Semantics and Verification 2005

Lecture 5

- Hennessy-Milner logic
- syntax and semantics
- correspondence with strong bisimilarity
- examples in CWB

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Equivalence Checking vs. Model Checking
Modal and Temporal Properties

Verifying Correctness of Reactive Systems

Let *Impl* be an implementation of a system (e.g. in CCS syntax).

Equivalence Checking Approach

$$Impl \equiv Spec$$

- $\equiv$ 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

$$Impl \models Property$$

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

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Equivalence Checking vs. Model Checking
Modal and Temporal Properties

Model Checking of Reactive Systems

Our Aim

Develop a logic in which we can express interesting properties of reactive systems.

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Equivalence Checking vs. Model Checking
Modal and Temporal Properties

Logical Properties of Reactive Systems

Modal Properties – what can happen now (possibility, necessity)

- drink a coffee (can drink a coffee now)
- does not drink tea
- drinks both tea and coffee
- drinks tea after coffee

Temporal Properties – behaviour in time

- never drinks any alcohol
  (safety property: nothing bad can happen)
- eventually will have a glass of wine
  (liveness property: something good will happen)

Can these properties be expressed using equivalence checking?

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Syntax
Semantics
Negation in Hennessy-Milner Logic
Denotational Semantics

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
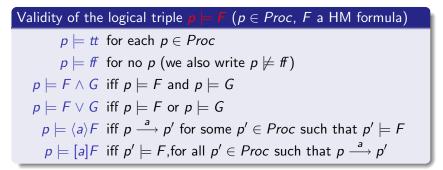
$[a]F$ all a-successors have to satisfy F

Remark

Temporal properties like *always/never in the future* or *eventually* are not included.

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Syntax
Semantics
Negation in Hennessy-Milner Logic
Denotational Semantics

Hennessy-Milner Logic – Semantics

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

Validity of the logical triple $p \models F$ ($p \in Proc$, F a HM formula)

$\qquad p \models tt$ for each $p \in Proc$

$\qquad p \models ff$ for no p (we also write $p \not\models ff$)

$\quad p \models F \wedge G$ iff $p \models F$ and $p \models G$

$\quad p \models F \vee G$ iff $p \models F$ or $p \models G$

$\quad\ p \models \langle a \rangle F$ iff $p \xrightarrow{a} p'$ for some $p' \in Proc$ such that $p' \models F$

$\quad\ p \models [a]F$ iff $p' \models F$, for all $p' \in Proc$ such that $p \xrightarrow{a} p'$

We write $p \not\models F$ whenever p does not satisfy F.

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Syntax
Semantics
Negation in Hennessy-Milner Logic
Denotational Semantics

What about Negation?

For every formula F we define the formula F^c as follows:

- $tt^c = ff$
- $ff^c = tt$
- $(F \wedge G)^c = F^c \vee G^c$
- $(F \vee G)^c = F^c \wedge G^c$
- $(\langle a \rangle F)^c = [a]F^c$
- $([a]F)^c = \langle a \rangle F^c$

Theorem (F^c is equivalent to the negation of F)

For any $p \in Proc$ and any HM formula F

1. $p \models F \Longrightarrow p \not\models F^c$
2. $p \not\models F \Longrightarrow p \models F^c$

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Syntax
Semantics
Negation in Hennessy-Milner Logic
Denotational Semantics

Hennessy-Milner Logic – Denotational Semantics

For a formula F let $\llbracket F \rrbracket \subseteq Proc$ contain all states that satisfy F.

Denotational Semantics: $\llbracket \_ \rrbracket : Formulae \rightarrow 2^{Proc}$

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

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

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

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

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Syntax
Semantics
Negation in Hennessy-Milner Logic
Denotational Semantics

The Correspondence Theorem

Theorem

Let $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ be an LTS, $p \in Proc$ and F a formula of Hennessy-Milner logic. Then

$$p \models F \quad \text{if and only if} \quad p \in \llbracket F \rrbracket.$$

Proof: by structural induction on the structure of the formula F.

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Image-Finite Labelled Transition Systems
Hennessy-Milner Theorem
Example Sessions in CWB

Image-Finite Labelled Transition System

Image-Finite System

Let $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ be an LTS. We call it image-finite iff for every $p \in Proc$ and every $a \in Act$ the set

$$\{p' \in Proc \mid p \xrightarrow{a} p'\}$$

is finite.

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Image-Finite Labelled Transition Systems
Hennessy-Milner Theorem
Example Sessions in CWB

Relationship between HM Logic and Strong Bisimilarity

Theorem (Hennessy-Milner)

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

$$p \sim q$$

if and only if

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

Introduction
Hennessy-Milner Logic
Correspondence between HM Logic and Strong Bisimilarity

Image-Finite Labelled Transition Systems
Hennessy-Milner Theorem
Example Sessions in CWB

CWB Session

```
borg$ /pack/FS/CWB/cwb
```

hm.cwb

```
agent S = a.S1;
agent S1 = b.0 + c.0;

agent T = a.T1 + a.T2;
agent T1 = b.0;
agent T2 = c.0;
```

```
> input "hm.cwb";
> print;
> help logic;
> checkprop(S,<a>(<b>T & <c>T));
 true
> checkprop(T,<a>(<b>T & <c>T));
 false
> help dfstrong;
> dfstrong(S,T);
 [a]<b>T
> exit;
```