Concurrency Theory

Winter 2025/26

Lecture 9: Properties of Hennessy-Milner Logic

Thomas Noll, Peter Thiemann
Programming Languages Group
University of Freiburg

https://proglang.github.io/teaching/25ws/ct.html

Thomas Noll, Peter Thiemann

Winter 2025/26

Closure under Negation I

Observation: Negation is *not* one of the HML constructs.

Reason: HML is closed under complement.

Lemma 9.1

For every $F \in HMF$ *there exists* $F^c \in HMF$ *such that* $[\![F^c]\!] = S \setminus [\![F]\!]$ *for every LTS* $(S, Act, \longrightarrow)$.

Proof.

Definition of F^c:

$$\begin{array}{rclcrcl} \mathrm{tt}^c & := & \mathrm{ff} & \qquad & \mathrm{ff}^c & := & \mathrm{tt} \\ (F_1 \wedge F_2)^c & := & F_1^c \vee F_2^c & & (F_1 \vee F_2)^c & := & F_1^c \wedge F_2^c \\ (\langle\alpha\rangle F)^c & := & [\alpha]F^c & & ([\alpha]F)^c & := & \langle\alpha\rangle F^c \end{array}$$

Closure under Negation II

Proof (Lemma 9.1; continued).

We show $[\![F^c]\!] = S \setminus [\![F]\!]$ by induction on the structure of $F \in HMF$:

- $F = \mathrm{tt}$ ($F = \mathrm{ff}$ analogously):

$$[\![F^c]\!] = [\![\mathrm{ff}]\!] \overset{Def.\ 8.2}{=} \emptyset = S \setminus S \overset{Def.\ 8.2}{=} S \setminus [\![\mathrm{tt}]\!] = S \setminus [\![F]\!]$$

- $F = F_1 \wedge F_2$ ($F = F_1 \vee F_2$ analogously):

$$\begin{aligned}
[\![F^c]\!] &= [\![F_1^c \vee F_2^c]\!] \\
&\overset{Def.\ 8.2}{=} [\![F_1^c]\!] \cup [\![F_2^c]\!] \\
&\overset{ind.\ hyp.}{=} S \setminus [\![F_1]\!] \cup S \setminus [\![F_2]\!] \\
&\overset{de\ Morgan}{=} S \setminus ([\![F_1]\!] \cap [\![F_2]\!]) \\
&\overset{Def.\ 8.2}{=} S \setminus [\![F]\!]
\end{aligned}$$

Closure under Negation II

Proof (Lemma 9.1; continued).

We show $[\![F^c]\!] = S \setminus [\![F]\!]$ by induction on the structure of $F \in HMF$:

- $F = \langle\alpha\rangle F_0$ ($F = [\alpha]F_0$ analogously):

$$
\begin{aligned}
[\![F^c]\!] &= [\![[\alpha]F_0^c]\!] \\
&\overset{Def.\ 8.2}{=} [\cdot\alpha\cdot]([\![F_0^c]\!]) \\
&\overset{Def.\ 8.2}{=} \{s \in S \mid \forall s' \in S : s \xrightarrow{\alpha} s' \Rightarrow s' \in [\![F_0^c]\!]\} \\
&\overset{ind.\ hyp.}{=} \{s \in S \mid \forall s' \in S : s \xrightarrow{\alpha} s' \Rightarrow s' \in S \setminus [\![F_0]\!]\} \\
&= \{s \in S \mid \forall s' \in [\![F_0]\!] : s \not\xrightarrow{\alpha} s'\} \\
&= S \setminus \{s \in S \mid \exists s' \in [\![F_0]\!] : s \xrightarrow{\alpha} s'\} \\
&\overset{Def.\ 8.2}{=} S \setminus \langle\cdot\alpha\cdot\rangle([\![F_0]\!]) \\
&\overset{Def.\ 8.2}{=} S \setminus [\![F]\!]
\end{aligned}
$$

$\square$

HML and Process Traces I

Lemma 9.2 (HML and process traces)

Let $(S, Act, \longrightarrow)$ be an LTS, and let $s, t \in S$ satisfy the same HMF (i.e., for all $F \in HMF$: $s \models F \iff t \models F$). Then $Tr(s) = Tr(t)$.

Proof.

Let $s, t \in S$ such that for all $F \in HMF$: $s \models F \iff t \models F$.

Assumption: $Tr(s) \neq Tr(t)$.
Then there exists $n \geq 1$ and $w = \alpha_1 \ldots \alpha_n \in Act^+$ with $w \in Tr(s) \setminus Tr(t)$
(or vice versa).
Hence, for $F := \langle\alpha_1\rangle \ldots \langle\alpha_n\rangle \mathrm{tt} \in HMF$: $s \models F$ but $t \not\models F$. ↯ $\square$

HML and Process Traces II

Remark: The converse does *not* hold.

Example 9.3

- Let
  - $P := a.(b.\text{nil} + c.\text{nil}) \in Prc$ and
  - $Q := a.b.\text{nil} + a.c.\text{nil} \in Prc$.
- Then $Tr(P) = Tr(Q) = \{\varepsilon, a, ab, ac\}$.
- Let $F := [a](\langle b\rangle\text{tt} \wedge \langle c\rangle\text{tt}) \in HMF$.
- Then $P \models F$ but $Q \not\models F$.
- Thus: HML can distinguish branching behaviour of processes (just as bisimulation can...).

Strong Bisimilarity and HML

- Strong bisimilarity (and observation congruence) are based on mutual mimicking of processes.
- They possess the required properties of behavioural equivalences.
- In particular, $\sim$ and $\approx^c$ are deadlock-sensitive CCS congruences.
- Hennessy-Milner Logic (HML) is a logic for expressing properties of processes.

Aim

Study the connection between strong bisimilarity and satisfaction of HML formulae.

Finitely Branching Transition Systems

Definition 9.4 (Finitely branching LTS)

- A process $P \in Prc$ is finitely branching if the set $\{P' \in Prc \mid P \xrightarrow{\alpha} P'\}$ is finite for every $\alpha \in Act$.
- A labelled transition system is finitely branching if each state is finitely branching.

Example 9.5

(1) The process $A_{rep} = a.\text{nil} \parallel A_{rep}$ ("A replicated") is not finitely branching. By induction on n, one can prove that for each $n \in \mathbb{N}$:

$$A_{rep} \xrightarrow{a} \underbrace{a.\text{nil} \parallel \cdots \parallel a.\text{nil}}_{n \text{ times}} \parallel \text{nil} \parallel A_{rep}$$

(2) Also the "process" $A^{<\omega} = \sum_{i \in \mathbb{N}} a^i$ with $a^0 = \text{nil}$ and $a^{i+1} = a.a^i$ is not finitely branching:

Relationship Between HML and Strong Bisimilarity I

Theorem 9.6 (Hennessy-Milner Theorem)

Let $(S, Act, \{\xrightarrow{a} \mid a \in Act\})$ *be a finitely branching LTS and* $s, t \in S$. *Then:*

$$s \sim t \quad \textit{iff} \quad \textit{for every } F \in HMF : (s \models F \iff t \models F)\,.$$

Proof.

"$\Rightarrow$": Assume $s \sim t$ and $s \models F$ for some $F \in HMF$.
We show $t \models F$ by structural induction on F. Interesting cases:

- $F = \langle\alpha\rangle F'$:
  - Since $s \models F$, there ex. $s' \in S$ such that $s \xrightarrow{\alpha} s'$ and $s' \models F'$.
  - Since $s \sim t$, there ex. $t' \in S$ such that $t \xrightarrow{\alpha} t'$ and $s' \sim t'$.
  - By induction hypothesis, $t' \models F'$. Thus, $t \models \langle\alpha\rangle F' = F$.
- $F = [\alpha]F'$: Assume that $t \xrightarrow{\alpha} t'$ for some $t' \in S$.
  - Since $s \sim t$, there ex. $s' \in S$ such that $s \xrightarrow{\alpha} s'$ and $s' \sim t'$.
  - Since $s \models [\alpha]F'$, also $s' \models F'$.
  - By induction hypothesis, $t' \models F'$. Thus,

Relationship Between HML and Strong Bisimilarity II

Theorem (Hennessy-Milner Theorem)

Let $(S, Act, \{\xrightarrow{a} \mid a \in Act\})$ *be a finitely branching LTS and* $s, t \in S$. *Then:*

$$s \sim t \quad \text{iff} \quad \text{for every } F \in HMF : (s \models F \iff t \models F)\,.$$

Proof.

"$\Leftarrow$": Define $u \equiv v$ iff $(u \models F \iff v \models F)$ for every $F \in HMF$, and let $s \equiv t$.

We prove $s \sim t$ by showing that $\equiv$ is a strong bisimulation.

To this aim, let $u \equiv v$ and $u \xrightarrow{\alpha} u'$ for some $u' \in S$.

We have to show that ex. $v' \in S$ with $v \xrightarrow{\alpha} v'$ and $u' \equiv v'$.

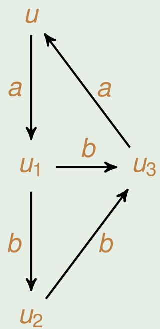
- Assume that there is no such v'.
- Let $\{v' \in S \mid v \xrightarrow{\alpha} v'\} = \{v'_1, \ldots, v'_n\}$ with $n \in \mathbb{N}$ (finitely branching!).
- By the previous assumption, $u' \not\equiv v'_i$ for each $i \in [n]$.
- Thus, for each $i \in [n]$ there ex. $F_i \in HMF$ with $u' \models F_i$ and $v'_i \not\models F_i$.
  (If $u' \not\models F_i$ and $v'_i \models F_i$, then consider F_i^c [Lemma 9.1]

Proving Non-Bisimilarity

Proving non-bisimilarity

Showing $P \not\sim Q$ thus amounts to finding a single HML-formula F with $P \models F$ and $Q \not\models F$.

Example 9.7



Distinguishing formulae
(satisfied by row state / violated by column state):

	u	u_1	u_2	u_3
u	—	$\langle a\rangle$tt	$\langle a\rangle$tt	$\langle a\rangle\langle b\rangle$tt
u_1	$[a]$ff	—	—	$[a]$ff
u_2	$[a]$ff	—	—	$[a]$ff
u_3	$\langle a\rangle\langle a\rangle$tt	$\langle a\rangle$tt	$\langle a\rangle$tt	—

Counterexample for Non-Finitely Branching Processes

Lemma 9.8

Let $A^{<\omega} = \sum_{i \in \mathbb{N}} a^i$ *(see Example 9.5) and* $A^\omega = a.A^\omega$*. Then* $A^{<\omega}$ *and* $A^{<\omega} + A^\omega$

(1) *are not strongly bisimilar, but*

(2) *satisfy the same HML formulae.*

Proof.

(1) Assume that $A^{<\omega} \sim A^{<\omega} + A^\omega$. Then $A^{<\omega} + A^\omega \xrightarrow{a} A^\omega$ must be mimicked by $A^{<\omega} \xrightarrow{a} a^{i-1}$ for some $i \geq 1$. But obviously $A^\omega \not\sim a^{i-1}$.

(2) By structural induction on $F \in HMF$, using the following lemma. $\square$

Lemma 9.9

For every $F \in HMF$*,* $A^\omega \models F$ *iff* $a^k \models F$*, where* k *is the modal depth*[a] *of* F*.*

[a] the maximal number of nested occurrences of modal operators in F

Recap: Weak Bisimulation

Definition (Weak transition relation; Definition 5.8)

For $\alpha \in Act$, $\stackrel{\alpha}{\Longrightarrow} \subseteq Prc \times Prc$ is given by

$$\stackrel{\alpha}{\Longrightarrow} := \begin{cases} \left(\stackrel{\tau}{\longrightarrow}\right)^* \circ \stackrel{\alpha}{\longrightarrow} \circ \left(\stackrel{\tau}{\longrightarrow}\right)^* & \text{if } \alpha \neq \tau \\ \left(\stackrel{\tau}{\longrightarrow}\right)^* & \text{if } \alpha = \tau. \end{cases}$$

where $\left(\stackrel{\tau}{\longrightarrow}\right)^*$ denotes the reflexive and transitive closure of relation $\stackrel{\tau}{\longrightarrow}$.

Definition (Weak bisimulation; Definition 5.9) (Milner 1989)

A binary relation $\rho \subseteq Prc \times Prc$ is a weak bisimulation whenever for every $(P, Q) \in \rho$ and $\alpha \in Act$ (including $\alpha = \tau$):

(1) if $P \stackrel{\alpha}{\longrightarrow} P'$, then there exists $Q' \in Prc$ such that $Q \stackrel{\alpha}{\Longrightarrow} Q'$ and $P' \,\rho\, Q'$, and

(2) if $Q \stackrel{\alpha}{\longrightarrow} Q'$, then there exists $P' \in Prc$ such that $P \stackrel{\alpha}{\Longrightarrow} P'$ and $P' \,\rho\, Q'$.

Introducing Weak Modalities

Goal: Modify HML by turning strong modal operators into weak ones
(see J. Parrow et al.: *Weak Nominal Modal Logic*, FORTE 2017)

Introducing Weak Modalities

Definition 9.10 (Syntax and semantics of weak modalities)

- *wHMF* is obtained from *HMF* of (Definition 8.1) by replacing $\langle\alpha\rangle$ and $[\alpha]$ with

$$\langle\langle\alpha\rangle\rangle F \quad \text{and} \quad [[\alpha]]F$$

  for $\alpha \in Act$ and $F \in wHMF$.

- Modifying Definition 8.2, for an LTS $(S, Act, \longrightarrow)$ and $F \in wHMF$ we let

$$[\![\langle\langle\alpha\rangle\rangle F]\!] := \langle\langle\cdot\alpha\cdot\rangle\rangle([\![F]\!]) \qquad [\![[[\alpha]]F]\!] := [[\cdot\alpha\cdot]]([\![F]\!])$$

  where $\langle\langle\cdot\alpha\cdot\rangle\rangle, [[\cdot\alpha\cdot]] : 2^S \to 2^S$ are given by

$$\langle\langle\cdot\alpha\cdot\rangle\rangle(T) := \{s \in S \mid \exists s' \in T : s \overset{\alpha}{\Longrightarrow} s'\}$$
$$[[\cdot\alpha\cdot]](T) := \{s \in S \mid \forall s' \in S : s \overset{\alpha}{\Longrightarrow} s' \text{ implies } s' \in T\}$$

  Again, we write $s \models F$ iff $s \in [\![F]\!]$, and $F, G \in wHMF$ are equivalent (written $F \equiv G$) iff they are satisfied by the same processes in every LTS.

Relationship Between HML with Weak Modalities and Weak Bisimilarity

Theorem 9.11 (Hennessy-Milner Theorem for weak bisimulation)

Let $(S, Act, \{\xrightarrow{a} \mid a \in Act\})$ *be a finitely branching LTS and* $s, t \in S$. *Then:*

$$s \approx t \quad \text{iff} \quad \text{for every } F \in wHMF : (s \models F \iff t \models F).$$

Proof.

see J. Parrow et al.: *Weak Nominal Modal Logic*, FORTE 2017 □

Example 9.12 (Counterexample to congruence of weak bisimilarity)

- Lecture 6: $\tau.a.\text{nil} + b.\text{nil} \not\approx a.\text{nil} + b.\text{nil}$
- Distinguishing *wHMF* formula: $\langle\langle\tau\rangle\rangle[[b]]\text{ff}$
- Check using CAAL