Act = \{a_1, a_2, \ldots, a_n\}$ be a finite set of actions. We define

- $\langle Act \rangle F \stackrel{\text{def}}{=} \langle a_1 \rangle F \vee \langle a_2 \rangle F \vee \ldots \vee \langle a_n \rangle F$
- $[Act]F \stackrel{\text{def}}{=} [a_1]F \wedge [a_2]F \wedge \ldots \wedge [a_n]F$

$Inv(F) \equiv F \wedge [Act]F \wedge [Act][Act]F \wedge [Act][Act][Act]F \wedge \ldots$
$Pos(F) \equiv F \vee \langle Act \rangle F \vee \langle Act \rangle\langle Act \rangle F \vee \langle Act \rangle\langle Act \rangle\langle Act \rangle F \vee \ldots$

- no deadlock $= Inv(\langle Act \rangle tt)$

Infinite Conjunctions and Disjunctions vs. Recursion

Problems

- Infinite formulae are not allowed in HM logic
- Infinite formulae are difficult to handle

Why not to use recursion?

- $Inv(F)$ expressed by $X \stackrel{\text{def}}{=} F \wedge [Act]X$
- $Pos(F)$ expressed by $Y \stackrel{\text{def}}{=} F \vee \langle Act \rangle Y$

Question: How to define the semantics of such equations?

- Want sets $[\![X]\!], [\![Y]\!] \subseteq 2^{Proc}$

Solving Equations is Tricky

Equations over Natural Numbers ($n \in \mathbb{N}$)

$n = 2 * n$	one solution $n = 0$
$n = n + 1$	no solution
$n = 1 * n$	many solutions (every $n \in \mathbb{N}$ is a solution)

Equations over Sets of Integers ($M \in 2^{\mathbb{N}}$)

$M = (\{7\} \cap M) \cup \{7\}$	one solution $M = \{7\}$
$M = \mathbb{N} \setminus M$	no solution
$M = \{3\} \cup M$	many solutions (every $M \supseteq \{3\}$)

What about Equations over Processes?

$$X \stackrel{\text{def}}{=} [a]ff \vee \langle a \rangle X \quad \Rightarrow \quad \text{find } S \subseteq 2^{Proc} \text{ s.t. } S = [\cdot a \cdot]\emptyset \cup \langle \cdot a \cdot \rangle S$$

General Approach – Lattice Theory

Problem

For a set D and a function $f : D \to D$, for which elements $x \in D$ do we have

$$x = f(x) \text{ ?}$$

Such elements are called fixed points.

Theorem (Tarski)

Let $(D, \sqsubseteq)$ be a complete lattice and let $f : D \to D$ be a monotonic function. Then f has a unique largest fixed point z_{max} and a unique least fixed point z_{min} given by:

$$z_{max} = \sqcup\{x \in D \mid x \sqsubseteq f(x)\}$$

$$z_{min} = \sqcap\{x \in D \mid f(x) \sqsubseteq x\}$$

Partially Ordered Sets

Partially ordered set

A partially ordered set (or simply a partial order) is a pair $(D, \sqsubseteq)$ such that

- D is a set
- $\sqsubseteq \subseteq D \times D$ is a binary relation on D which is
  - reflexive: $\forall d \in D.\ d \sqsubseteq d$
  - antisymmetric: $\forall d, e \in D.\ d \sqsubseteq e \ \wedge\ e \sqsubseteq d \ \Rightarrow\ d = e$
  - transitive: $\forall d, e, f \in D.\ d \sqsubseteq e \ \wedge\ e \sqsubseteq f \ \Rightarrow\ d \sqsubseteq f$

Monotonic Functions

A function $f : D \to D$ is called monotonic if

$$d \sqsubseteq e \ \Rightarrow\ f(d) \sqsubseteq f(e)$$

for all $d, e \in D$.

Supremum and Infimum

Upper/Lower Bounds (Let $X \subseteq D$)

- $d \in D$ is an upper bound for X (written $X \sqsubseteq d$) iff $x \sqsubseteq d$ for all $x \in X$
- $d \in D$ is a lower bound for X (written $d \sqsubseteq X$) iff $d \sqsubseteq x$ for all $x \in X$

Supremum and Infimum

Upper/Lower Bounds (Let $X \subseteq D$)

- $d \in D$ is an upper bound for X (written $X \sqsubseteq d$) iff $x \sqsubseteq d$ for all $x \in X$
- $d \in D$ is a lower bound for X (written $d \sqsubseteq X$) iff $d \sqsubseteq x$ for all $x \in X$

Least Upper Bound and Greatest Lower Bound (Let $X \subseteq D$)

- $d \in D$ is the least upper bound (supremum) for X ($\sqcup X$) iff
  1. $X \sqsubseteq d$
  2. $\forall d' \in D.\ X \sqsubseteq d' \Rightarrow d \sqsubseteq d'$
- $d \in D$ is the greatest lower bound (infimum) for X ($\sqcap X$) iff
  1. $d \sqsubseteq X$
  2. $\forall d' \in D.\ d' \sqsubseteq X \Rightarrow d' \sqsubseteq d$

Complete Lattices and Tarski's Theorem

Complete Lattice

A partially ordered set $(D, \sqsubseteq)$ is called a complete lattice iff $\sqcup X$ and $\sqcap X$ exist for all $X \subseteq D$.

Theorem (Tarski)

Let $(D, \sqsubseteq)$ be a complete lattice and let $f : D \to D$ be a monotonic function.

Then f has a unique largest fixed point z_{max} and a unique least fixed point z_{min} given by:

$$z_{max} \stackrel{\text{def}}{=} \sqcup\{x \in D \mid x \sqsubseteq f(x)\}$$

$$z_{min} \stackrel{\text{def}}{=} \sqcap\{x \in D \mid f(x) \sqsubseteq x\}$$

Computing Fixed Points on Finite Lattices

Let $(D, \sqsubseteq)$ be a complete lattice and $f : D \to D$ monotonic.
Let $f^1(x) \stackrel{\text{def}}{=} f(x)$ and $f^n(x) \stackrel{\text{def}}{=} f(f^{n-1}(x))$ for $n > 1$, i.e.,

$$f^n(x) = \underbrace{f(f(\ldots f}_{n \text{ times}}(x)\ldots)).$$

Theorem

If D is a finite set then there exist integers $M, m > 0$ such that

- $z_{max} = f^M(\top)$
- $z_{min} = f^m(\bot)$

Idea (for z_{min}): The following sequence stabilizes for any finite D

$$\bot \sqsubseteq f(\bot) \sqsubseteq f(f(\bot)) \sqsubseteq f(f(f(\bot))) \sqsubseteq \cdots$$