Lecture 6

- Hennessy-Milner logic and temporal properties
- Tarski's fixed point theorem
- computing fixed points on finite sets
- bisimulation as a fixed point
- Hennessy-Milner logic with recursively defined variables
- game semantics and temporal properties of reactive systems

Verifying Correctness of Reactive Systems

Equivalence Checking Approach

$$Impl \equiv Spec$$

where $\equiv$ is e.g. strong or weak bisimilarity.

Model Checking Approach

$$Impl \models F$$

where F is a formula from e.g. Hennessy-Milner logic.

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

Theorem (for Image-Finite LTS)

It holds that $p \sim q$ if and only if p and q satisfy exactly the same Hennessy-Milner formulae.

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 defending strategy in the strong bisimulation game from s and t upto k rounds then $s \models F$ if and only if $t \models F$.

Corollary

E.g., there is no Hennessy-Milner formula F that expresses reachability of deadlock.

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

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

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

Infinite Conjunctions and Disjunctions vs. Recursion

Problems

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

What about to use recursion?

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

Question: How to define the semantics of such equations?

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

What about Equations over Processes?

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

Tarski's Fixed Point Theorem (for powersets)

Given a set S, we consider its powerset $2^S = \{X \mid X \subseteq S\}$, partially ordered by the set inclusion $\subseteq$ (reflexive, transitive and antisymmetric).
A set $Z \subseteq S$ is called a fixed point (or a fixpoint) of a function $f : 2^S \rightarrow 2^S$ if $f(Z) = Z$. A fixed point Z of f is the greatest fixed point of f if for every fixed point Y of f we have $Y \subseteq Z$; Z is the least fixed point of f if for every fixed point Y of f we have $Z \subseteq Y$.
A function $f : 2^S \rightarrow 2^S$ (mapping subsets of S to subsets of S) is monotonic iff $X \subseteq Y$ implies $f(X) \subseteq f(Y)$.

Theorem (Knaster, Tarski)

Let $f : 2^S \rightarrow 2^S$ be a monotonic function.
Then f has the (unique) greatest fixed point Z_{max} and the (unique) least fixed point Z_{min}, given by:

$$Z_{max} \stackrel{\text{def}}{=} \cup\{X \subseteq S \mid X \subseteq f(X)\}$$

$$Z_{min} \stackrel{\text{def}}{=} \cap\{X \subseteq S \mid f(X) \subseteq X\}$$

A relation of the greatest and least fixed points

Suppose $f : 2^S \rightarrow 2^S$ is monotonic.

$$Z_{max} = \cup\{X \subseteq S \mid X \subseteq f(X)\}$$

What is the complement of Z_{max}, i.e. $\overline{Z_{max}} = S - Z_{max}$?

$\overline{Z_{max}} = \overline{\cup\{X \mid X \subseteq f(X)\}} = \cap\{\overline{X} \mid X \subseteq f(X)\} = \cap\{Y \mid \overline{Y} \subseteq f(\overline{Y})\} = \cap\{Y \mid \overline{f(\overline{Y})} \subseteq Y\} = \cap\{Y \mid f_d(Y) \subseteq Y\}$

where $f_d(Y) = \overline{f(\overline{Y})}$ (f_d is the dual function to f)
We note that f_d is monotonic
$X \subseteq Y \Rightarrow \overline{Y} \subseteq \overline{X} \Rightarrow f(\overline{Y}) \subseteq f(\overline{X}) \Rightarrow \overline{f(\overline{X})} \subseteq \overline{f(\overline{Y})} \Rightarrow f_d(X) \subseteq f_d(Y))$
and thus

Observation

The complement of the greatest fixed point of f is the least fixed point of the dual function f_d.

Computing fixed points Min and Max for finite sets

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 S is finite and $f : 2^S \rightarrow 2^S$ is monotonic then there exist integers $M, m > 0$ such that

- $Z_{max} = f^M(S)$
- $Z_{min} = f^m(\emptyset)$

Idea (for Z_{min}): The following sequence stabilizes

$$\emptyset \subseteq f(\emptyset) \subseteq f(f(\emptyset)) \subseteq f(f(f(\emptyset))) \subseteq \cdots$$

(Recalling of) Definition of Strong Bisimulation

Let $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ be an LTS.

Strong Bisimulation

A binary relation $R \subseteq Proc \times Proc$ is a strong bisimulation iff whenever $(s, t) \in R$ then for each $a \in Act$:

- if $s \xrightarrow{a} s'$ then $t \xrightarrow{a} t'$ for some t' such that $(s', t') \in R$
- if $t \xrightarrow{a} t'$ then $s \xrightarrow{a} s'$ for some s' such that $(s', t') \in R$.

Two processes $p, q \in Proc$ are strongly bisimilar ($p \sim q$) iff there exists a strong bisimulation R such that $(p, q) \in R$.

$$\sim \; = \; \bigcup \{R \mid R \text{ is a strong bisimulation}\}$$

Strong Bisimulation as a Greatest Fixed Point

Function $\mathcal{F} : 2^{(Proc \times Proc)} \longrightarrow 2^{(Proc \times Proc)}$

Let $X \subseteq Proc \times Proc$. Then we define $\mathcal{F}(X)$ as follows:

$(s, t) \in \mathcal{F}(X)$ if and only if for each $a \in Act$:

- if $s \xrightarrow{a} s'$ then $t \xrightarrow{a} t'$ for some t' such that $(s', t') \in X$
- if $t \xrightarrow{a} t'$ then $s \xrightarrow{a} s'$ for some s' such that $(s', t') \in X$.

Observations

- $\mathcal{F}$ is monotonic
- S is a strong bisimulation if and only if $S \subseteq \mathcal{F}(S)$

Strong Bisimilarity is the Greatest Fixed Point of $\mathcal{F}$

$$\sim = \bigcup \{S \in 2^{(Proc \times Proc)} \mid S \subseteq \mathcal{F}(S)\}$$

HML with One Recursively Defined Variable

Syntax of Formulae

Formulae are given by the following abstract syntax

$$F ::= X \mid tt \mid ff \mid F_1 \wedge F_2 \mid F_1 \vee F_2 \mid \langle a \rangle F \mid [a]F$$

where $a \in Act$ and X is a distinguished variable with a definition

- $X \stackrel{\min}{=} F_X$, or $X \stackrel{\max}{=} F_X$ (syntax in CWB: $min(X.F_X)$, $max(X.F_X)$)

such that F_X is a formula of the logic (which can contain X).

How to Define Semantics?

For every formula F we define a function $O_F : 2^{Proc} \rightarrow 2^{Proc}$ s.t.

- if S is the set of processes that satisfy X then
- $O_F(S)$ is the set of processes that satisfy F.

Definition of $O_F : 2^{Proc} \longrightarrow 2^{Proc}$ (let $S \subseteq Proc$)

$$
\begin{array}{rcl}
O_X(S) & = & S \\
O_{tt}(S) & = & Proc \\
O_{ff}(S) & = & \emptyset \\
O_{F_1 \wedge F_2}(S) & = & O_{F_1}(S) \cap O_{F_2}(S) \\
O_{F_1 \vee F_2}(S) & = & O_{F_1}(S) \cup O_{F_2}(S) \\
O_{\langle a \rangle F}(S) & = & \langle \cdot a \cdot \rangle O_F(S) \\
O_{[a]F}(S) & = & [\cdot a \cdot] O_F(S)
\end{array}
$$

O_F is monotonic for every formula F

$$S_1 \subseteq S_2 \;\Rightarrow\; O_F(S_1) \subseteq O_F(S_2)$$

Proof: easy (structural induction on the structure of F).

Semantics

Observation

O_F is monotonic on $(2^{Proc}, \subseteq)$, so O_F has the (unique) greatest fixed point and the (unique) least fixed point.

Semantics of the Variable X

- If $X \stackrel{\max}{=} F_X$ then

$$[\![X]\!] = \bigcup \{S \subseteq Proc \mid S \subseteq O_{F_X}(S)\}.$$

- If $X \stackrel{\min}{=} F_X$ then

$$[\![X]\!] = \bigcap \{S \subseteq Proc \mid O_{F_X}(S) \subseteq S\}.$$

Game Characterization

Intuition: the attacker claims $s \not\models F$, the defender claims $s \models F$.

Configurations of the game are of the form (s, F)

- (s, tt) and (s, ff) have no successors
- (s, X) has one successor (s, F_X)
- $(s, F_1 \wedge F_2)$ has two successors (s, F_1) and (s, F_2) (selected by the attacker)
- $(s, F_1 \vee F_2)$ has two successors (s, F_1) and (s, F_2) (selected by the defender)
- $(s, [a]F)$ has successors (s', F) for every s' s.t. $s \xrightarrow{a} s'$ (selected by the attacker)
- $(s, \langle a \rangle F)$ has successors (s', F) for every s' s.t. $s \xrightarrow{a} s'$ (selected by the defender)

Who is the Winner?

Play is a maximal sequence of configurations formed according to the rules given on the previous slide.

Finite Play

- The attacker is the winner of a finite play if the defender gets stuck or the players reach a configuration (s, ff).
- The defender is the winner of a finite play if the attacker gets stuck or the players reach a configuration (s, tt).

Infinite Play

- The attacker is the winner of an infinite play if X is defined as $X \stackrel{\min}{=} F_X$.
- The defender is the winner of an infinite play if X is defined as $X \stackrel{\max}{=} F_X$.

Game Characterization

Theorem

- $s \models F$ if and only if the defender has a universal winning strategy from (s, F)
- $s \not\models F$ if and only if the attacker has a universal winning strategy from (s, F)

Selection of Temporal Properties

- *Inv*(F): $X \overset{\max}{=} F \wedge [Act]X$
- *Pos*(F): $X \overset{\min}{=} F \vee \langle Act\rangle X$

- *Safe*(F): $X \overset{\max}{=} F \wedge ([Act]\mathit{ff} \vee \langle Act\rangle X)$
- *Even*(F): $X \overset{\min}{=} F \vee (\langle Act\rangle \mathit{tt} \wedge [Act]X)$

- $F\ \mathcal{U}^w\ G$: $X \overset{\max}{=} G \vee (F \wedge [Act]X)$
- $F\ \mathcal{U}^s\ G$: $X \overset{\min}{=} G \vee (F \wedge \langle Act\rangle \mathit{tt} \wedge [Act]X)$

Using until we can express e.g. *Inv*(F) and *Even*(F):

$$Inv(F) \equiv F\ \mathcal{U}^w\ \mathit{ff} \qquad\qquad Even(F) \equiv \mathit{tt}\ \mathcal{U}^s\ F$$

Examples of More Advanced Recursive Formulae

Nested Definitions of Recursive Variables

$$X \stackrel{\min}{=} Y \vee \langle Act \rangle X \qquad\qquad Y \stackrel{\max}{=} \langle a \rangle tt \wedge \langle Act \rangle Y$$

Solution: compute first $[\![Y]\!]$ and then $[\![X]\!]$.

Mutually Recursive Definitions

$$X \stackrel{\max}{=} [a] Y \qquad\qquad Y \stackrel{\max}{=} \langle a \rangle X$$

Solution: consider a complete lattice $(2^{Proc} \times 2^{Proc}, \sqsubseteq)$ where $(S_1, S_2) \sqsubseteq (S_1', S_2')$ iff $S_1 \subseteq S_1'$ and $S_2 \subseteq S_2'$.

Note: In the previous case we refer to a generalization of Tarski's Theorem which holds for all complete lattices.